

Министерство цифрового развития, связи и массовых коммуникаций РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет телекоммуникаций и
информатики»



В.Г. Фокин

Оптические сети и квантовые коммуникации

Практикум
для образовательной программы по направлению (специальности)
11.03.02 «Инфокоммуникационные технологии и системы связи»,
профиль/специализация – «Транспортные сети и системы связи»,
«Мультисервисные телекоммуникационные системы»
квалификация бакалавр

Новосибирск 2024

УДК 621.39

В.Г.Фокин. Оптические сети и квантовые коммуникации. Практикум. - Новосибирск: ФГБОУ ВО СибГУТИ. 2024 г. – 219 с.

Практикум «Оптические сети и квантовые коммуникации» предназначен для студентов направления 11.03.02 «Инфокоммуникационные технологии и системы связи», профиль/специализация – «Транспортные сети и системы связи», «Мультисервисные телекоммуникационные системы», обучающихся по очной и заочной форме. Практикум состоит из 5 разделов (глав) и списка литературы. Каждая глава содержит отдельную тему с кратким конспектом лекционного материала, контрольные вопросы и расчётно-графическое задание по индивидуальному варианту для студента по программе дисциплины.

Кафедра «Фотоники в телекоммуникациях»

Ил. 158 , табл.10, список лит. 58 назв.

Рецензент:

Утверждено редакционно-издательским советом СибГУТИ в качестве практикума

© Сибирский государственный университет
телекоммуникаций и информатики, 2024.

Содержание

1. Введение. Необходимость построения защищённых оптических сетей и роль квантовых технологий.....	5
1.1. Оптические сети. Определение, назначение, технологии.....	6
1.2. Квантовые коммуникации	7
1.3. Терминология для оптических сетей и квантовых коммуникаций.....	10
1.4. Стандартизация оптических транспортных сетей и оптических сетей доступа с применением защиты информации.....	22
1.5. Физическая защита в волоконно-оптических системах передачи и оптических сетей.....	31
Контрольные вопросы.....	48
Задача 1.....	50
2. Оптические транспортные сети и сети доступа с физической защитой информационных соединений и защитой на основе криптографии в интерфейсах.....	52
2.1. Классификация защиты оптических соединений.....	52
2.2. Технические средства физической защиты оптических соединений и информации.....	53
2.3. Криптография для защиты оптических соединений. Основные Определения.....	58
2.4. Нормативное регулирование средств криптографической защиты информации в каналах связи, основанное на Федеральных законах, стандартах, приказах, положениях и инструкциях.....	61
2.5. Государственное регулирование.....	62
2.6. Симметричные и асимметричные криптосистемы.....	66
2.7. Алгоритм шифрования с симметричным ключом, получивший наибольшее распространение.....	75
2.8. Применение криптографии в каналах оптических сетей связи.....	79
Контрольные вопросы.....	100
Задача 2.....	102
3. Оптические квантовые коммуникации и место применения квантово-криптографической защиты оптических сетевых соединений.....	103
3.1. Что такое квантовые коммуникации?.....	103
3.2. Основы физики квантовых коммуникаций.....	105
3.3. Протоколы квантового распределения ключей.....	110
3.4. Протокол распределения квантовых ключей BB84.....	118
3.5. Квантовая запутанность и протоколы распределения ключей.....	120
3.6. Оборудование квантовых коммуникаций для сетей связи.....	122
3.7. Построение квантово-защищённых оптических сетей.....	134
3.8. Проблемы шифрования и квантовых коммуникаций.....	136
3.9. Постквантовая криптография.....	138
Контрольные вопросы.....	138

Задача 3.....	140
4. Инженерная инфраструктура центров обработки данных, кабельная инфраструктура и способы защиты соединений.....	142
4.1. Инженерная инфраструктура ЦОД. Основные компоненты.....	147
4.2. Структурированная кабельная система и телекоммуникационное оборудование ЦОД.....	149
4.3. Обязательная разрабатываемая документация для ЦОД.....	150
4.4. Топологии ЦОД.....	150
4.5. Кабельная инфраструктура ЦОД.....	153
4.6. Функциональные узлы ЦОД.....	154
4.7. СКС в ЦОД.....	155
4.8. Оптические кабели ЦОД. Многомодовые OM1-OM5 (MMF).....	158
4.9. Оптические кабели ЦОД. Одномодовые решения SMF.....	162
4.10. Электрические кабели ЦОД. Международный стандарт ISO / IEC 11801 <i>"Информационные технологии — универсальные кабели для помещений заказчика"</i>	167
4.11. Основные варианты кабельной инфраструктуры СКС и размещения коммутаторов в ЦОД.....	173
4.12. Претерминированные соединения в ЦОД.....	180
4.13. Соединения между ЦОД (на примере комплекса оборудования ВОЛГА, Т8).....	183
4.14. Безопасность коммутаций в ЦОД.....	185
4.15. Системы обеспечения безопасности ЦОД.....	189
4.16. ЦОДы в России.....	191
Контрольные вопросы.....	193
Задача 4.....	194
5. Профессиональные стандарты направления оптических сетей и квантовых коммуникаций для специалистов.....	195
5.1. Специалист по монтажу и технической эксплуатации квантовых сетей 06.050.....	195
5.2. Специалист по исследованиям и разработкам в области квантовых коммуникаций 06.054.....	202
Контрольные вопросы.....	214
Заключение.....	214
Список литературы.....	215

1. Введение. Необходимость построения защищённых оптических сетей и роль квантовых технологий.

Терминология для оптических сетей и квантовых коммуникаций.
Стандартизация оптических транспортных сетей и оптических сетей доступа.



ВВЕДЕНИЕ

Проблема, связанная с защитой персональной информации, передаваемой по телекоммуникационным каналам сетей общего пользования, на сегодняшний день представляет большой интерес. Возможности высокоскоростных компьютеров и квантовых компьютеров, интенсивно развивающихся последнее время, значительно упростили процесс расшифровки информации. К примеру, с расшифровкой 1024-битного кода RSA процессор Pentium 4 управился чуть более чем за 104 часа. Вне зависимости от конкретной реализации, безопасность информации сегодня обеспечивается за счёт превышения среднего времени расшифровки над временем актуальности данных. Данная проблема может быть решена с помощью специального шифра, разработанного К. Шенноном, который принято считать «абсолютным». Однако в этом случае перед пользователем встанет задача обмениваться уникальными ключами перед каждым сеансом связи, что увеличивает риск их перехвата и последующей компрометации данных. А теперь представьте себе такую линию связи, которую невозможно прослушать никакими способами, поскольку это противоречит законам физики. Что бы ни пытался предпринять злоумышленник, у него не получится перехватить передаваемую информацию. Такие устройства для передачи данных, использующие принципы квантовой криптографии, создаются рядом предприятий по заказам различных пользователей каналов связи. Примерами

таких компаний в России являются: ООО «Квантовые коммуникации» – малом инновационном предприятии при университете ИТМО (С-Пб); предприятие «Квазар»; центр квантовых технологий (ЦКТ) МГУ им. М.В. Ломоносова; компания «Инфотекс», Казанский квантовый центр («КАИ-КВАНТ») Казанского НИТУ им. А.Н. Туполева и другие. В развитии квантовых коммуникаций проявили большую заинтересованность и включились в сотрудничество крупные государственные и акционерные предприятия: ПАО «Ростелеком», ОАО «РЖД», ГК «Росатом», ГК «Ростех», ПАО «Микрон», АО «Газпромбанк», ПАО «Сбербанк». МФТИ и Центр компетенций НТИ «Квантовые коммуникации» НИТУ «МИСиС» реализуют программу «Управление проектами в сфере квантовых коммуникаций». Применение квантовых коммуникаций нацелено на защиту информационных сообщений, передаваемых в оптических каналах оптических транспортных сетей различного масштаба (местных, региональных, магистральных), в частности между центрами обработки данных (ЦОД), которые создают и поддерживают выше перечисленные предприятия. Кроме того, правительство России подготовило документ «Распоряжение Правительства РФ от 11 июля 2023 г. № 1856-р Об утверждении Концепции регулирования отрасли квантовых коммуникаций в РФ до 2030 г.» (<https://www.garant.ru/products/ipo/prime/doc/407297268/?ysclid=lmiqse24rb159880381>).

Первые стандарты в области квантовых коммуникаций и квантового интернета вещей, которые открывают серию национальных стандартов в области квантовых технологий, утвердили в России. В рамках дорожной карты "Квантовые коммуникации" разработаны 6 национальных стандартов, 4 из них уже утверждены Росстандартом. Таким образом, можно говорить о том, что сформированы единые требования к оборудованию, что, в свою очередь, обеспечит конкурентоспособность и качество продукции, а также повысит экономическую эффективность внедрения технологии

1.1. Оптические сети. Определение, назначение, технологии

Что представляют собой оптические сети связи в современном положении?

Оптические сети представляют собой коммуникационные сети высокой и сверхвысокой (от десятков Гбит/с, сотен Тбит/с и до Пбит/с) пропускной способности, базирующиеся на волоконно-оптических технологиях и элементах, предполагающих маршрутизацию и коммутацию оптических соединений, формирования и восстановления уровней мощности оптических волн, переносящих информационную нагрузку. Основная задача оптических сетей связи состоит в транспортировке любого вида информационной нагрузки на любые дистанции с заданным высоким качеством.

Оптические сети имеют детальное классификационное деление на локальные, сети доступа, технологические сети, ведомственные сети, сети городов (или метро-сети), сети региональные и сети магистральные. При этом информационные виды нагрузки в оптических сетях могут быть представлены аналоговыми и цифровыми сигналами.

Цифровые сигналы из-за их высокой помехоустойчивости являются преобладающими в современных коммуникациях и представляют собой потоки с циклической (TDM, Time Division Multiplexing - мультиплексирование с разделением во времени) и пакетной организацией (PDM, Packet Division Multiplexing - мультиплексирование с разделением пакетов), переносящие любой вид информации (речевые сообщения, документальные данные, видеоизображения, мультисервисную нагрузку и т.д.) в оптических каналах.

Аналоговые решения в оптических сетях с точки зрения качества оцениваются отношением сигнал/шум (SNR, signal noise ratio), в оптических каналах оптическим отношением сигнал/шум (OSNR, optical signal noise ratio). Цифровые решения в оптических сетях с точки зрения качества оцениваются коэффициентом битовых ошибок (BER, bit error rate). В каналах оптических сетей для цифровой передачи показатели OSNR и BER имеют прямую взаимосвязь, т.е. первично величина OSNR определяется допустимой величиной BER.

Любой вид информационных сигналов в современном обществе во многих случаях нуждается не только в высоком качестве передачи от источника к получателю, но и в защите от несанкционированного доступа сторонних лиц и организаций. Для защиты информации, транспортируемой в оптических сетях, применяются различные средства и технологии засекречивания и ограничения доступа. К технологиям засекречивания относятся криптографические решения и решения по квантовым коммуникациям. Среди средств защиты оптических соединений чаще всего применяются технические решения на основе оптической рефлектометрии, зашумление линий связи, предискажения сигналов и др.

Всё выше перечисленное является предметом изучения в дисциплине, т.е. средства защиты оптических сетей, криптографические решения и квантовые коммуникации.

1.2. Квантовые коммуникации

Что представляют собой квантовые коммуникации?

Общее определение квантовым коммуникациям приводится в Национальном стандарте РФ ГОСТ Р 58568-2019 "ОПТИКА И ФОТОНИКА. ФОТОНИКА. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ" в разделе, посвящённом оптической связи.

Оптическая связь: способ передачи информации, использующий в качестве носителя информационного сигнала электромагнитное излучение оптического диапазона.

Квантовые коммуникации: раздел оптической связи, связанный с изучением и практическим применением методов передачи информации фотонами, находящимися в неклассических (квантовых) состояниях.

Национальный стандарт ПНСТ 829—2023 «Квантовые коммуникации. Общие положения и терминология» установит единые требования к архитектуре квантовой сети и терминологии, а также типовые примеры применения данных технологий. Введён в действие с 1.09.2023. Определение квантовых коммуникаций по стандарту ПНСТ 829—2023:

Квантовые коммуникации — это передача информации посредством прямой передачи квантовых состояний или посредством квантовой запутанности. Основным носителем информации в квантовых коммуникациях являются квантовые системы, состояния которых кодируются (изменяются) в соответствии с передаваемой информацией. Сигнал, описываемый квантовым состоянием, является квантовым сигналом.

Связанное с этим определением ещё одно понятие в стандартизации:

квантовая криптография (рис.1.1): система защиты передаваемой по сети оптической связи информации, в которой используются квантовые свойства частиц, находящихся в неклассических состояниях.



Рис.1.1. Квантовая криптография и квантовые технологии

Оптическая пакетная коммутация: Технология оптической передачи информации путем деления ее на части небольшого размера (так называемые пакеты), которые передаются в сети независимо друг от друга и содержат заголовки, в соответствии с которыми расположенные в узлах сети коммутаторы перенаправляют пакеты либо на клиентское оборудование, либо на другой промежуточный узел.

Квантово-оптические системы: функциональные системы, в которых используются квантовые свойства света.

Оптико-электронные системы: системы, в которых информация об исследуемом или наблюдаемом объекте переносится оптическим излучением или содержится в оптическом сигнале, а ее первичная обработка сопровождается преобразованием энергии излучения в электрическую энергию.

Квантовая сеть – это коммуникационная сеть, которая предназначена для предохранения передаваемой информации посредством применения основополагающих законов квантовой механики.

Квантовая сеть будет выполнена на основе систем квантовой криптографии, предназначенных для использования в ВОЛС, к которым предъявляются следующие требования:

- высокая скорость рассылки ключей;
- функционирование в стандартных волокнах;
- устойчивость к внешним условиям на канал связи, соответствующим нормальному режиму эксплуатации волоконно-оптических линий;
- стабильность оптических схем внутри блоков отправителя и получателя;
- возможность синхронизации приёмного и передающего устройств оптическими методами.

Итог: квантовые коммуникации часть направления развития фотонных технологий или квантовых технологий (рис.1.2). Квантовая технология – область физики, в которой используются специфические особенности квантовой механики. Предмет внимания дисциплины «Оптические сети и квантовые коммуникации» в общем обзоре квантовых технологий – только квантовые коммуникации для проводных оптических сетей.

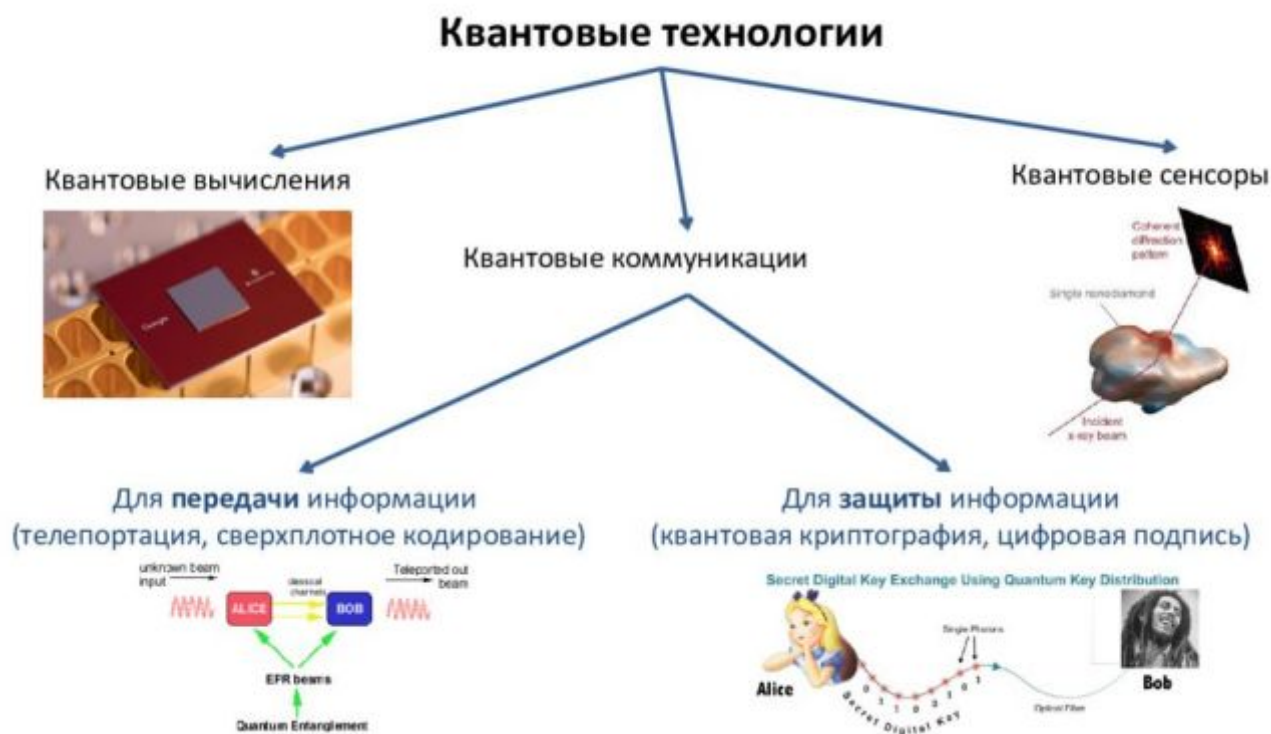


Рис.1.2. Квантовые технологии по направлениям развития

Всего предусмотрено три варианта реализации квантовой коммуникации:

по оптоволоконному кабелю — серверы связаны по уже существующим каналам коммуникации; по открытому пространству — по оборудованию и сетям сотовых операторов; через спутниковую связь — обмен квантовым ключом шифрования с наземной станцией и орбитальным спутником.

Направления развития квантовых коммуникаций в России до 2025 года

НАПРАВЛЕНИЕ РАЗВИТИЯ	СОСТОЯНИЕ НА 2019 ГОД 2-3 технические характеристики	ЦЕЛЕВОЙ РЕЗУЛЬТАТ НА 2024 ГОД 2-3 технические характеристики	ПРОГНОЗИРУЕМЫЕ БЮДЖЕТНЫЕ РАСХОДЫ Млрд. рублей	ПРОГНОЗИРУЕМЫЕ ВНЕБЮДЖЕТНЫЕ РАСХОДЫ Млрд. рублей	ПОТЕНЦИАЛЬНЫЕ УЧАСТНИКИ РЕАЛИЗАЦИИ ДК
1. Квантовые вычисления	1. 2-кубитный процессор 2. 10-кубитный симулятор 3. Научный задел по квантовым алгоритмам	1. 30–50-кубитный компьютер 2. 100-1000-кубитный симулятор 3. Разработано 5-10 квантовых алгоритмов. 4. Создана платформа с 10 000 запусками в год для решения задач	12,8	2,4	ЦКТ МГУ, МИСиС, ИФТТ РАН, ВНИИА им. Н.Л. Духова, РКЦ, МФТИ, Сколтех, Сбербанк, ГПБ, РЖД, Сибур, ГПН, Аэрофлот, Минауки, Минкомсвязи, Росатом и др.
2. Квантовые коммуникации	1. Решение точка-точка для оптоволоконных линий до 100 км и скоростями до 10 кбит/сек 2. Лабораторные демонстрации для открытого пространства на десятки метров 3. Прототипы сетей до 4х узлов	1. Продуктовые решения точка-точка на расстояния более 200 км и скоростью 1-10 Мбит/с на 25 км 2. Междугородние квантовые сети и развитые городские сети общей протяженностью более 10 000 км 3. Решения точка-многоточка - более 128 пользователей	7,8	3,4	ЦК НТИ «Квантовые коммуникации» МИСиС, РКЦ, ЦКТ МГУ, ИТМО, ККЦ, МПГУ, ФСБ, Министерство Обороны, ФСТЭК, КурЭйт, Инфотекс, ГПБ, Сбербанк, Ростелеком, С-Терра, Т8, Код безопасности, Квант телеком, Росатом и др.

Цель дисциплины состоит в формировании знаний для обеспечения информационной безопасности оптических телекоммуникационных систем и сетей посредством различных технических приложений, криптозащиты и внедрения квантовых технологий (коммуникаций) в различные сети связи.

Одной из проблем «классической» сферы информационной безопасности является неумение многих профессионалов разговаривать на понятном языке с пользователями и потребителями услуг защиты информации. Вместо такого, понятного, языка — англицизмы вкупе с «птичьим языком», где пара терминов может содержать смыслы, объяснение которых обычным языком требует целой страницы или очень точной яркой аналогии. Изучите внимательно предлагаемый далее терминологический словарь полностью или частично устоявшихся понятий, названий, определений.

1.3. Терминология для оптических сетей и квантовых коммуникаций

А

Аутентификация — определение субъекта передачи информации по принципу «свой — чужой». Классическая аутентификация с открытым ключом подвержена атакам с квантовым компьютером. Квантовые ключи обеспечивают защиту от атак с любой вычислительной мощностью. Реальное знание пароля и есть аутентификация, основная задача которой — убедить собеседника в собственной личности.

Б

Блокчейн (англ. *blockchain*, изначально *block chain* — цепь из блоков) — выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную хеш-сумму и хеш-сумму предыдущего блока. Изменение любой информации в блоке изменит его хеш-сумму.

Блокчейн, квантово-защищенный — непрерывная цепочка блоков информации, использующая квантовую или постквантовую криптографию (или комбинирующая их). Такой вид блокчейна позволяет сделать подписи и консенсус устойчивыми к взлому со стороны квантового компьютера. Первыми в мире

квантово-защищенный блокчейн разработали ученые из Российского квантового центра и QRate.

Блочный шифр — разновидность симметричного шифра, оперирующего группами бит фиксированной длины — блоками, характерный размер которых меняется в пределах 64–256 бит. Если исходный текст (или его остаток) меньше размера блока, перед шифрованием его дополняют. Фактически, блочный шифр представляет собой подстановку на алфавите блоков, которая, как следствие, может быть моно- или полиалфавитной. Блочный шифр является важной компонентой многих криптографических протоколов и широко используется для защиты... Блочный шифр «**Кузнечик**» (входит в стандарт ГОСТ Р 34.12-2015) — симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 256 бит и использующий для генерации раундовых ключей сеть Фейстеля.

В

Волоконно-оптическая линия связи — это вид системы передачи данных, при которой информация передается по оптическому волокну. Оптоволоконная связь имеет ряд преимуществ по сравнению с другими способами передачи информации: она позволяет передавать данные на большие расстояния без использования усилителей, а скорость передачи настолько высока, что остается недостижимой для других систем связи. Широко используется в телекоммуникационных сетях разных уровней, а также в промышленности, энергетике, медицине, системах безопасности и других областях.

Г

Генератор случайных чисел, квантовый — один из основных компонентов системы квантового распределения ключей, который используется для формирования криптографического ключа. В отличие от математического и аппаратного генераторов случайных чисел, квантовый — истинно случаен, а значит, устойчив к атакам квантового компьютера. Помимо квантового распределения ключей, квантовый генератор случайных чисел может использоваться в инженерных расчетах и финансовом моделировании (метод Монте-Карло), азартных играх, а также для ускорения машинного обучения.

Методы Монте-Карло — группа численных методов для изучения случайных процессов. Процесс в этом методе описывается математической моделью с использованием генератора случайных величин, модель многократно обчисляется, а на основе полученных данных вычисляются вероятностные характеристики рассматриваемого процесса.

Д

Дорожная карта по квантовым коммуникациям — документ, утвержденный Правительственной комиссией по цифровому развитию РФ в сентябре 2020 года, он описывает поэтапное развитие квантовых коммуникаций в стране до 2024 года. В рамках дорожной карты планируется создание интернета вещей на базе квантовых вычислений и *внедрение магистральных квантовых*

сетей для безопасной передачи данных. Технология предполагает квантовое распределение ключей шифрования при передаче данных по волоконно-оптической связи. Одним из первых пилотных проектов стало строительство магистральной квантовой сети «Москва — Санкт-Петербург» протяженностью около 800 км. За реализацию дорожной карты отвечает ОАО «РЖД» совместно с ведущими экспертами и научными организациями.

Декогерентность. Воздействие внешней среды разрушает кванты (эффект носит название декогерентности). Этот эффект также является причиной сложности длительного удержания «запутанного» состояния квантовых частиц.

Е

Е91 — протокол квантового распределения ключей с помощью квантовой запутанности. Был предложен Артуром Экертом в 1991 году. Играл большое значение при доказательстве секретности квантовых коммуникаций. Прототип системы квантовой криптографии на основе этого протокола был сделан в Сингапурском центре квантовых технологий CQT.

Ж

Жиль Брассар — канадский физик-теоретик, который в 1984 году совместно с Чарльзом Х. Беннеттом разработал первый в мире протокол квантового распределения ключей, названный в их честь, Bennett-Brassard 1984 (BB84). Помимо этого, Жиль Брассар — автор большого количества работ по квантовой телепортации, квантовой запутанности и квантовой криптографии. Сейчас только этот протокол в модификации Decoy-state BB84 имеет полное доказательство от наиболее общих атак, не только индивидуальных, но и коллективных.

З

Закрытый ключ — сохраняемый в тайне компонент ключевой пары, применяющейся в асимметричных шифрах, то есть таких шифрах, в которых для прямого и обратного преобразований используются разные ключи. В отличие от закрытого ключа, другой компонент ключевой пары — открытый ключ, как правило, не хранится в тайне, а защищается от подделки и публикуется.

«Звезда» — топология сети квантового распределения ключей, берет истоки в сфере больших электронно-вычислительных машин, где головной компьютер, выполняющий функции сервера, получает и обрабатывает всю информацию с периферийных устройств. По сравнению с другими топологиями, «Звезда» является наиболее дешевой во внедрении. Однако есть и недостатки, например, нарушение связи при выходе из строя сервера.

Топология «Звезда».

Задачи проектов квантовых сетей:

— разработка систем квантовой криптографии, предназначенных для использования в сетевом режиме в линиях связи телекоммуникационного стандарта;

— разработка протоколов сетевого взаимодействия систем квантовой криптографии для сетей различной топологии с динамической маршрутизацией;

—разработка и программная реализация методов и алгоритмов динамической маршрутизации (коммутации) в многоузловых (многоканальных) квантовых сетях;

—исследование, обоснование и выбор методов обеспечения качества сетевого обслуживания абонентов квантово-криптографических сетей;

—разработка лабораторного прототипа устройства динамического управления маршрутами в квантовой сети;

—создание экспериментального макета квантовой сети с динамической маршрутизацией;

—разработка методов передачи оптической квантовой информации в воздушном пространстве на дальние расстояния;

—разработка подходящей технологии реализации оптической квантовой памяти для квантового повторителя, работающего на нескольких несущих частотах;

—построение элемента квантовой сети, основанного на использовании многочастотных квантовых повторителей;

—экспериментальная демонстрация эффективной интеграции квантовой памяти и вычислителей различных пользователей в единую квантовую сеть.

И

Интернет, квантовый — сеть, соединяющая квантовые компьютеры и другие устройства, использующие квантовые технологии. В отличие от традиционного интернета, квантовый использует данные, закодированные в кубитах. Они же способны удерживать два состояния одновременно, за счет чего достигается максимальная защита пользовательской информации.

Индустрии, в которых квантовые коммуникации будут применимы в ближайшее время

- **Финансы.** Банки — первые адепты новых технологий.
- **Госсектор.** Здесь коммуникации связаны с данными пользователей, государственными системами, выборами, то есть всеми сферами, в которых важен высокий уровень защиты.
- **Телекоммуникации.** Сервисы удаленного хранения информации (им также важна хорошая защита). Данные для хранения могут быть зашифрованы квантовым способом.
- **Медицина.** В мире собирают все больше генетических данных, которые определяют всю жизнь человека и ее особенности. В ряде стран уже идет процесс по наделению юридической силой части генетических данных человека, приравнивая их к паспортным данным. Их также важно защищать от атак и манипуляций.
- **Энергетика.** Важно защищать управление крупной инфраструктурой, системы автоматизации, передачи энергии. Уже сейчас во многих точках таких систем используется криптография.
- **Транспорт.** Железнодорожный, авиационный, морской, трубопроводный, автомобильный, речной.

Имитовставка (MAC, англ. message authentication code — код аутентификации сообщения) — средство обеспечения имитозащиты в протоколах аутентификации сообщений с доверяющими друг другу участниками — специальный набор символов, который добавляется к сообщению и предназначен для обеспечения его целостности и аутентификации источника данных.

К

Квантовый бит (q-бит) (кубит) — основной объект, ответственный за передачу данных. По физическим характеристикам он представляет собой поляризованный фотон, состояние которого невозможно прочитать дважды. После того, как он переместился по каналу оптической связи, его состояние меняется, и повторная попытка прочтения выдаст совсем другой результат.

Квантовая запутанность (quantum entanglement) — свойство микрочастиц находиться в особом состоянии, в котором они образуют связанные пары: изменение характеристик одной частицы при этом мгновенно приводит к изменению характеристик другой. Измерение состояния одной из частиц поэтому автоматически позволяет узнать о состоянии другой. Частицы при этом не обязательно находятся близко друг к другу — как соседние атомы в кристалле или атомы в молекуле. Расстояние между ними квантовая механика (в теории) не ограничивает. Запутанность — одна из самых странных на сегодня и неинтуитивных характеристик квантовых систем. Запутанные частицы ведут себя как одно целое; что ещё более странно, изменения в их состояниях могут передаваться мгновенно.

Квантовый блокчейн - большое внимание последние годы уделялось технологии блокчейнов — технологий для управления распределенными базами данных. Блокчейны используют два важных криптографических инструмента. Во-первых, электронные подписи для подтверждения авторства транзакций, которые мы хотим направить в блоки. Во-вторых, разнообразные методы достижения консенсуса. Например, один из методов — доказательство работы (на англ. proof-of-work — «Хайтек») — базируется на криптографических хэш-функциях.

Квантовая сеть — это коммуникационная сеть, которая предназначена для предохранения передаваемой информации посредством применения основополагающих законов квантовой механики. Квантовая сеть будет выполнена на основе систем квантовой криптографии, предназначенных для использования в ВОЛС, к которым предъявляются следующие требования:

- высокая скорость рассылки ключей;
- функционирование в стандартных волокнах;
- устойчивость к внешним условиям на канал связи, соответствующим нормальному режиму эксплуатации ВОЛС;
- стабильность оптических схем внутри блоков отправителя и получателя;
- возможность синхронизации приёмного и передающего устройств оптическими методами.

Коммуникация — набор технологий для передачи информации.

В **квантовых коммуникациях**, в отличие от традиционных, в качестве носителя выступают не обычные световые импульсы достаточно большой мощности, а квантовые сигналы, то есть те, которые обладают существенной квантовой природой. Методы квантовых коммуникаций (квантовой криптографии) позволяют безопасно распределять криптографические ключи между клиентами по незащищённой волоконно-оптической сети или атмосферной линии связи. При этом попытка перехватить ключ может гарантированно обнаруживаться.

Квантовая коммуникационная сеть (далее — **квантовая сеть**) — технологическая система, включающая средства и линии связи, предназначенные для передачи квантовой информации. Квантовая сеть образована из узлов, которые могут передавать, принимать или распределять квантовую информацию. Узлы квантовой сети соединены между собой квантовыми каналами и классическими каналами связи для обмена служебной информацией, включая информацию о принимаемых и передаваемых квантовых сигналах, а также для синхронизации квантового оборудования.

Криптосистема — это завершённая комплексная модель, способная производить двусторонние криптопреобразования над данными произвольного объёма и подтверждать время отправки сообщения, обладающая механизмом преобразования паролей, ключей и системой транспортного кодирования.

Криптопакет — конкретная программная реализация криптосистемы.

Криптографический протокол (англ. Cryptographic protocol) — это абстрактный или конкретный протокол, включающий набор криптографических алгоритмов. В основе протокола лежит набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах.

Криптография, квантовая — метод защиты коммуникаций, основанный на принципах квантовой физики. В отличие от традиционной криптографии, использующей математические методы, здесь данные переносятся с помощью кубитов. Ее реализуют при помощи фотонов в оптоволоконных линиях или по воздушному пространству. Квантовая криптография, или, более точно, квантовое распределение ключей. Это совокупность методов, направленных на выработку между удалёнными пользователями общего секретного ключа, который в дальнейшем используется для шифрования.

Криптографическая система с открытым ключом (разновидность асимметричного шифрования, асимметричного шифра) — система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых...

Ключ — это секретная информация, используемая криптографическим алгоритмом при зашифровании/расшифровании сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности (MAC). При

использовании одного и того же алгоритма результат шифрования зависит от ключа. Для современных алгоритмов сильной криптографии утрата ключа приводит к практической невозможности расшифровать информацию.

Криптографические хеш-функции — это выделенный класс хеш-функций, который имеет определенные свойства, делающие его пригодным для использования в криптографии.

Криптографическая стойкость (или криптостойкость) — способность криптографического алгоритма противостоять криптоанализу. Стойким считается алгоритм, атака на который требует от атакующего наличия столь значительных вычислительных ресурсов или огромных затрат времени на расшифровку перехваченных сообщений, что к моменту их расшифровки защищённая информация теряет свою актуальность. В большом количестве случаев криптостойкость не может быть математически доказана; можно только доказать уязвимость...

Л

Линия квантовой связи — это совокупность методов для передачи информации в квантовых состояниях из одной точки в другую. В 2016 году в России провели первую в стране городскую линию квантовой связи протяженностью около 30 км, которая соединила два отделения «Газпромбанка» в Москве. Позже, летом 2021 года, запустилась вторая линия квантовой связи между Москвой и Санкт-Петербургом протяженностью 700 км, став самой крупной в Европе и второй по величине в мире. К 2030 году квантовые линии РЖД превысят протяженность 15 тыс. км.



М

Маршрутизация в квантовой сети. Созданные в мире экспериментальные квантовые сети характеризуются жёстко заданной маршрутизацией. В то же время, возможность управления маршрутами в квантовой сети имеет большое значение по следующим причинам:

1. При создании разветвлённых квантовых сетей с большим количеством узлов динамический мониторинг состояния линий и выбор оптимального маршрута на его основе позволит увеличить дальность и скорость рассылки ключей.

2. Эффективное управление маршрутами позволит при необходимости распределять пропускную способность квантового канала: переключаться между режимами генерации «точка-точка» и многопользовательским.

3. Устройство QKD не позволяет осуществлять рассылку по каналу, блокированному нелегитимным пользователем. В этом случае динамическая маршрутизация в сети обеспечит поддержание связи с помощью переключения на резервные линии или альтернативные маршруты.

Миниатюризация — современный тренд, заключающийся в создании устройств уменьшенного размера и массы. Она применима во всех направлениях квантовых технологий. В частности, уменьшить размер квантового компьютера позволит новая технология электронного охлаждения, которая заменит смеси криогенных жидкостей. В коммуникациях уменьшение устройства для квантового распределения ключей позволит сократить стоимость устройства в 10–15 раз.

Н

Нелокальность — возможность мгновенной корреляции (взаимосвязи) одной системы или частицы к другой со скоростью, превосходящей скорость света. На основании данного явления возможно реализовать квантовую телепортацию, когда передача двух бит информации может очень точно передать кубит, требующий для своего описания гораздо больше информации.

О

Оптический сигнал — оптическое излучение, один или несколько параметров которого изменяются в соответствии с передаваемой информацией.

Образец квантовой сети на основе механизма программно-конфигурируемых сетей (SDN) и *метода квантовой криптографии на боковых частотах модулированного излучения* (SCW QKD). Новизна включает ряд аспектов:

1. Впервые будет создан экспериментальный макет квантовой сети с динамической маршрутизацией.

2. Впервые для построения квантовой сети будут использованы системы SCW QKD, предназначенные для ВОЛС телекоммуникационного стандарта.

3. Впервые будет разработан оригинальный макет сети, демонстрирующий возможность устойчивой передачи фотонных кубитов в турбулентной атмосфере.

4. В целом по проекту будет разработан и продемонстрирован макет квантовой сети с квантовыми репитерами.

Открытый текст (англ. plain text) — в криптографии исходный текст, подлежащий шифрованию, либо получившийся в результате расшифровки. Может быть прочитан без дополнительной обработки (без расшифровки).

Отличия: кодирование, шифрование и хеширование

кодирование используется, чтобы передать сообщение и его смогли прочесть на разных устройствах;

шифрование используется, чтобы ваше сообщение не смог прочесть никто посторонний;

хеширование используется, чтобы никто не смог незаметно изменить ваше сообщение.

П

Протокол квантовых коммуникаций — свод правил, по которым осуществляется приготовление и измерение квантовых состояний света. Первый в мире протокол квантовой криптографии разработали ученые Чарльз Беннетт и Жиль Brassar в 1984 году.

Квантовый протокол BB84

Протокол Диффи — Хеллмана (англ. Diffie–Hellman, DH) — криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.

Постквантовая криптография: раздел криптографии, связанный с оценкой способности криптографических систем противостоять атакам с применением квантовых компьютеров, а также синтезом криптографических систем, устойчивых к таким атакам.

Постквантовая криптография — идея создания новых асимметричных криптографических алгоритмов, построенных не на задачах разложения чисел на простые множители, а на других сложных математических задачах, при решении которых квантовый компьютер не будет иметь преимуществ. Например, поиск коллизии хеш-функции.

Р

Распределение ключей, квантовое (QKD) — метод передачи ключа, в основе которого лежит процесс коммуникации двух сторон. Он основан на создании общего случайного ключа, который известен только двум сторонам, соединенным по открытому каналу связи. Отправитель шифрует данные, кодируя их в состояния фотонов — кубиты, и передает получателю, который, в свою очередь, декодирует полученную информацию. Квантовое распределение ключей позволяет легко обнаружить, были ли передаваемые данные скомпрометированы или имела ли место попытка взлома передаваемой информации.

Раундом (или циклом) в криптографии называют один из последовательных шагов обработки данных в алгоритме блочного шифрования. В шифрах Фейстеля (построенных в соответствии с архитектурой сети Фейстеля) и близких ему по архитектуре шифрах — один шаг шифрования, в ходе которого одна или несколько частей шифруемого блока данных подвергается модификации путём применения круговой функции.

С

Сеть Фейстеля, или конструкция Фейстеля (англ. Feistel network, Feistel cipher), — один из методов построения блочных шифров. Сеть состоит из ячеек, называемых ячейками Фейстеля. На вход каждой ячейки поступают данные и ключ. На выходе каждой ячейки получают изменённые данные и изменённый ключ. Все ячейки однотипны, и говорят, что сеть представляет собой определённую многократно повторяющуюся (интегрированную) структуру. Ключ выбирается в зависимости от алгоритма шифрования/расшифрования и меняется.

Симметричные криптосистемы (также симметричное шифрование, симметричные шифры) (англ. symmetric-key algorithm) — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в тайне обеими сторонами, осуществляться меры по защите доступа к каналу, на всем пути следования криптограммы.

Скорость генерации ключа — количество бит секретного ключа, генерируемая за одну секунду. Это основной параметр квантового распределения ключей. Скорость влияет на количество генерируемых ключей и на то, насколько эффективно ключи используются. В идеале количество бит ключа должно быть равно количеству бит сообщения — одноразовый блокнот. Но так как скорость генерации ключей — десятки бит в секунду, то используется компромиссная схема, например, один 256-битный ключ на несколько гигабайт информации. Российские системы квантового распределения ключей находятся в тройке мировых лидеров по скорости генерации ключей. На первом месте Toshiba — 300 кбит/с, на втором — QuantumCtek с 80 кбит/с и на третьем — отечественная компания QRate с 50 кбит/с. Далее идет idQuantique со скоростью 3 кбит/с.

Схема Эль-Гамала (Elgamal) — криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. Схема Эль-Гамала лежит в основе бывших стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94).

Т

Телепортация, квантовая — это передача квантового состояния на какое-либо расстояние при помощи двух составляющих: разделенной в пространстве запутанной пары и классического канала связи. Квантовое состояние разрушается в точке отправления при проведении измерения и воссоздается обратно в точке приема. При этом информация не передается быстрее скорости света, так как надо передать на сторону получателя два бита информации о результате измерения, но при этом можно передать квантовое состояние, для точного описания которого потребовался бы значительно больший объем информации. Еще одним примечательным свойством является то, что при телепортации само квантовое состояние остается неизвестным для того, кто проводит протокол телепортации.

Тест неравенства Белла – в 1964 году физик Джон Белл предложил математическую теорему, которая позволила бы проверить квантовую механику на соответствие локальному реализму. Белл предложил провести

случайное измерение двух запутанных частиц одновременно и проверить его на соответствие неравенству. Из работы Белла следовали две однозначно распознаваемые ситуации при статистических измерениях состояний запутанных частиц. Если состояния двух запутанных частиц определены в момент разделения, то должно выполняться одно неравенство Белла. Если состояния двух запутанных частиц не определены до измерения состояния одной из них, то должно выполняться другое неравенство.

У

Узлы доверенного приема-передачи. Для квантовых сетей более 100 км необходимо строить промежуточные доверенные узлы приема-передачи. В этих узлах производятся измерения фотонов, получение квантового ключа и дальнейшая его передача с помощью квантового ключа, сгенерированного на следующем пролете сети. Так как узел принимает квантовые ключи, он должен быть защищен от действий злоумышленника. Например, в Китае построена сеть «Пекин — Шанхай», содержащая 32 промежуточных доверенных узла. В перспективе возможно сделать узлы полностью квантовыми, не требующими доверия, но для этого потребуется квантовый повторитель, устройство комбинирующее квантовую телепортацию и квантовую память, чтобы сохранять успешные попытки телепортации от узла к узлу.

Ф

Фотон — это частица света, самая распространенная элементарная частица во Вселенной. Фотоны можно представить как воздушные шары, наполненных водой. Волны на поверхности воды несут информацию, а получить эту информацию можно, лишь продырявив шар, т.е. уничтожив фотон. Если на единственный фотон записать бит информации и отправить его получателю, по пути никто не сможет его незаметно прочесть — это гарантируется законами физики.

Функция формирования ключа (англ. key derivation function, KDF) — функция, формирующая один или несколько секретных ключей на основе секретного значения (главный ключ, пароль или парольная фраза) с помощью псевдослучайной функции. Функция формирования ключа может использоваться для создания ключа необходимой длины или заданного формата. Примером этого может служить преобразование секретного ключа, полученного как результат протокола Диффи — Хеллмана, в симметричный ключ для использования в алгоритме AES-256.

Х

Хранение данных, распределенное — уровень защиты информации. Если вы разделите информацию между пятью узлами, и кто-то получит доступ меньше, чем к половине, например, к двум узлам, то он не сможет ничего восстановить из вашей информации. Но если у вас будет доступ к трём узлам, то вы сможете восстановить полную информацию, даже если два других окажутся уничтожены,

например, сгорят в пожаре. Таким образом, с помощью квантовых коммуникаций можно решить задачи не только защиты передачи, но и защиты хранения.

Хеширование (иногда «хэширование», англ. **hashing**) — преобразование по детерминированному алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются хеш-функциями или функциями свёртки, а их результаты называют хешем, хеш-кодом или сверткой сообщения (англ. message digest). Если у двух строк хеш-коды разные, строки гарантированно различаются, если одинаковые — строки, вероятно, совпадают. Хеширование (англ. hashing – «превращать в фарш», «мешанина») — преобразование массива входных данных произвольной длины в (выходную) битовую строку установленной длины, выполняемое определённым алгоритмом. Функция, воплощающая алгоритм и выполняющая преобразование, называется «хеш-функцией» или «функцией свёртки». Исходные данные называются входным массивом, «ключом» или «сообщением». Результат преобразования (выходные данные) называется «хешем», «хеш-кодом», «хеш-суммой», «сводкой сообщения».

Хеш-таблица — это структура данных, реализующая интерфейс ассоциативного массива, а именно, она позволяет хранить пары (ключ, значение) и выполнять три операции: операцию добавления новой пары, операцию поиска и операцию удаления пары по ключу.

Ц

Цайлингер, Антон — австрийский физик, известный работами в области квантовой информации и впервые осуществивший квантовую телепортацию с использованием фотонов. В 2010 году Цайлингер совместно с Джоном Клаузером и Аленом Аспе стали лауреатами премии Вольфа по физике «За фундаментальный концептуальный и экспериментальный вклад в основы квантовой физики, в частности за серию возрастающих по сложности проверок неравенств Белла с использованием запутанных квантовых состояний».

Ч

Частота фотона — его спектральная характеристика. Очень важна при определении, через какую среду отправлять фотон и как его детектировать. В случае оптоволокна наилучшая частота является примерно 190 тераГерц, что соответствует длине волны в 1 550 нм. Для детектирования такого фотона используются детекторы на основе арсенида галлия. Для атмосферы обычно используют вдвое меньшую частоту, так как, помимо окна прозрачности, для этой частоты подходят более эффективные кремниевые детекторы.

Ш

Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа,

который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

Шифратор, квантово-криптографический осуществляет действия по высокоскоростному шифрованию, передаче и приему информации, а также поддерживает функцию получения квантовых ключей от системы квантового распределения ключей.

Э

Энтропия — определяет уровень хаоса, а также является мерой количества информации. В теории информации вводится также понятие взаимной энтропии между двумя участниками коммуникации, которая используется для расчета энтропии взаимосвязанных систем (энтропии совместного появления статистически зависимых сообщений). Понятие энтропии широко используется при анализе передачи данных, в том числе доказательстве секретности квантового распределения ключей.

Ю

Юстировка оптики — процесс настройки оптической схемы. Важнейший параметр любого оптического прибора, особенно квантовой криптографии, которая очень чувствительна к настройке интерферометров и/или поляризационно зависимых элементов.

Я

Яркость источника одиночных фотонов — вероятность того, что триггерный импульс, посылаемый на источник одиночных фотонов, приведет к появлению одиночного фотона. Скорость генерации одиночных фотонов можно определить как произведение яркости на частоту следования импульсов накачки.

1.4. Стандартизация оптических транспортных сетей и оптических сетей доступа с применением защиты информации

В России идет работа по созданию национальной квантовой сети. Известна информация о двух проектах, которые лягут в основу глобального построения национальной квантовой сети, составной части «Евразийского квантового пути» и должны быть реализованы до 2030 года.

Проект «Создание автодорожных телекоммуникационных сетей». Он предусматривает прокладку магистральных волоконно-оптических линий связи (ВОЛС) в обочину автомобильных дорог протяженностью приблизительно 150 тыс. км на территории 85 субъектов РФ.

Проект «Создание системы управления географически распределенными центрами обработки данных (ЦОД)». Он обеспечит контроль доступа к информационным каналам, что повысит уровень информационной безопасности и решит задачи импортозамещения.

Для реализации этих и других проектов квантовых сетей важнейшую роль играют решения по стандартизации оптических технологий для интерфейсов транспортных сетей и сетей доступа.

За основу стандартизации транспортных сетей и сетей доступа принято считать семиуровневую модель взаимодействия открытых систем Международной организации по стандартизации ISO/OSI (International Standards Organization/ Open System Interconnection) (рис.1.3), где определены функциональные уровни с подразделением на форматы реализации: физическая реализация первого и второго уровней (условно называемая уровнем «железа») и программная реализация второго-седьмого уровней и представлением данных в виде пакетов различных стандартных форматов (IP, MPLS, TP-MPLS, Ethernet, FlexEthernet и др.).



Рис.1.3. Сетевая модель ISO-OSI

Всё, что касается стандартизации транспортных оптических сетей и сетей доступа соответствует 1,2 и 3 уровням модели ISO-OSI и это отражено в стандартных решениях Международного Союза Электросвязи сектора телекоммуникаций (МСЭ-Т, ITU-T, International Telecommunications Union – Telecommunications services sector) в виде рекомендаций серий: G.xxx, K.xxx, M.xxx, X.xxx, Y.xxx и в виде стандартов Института инженеров электротехники и электроники (IEEE, Institute of Electrical and Electronics Engineers) серии IEEE802.3, Международной электротехнической комиссии IEC (International Electrotechnical Commission).

Стандартизация защиты передаваемой информации также стандартизируется с опорой на стандартные транспортные решения и распределяется по уровням

семиуровневой модели (рис. 1.4). Защита информации клиентов транспортной сети возлагается на три нижних уровня модели (Layer 1, 2, 3), где реализуется физическая передача данных L1 в виде циклических структур (блоков OTUk в оптической транспортной иерархии, кадров STM-N синхронной цифровой иерархии), пакетных данных L 2, 3 в виде кадров или пакетов фиксированной или переменной ёмкости со статистическим мультиплексированием (кадры Ethernet, MPLS, TP-MPLS, IP, FlexE). Типовые обозначения функций защиты для уровня L1 Encryption/Optical Encryption, для уровней L2,3 MACsec, IPsec.

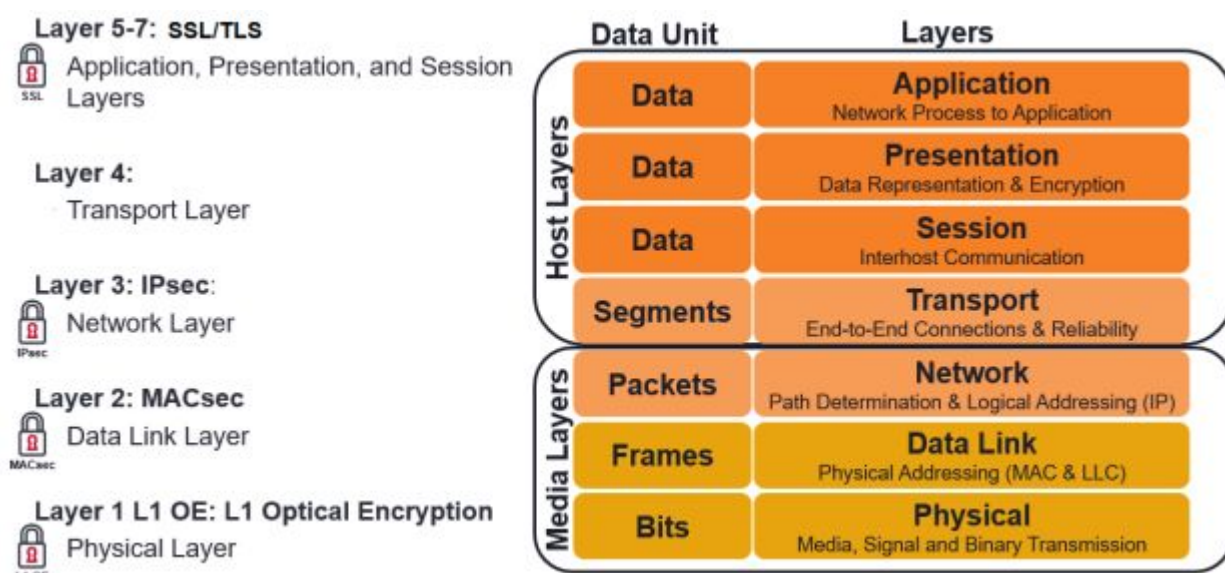


Рис.1.4. Привязка стандартов защиты информации к сетевой модели телекоммуникаций

1.4.1. Оптические транспортные сети в стандартизации защиты

Построение оптической транспортной сети на основе признанных стандартов, например, G.709, G.707, IEEE802.3, представляется технологиями DWDM/CWDM (G.694), OTN/OTN, Ethernet, SDH и предполагает протокольную и физическую совместимость (рис.1.5). В цифровом формате данных клиентов транспортной сети размещаются в циклические цифровые кадры транспортной сети (OPUk-ODUk-OTUk фиксированной ёмкости) и переносятся в оптическом канале с фиксированной или управляемой полосой частот (100 ГГц, 50 ГГц, flex 6,25×n ГГц) на подходящих оптических частотах с подходящим форматом модуляции (NRZ, QPSK, DP-QPSK и др.). Количество образуемых оптических каналов в самой популярной по использованию полосе волн оптического волокна C (1530-1565нм) зависит от канального интервала (0,8нм; 0,4нм; 0,2нм). Предметом стандартизации защиты клиентской нагрузки является поле Payload, предназначенное для транспортировки нагрузки клиента.

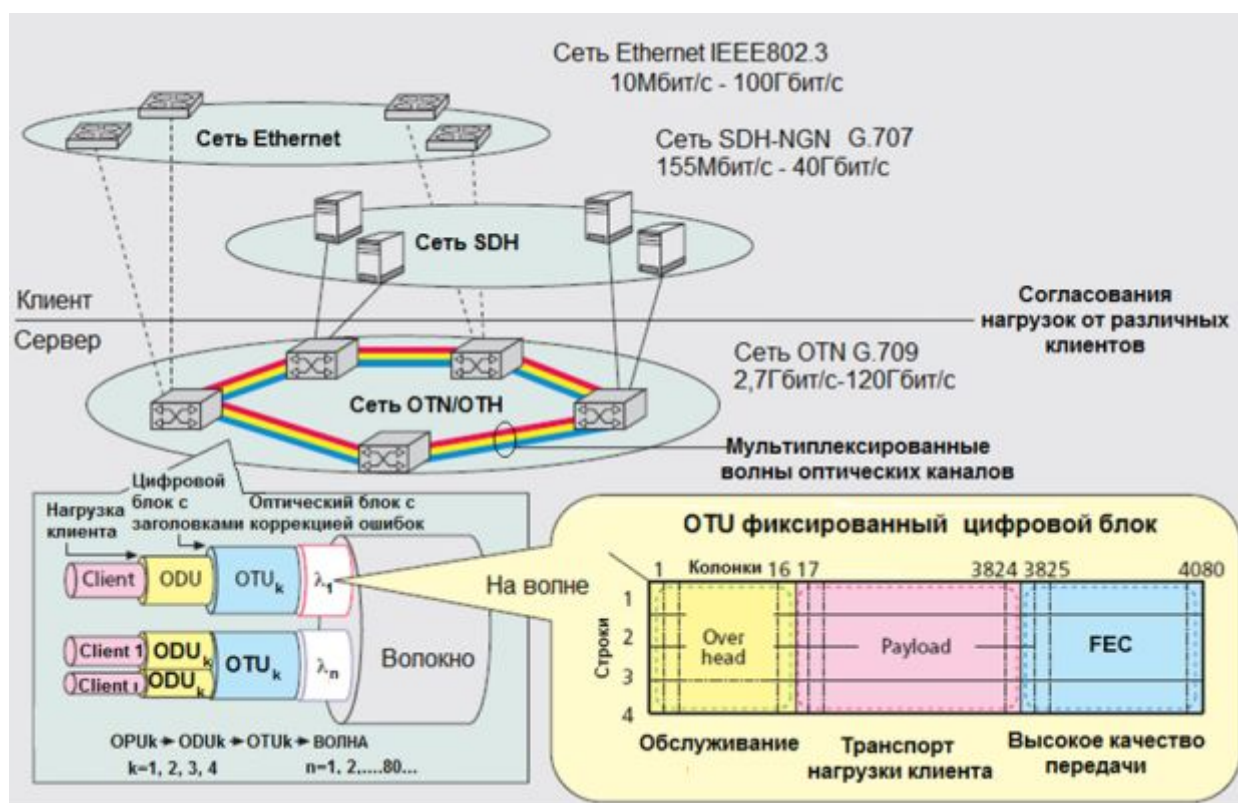


Рис.1.5. Структура оптической транспортной сети на основе оптического мультиплексирования волн

В оптической транспортной сети клиентское соединение на основе оптического канала может иметь различную протяженность с переключением в сетях одного или нескольких операторов (рис.1.6), где всегда существуют риски съёма информации.

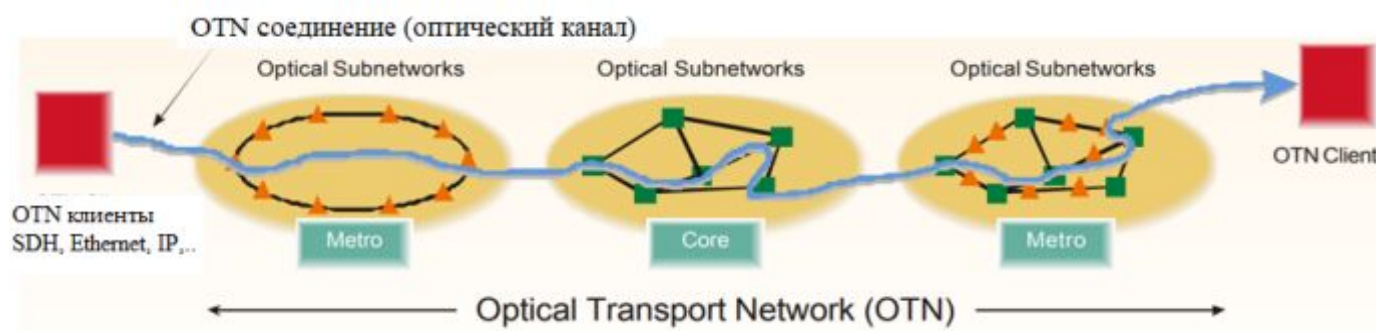


Рис.1.6. Построение оптического канала для поддержки клиентского соединения

Для защиты информации в таких сложных соединениях МСЭ-Т предложил совместимую структуру блока OTUk с шифрованием клиентской части цифровых данных (OPUk, ODUk) по рекомендации G-series Recommendations – Supplement 76 (12/2021)- Optical transport network security (рис.1.7). При этом для опознания защищённого соединения вводятся специальные метки (tag) аутентификации. Шифруемая часть цифрового блока обозначается Encryption Boundary (граница шифрования). Эта разновидность защиты клиентского трафика на физическом уровне обозначается Encryption/Optical Encryption (рис.1.4).

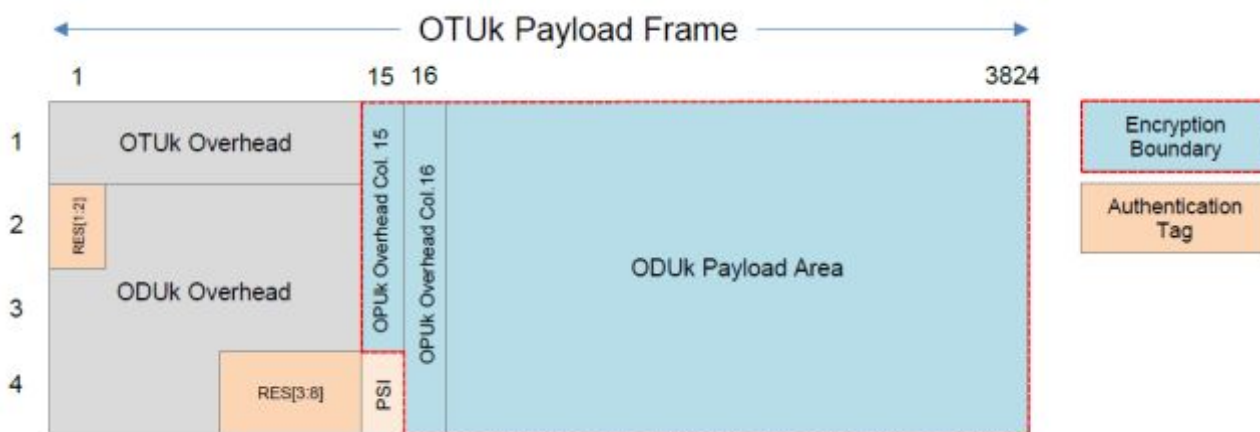


Рис.1.7. Пример структуры кадра OTUk оптической транспортной сети технологии OTN-OTN с защищённым блоком клиентской нагрузки ODUk Payload Area

Сквозная защита клиентского соединения в транспортных сетях также предусматривает возможности по перекодировке защиты на отдельных участках оптического канала (рис.1.8.). Также предусматривается сквозная защита клиентских данных (клиент-клиент) между клиентским оборудованием, подключаемому к сетям доступа. Для этого, как правило, используются протоколы IPsec и/или MACsec (рис.1.4).

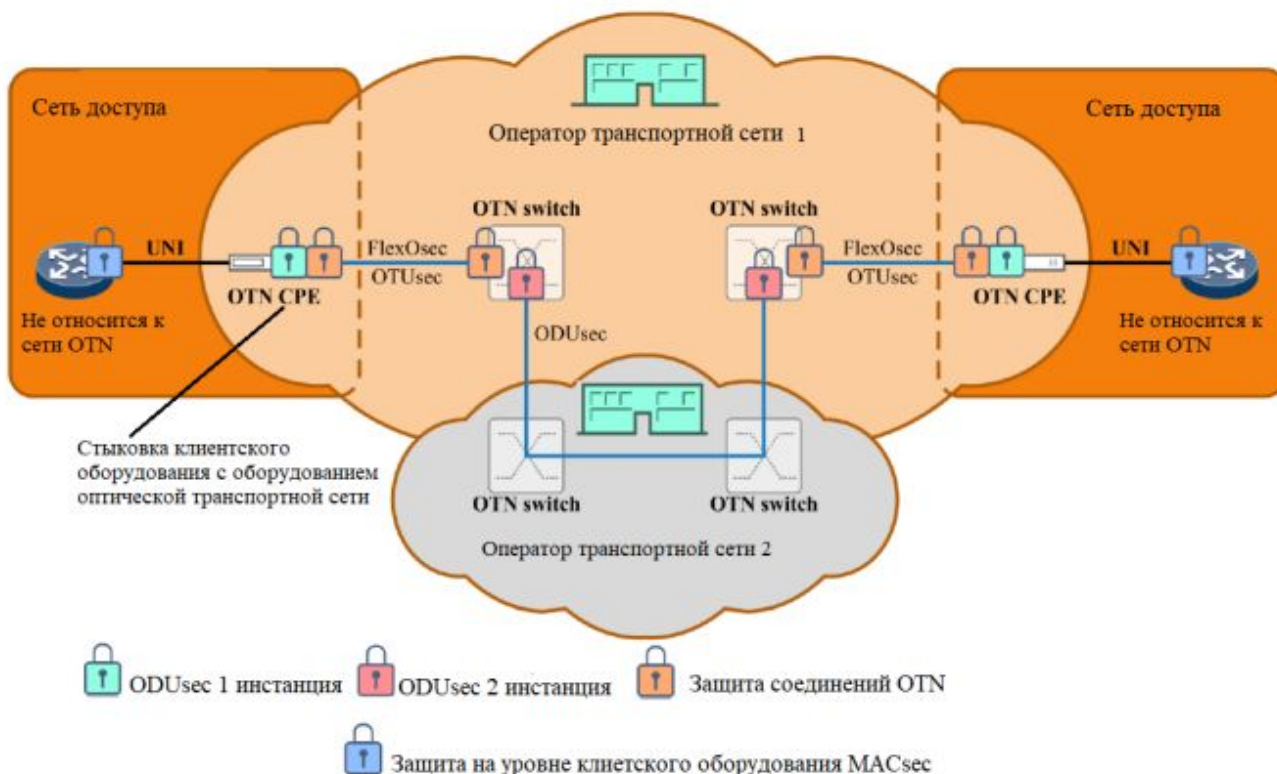


Рис.1.8. Пример стандартизированной структуры клиентского оптического канала в транспортных сетях различных операторов с изменением функций защиты

IPsec (сокращение от IP Security) представляет собой набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, что

необходимо для подтверждения подлинности передачи или аутентификации, проверку целостности и/или шифрование IP пакетов. Также IPsec включает в себя протоколы для защищённого обмена ключами в сети Интернет. Основное назначение – для организации соединений виртуальных частных сетей VPN (Virtual Private Network). IPsec представлено серией стандартов RFC (RFC2401-RFC2412, Request for Comments –запрос на изменение) , разработанных советом по архитектуре Интернета IAB (Internet Architecture Board). Протоколы IPsec могут функционировать в двух режимах: транспортном и туннельном. В транспортном шифруются (защищаются) только данные IP- пакета, а исходный заголовок сохраняется. Транспортный режим, как правило, используется для установления соединения между хостами, т.е. конечными устройствами, предоставляющими услуги типа «клиент-сервер». Он может также использоваться между шлюзами для защиты туннелей, организованных каким-нибудь другим способом, например протоколом сеансового уровня (L5) L2TP (Layer 2 Tunnelling Protocol).

Т.о., L2 TP/IPsec — это тип протокола VPN, который сочетает в себе протокол туннелирования уровня 2 (L2TP) и протокол безопасности интернет-протокола (IPsec) для создания безопасного и зашифрованного соединения между двумя устройствами через Интернет.

В туннельном режиме шифруется весь исходный IP-пакет: данные, заголовок, маршрутная информация, а затем зашифрованный пакет вставляется в поле данных нового пакета (инкапсуляция). Туннельный режим может использоваться для подключения удалённых компьютеров к виртуальной частной сети или для организации безопасной передачи данных через открытые каналы связи между шлюзами.

Протокол сеансового уровня SSL (Secure Sockets Layer, уровень защищённых сокетов, т.е. конечных точек соединения) и его наиболее современная версия TLS (Transport Layer Security) представляет собой криптографический протокол, который подразумевает более безопасную связь (рис.1.4). В протоколе предусмотрено использование асимметричной криптографии для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений. Протокол широко используется для передачи голосовых сообщений VoIP.

Протокол MACsec описывается стандартом IEEE802.1AE и служит для шифрования пакетов между двумя совместимыми устройствами (рис.1.4). Шифруется весь поток данных, скрыт отправитель и получатель, порты их приложений, а так же вся служебная информация. Здесь предусмотрена возможность шифрования с использованием ключа МКА (MACsec Key Agreement), как между коммутаторами (Switch-to-Switch), так и между коммутатором и конечными устройствами (Switch-to-Client). Это обеспечит шифрование трафика на L2 уровне при помощи алгоритма AES-128 или AES-256. Большой плюс этого решения в том, что криптография происходит на аппаратном уровне, и ресурсы процессоров сильно экономятся. Алгоритм AES (Advanced Encryption Standard) один из самых универсальных и популярных алгоритмов

шифрования с симметричным ключом в сфере криптографии. В основе AES лежит блочный шифр, который использует 128-битный размер блока и 128, 192 или 256-битные ключи для шифрования данных. AES256 - это версия стандарта с 256-битными ключами. Этот стандарт широко считается самым безопасным стандартом цифровой криптографии, который обычно используется для наиболее надежной сквозной зашифрованной связи, в том числе для высокоскоростных оптических каналов.

1.4.2. Оптические сети доступа в стандартизации защиты

Сети доступа или оптические сети доступа в ряде документов определяются как продолжение транспортной среды (сети) до терминала пользователя и их также называют «последней милей», и оптикой до клиента. Оптические сети доступа строятся на основе различных активных и пассивных технологий, обозначаемых в общем случае FTTx (рис.1.9.). Пассивные сети доступа в своей основе имеют волоконно-оптические линии и разветвители между стационарным оборудованием и терминалами пользователей. Активные оптические сети предполагают возможность использование электронного оборудования на различных участках доступа и большее количество и разнообразие трансиверов.

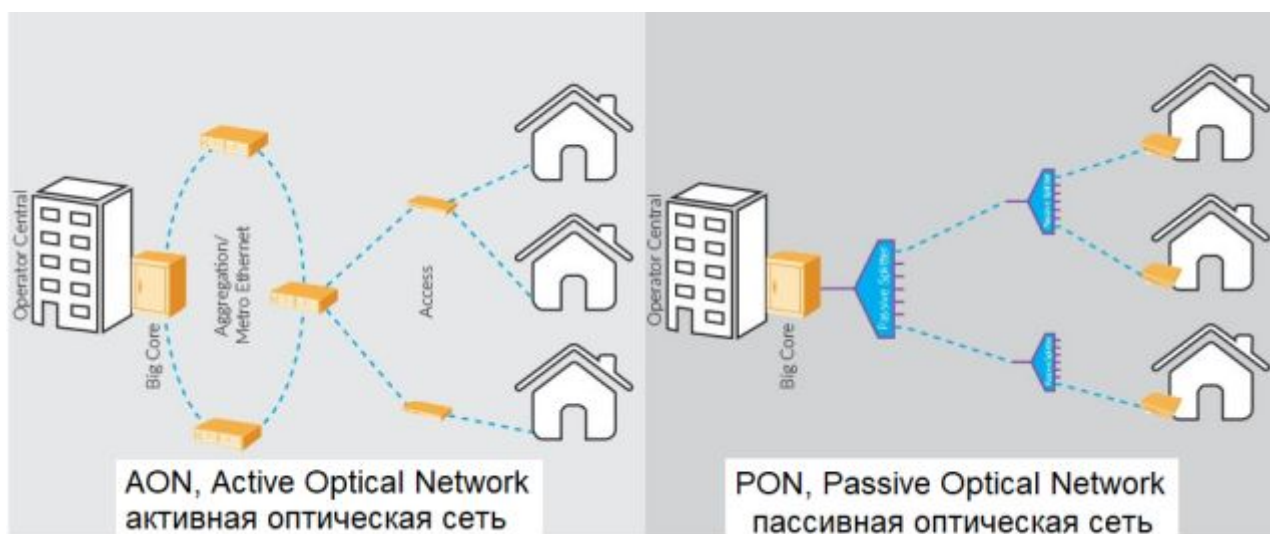


Рис.1.9. Активная и пассивная оптическая сеть доступа

Что такое FTTx?

FTTN. Волокно протянуто до сетевого узла (города, района, станции связи).

FTTC. Кабель протянут до подстанции (обычно это городской микрорайон, состоящий из нескольких десятков многоэтажных домов).

FTTB. Волокно проложено до здания: многоэтажного дома, торгового центра, предприятия, где расположен оптический сетевой терминал ONT.

FTTH. Кабель до квартиры или дома. Получается, провод напрямую подключен к роутеру ONT: создается домашняя сеть wi-fi. (Рис.1.10)

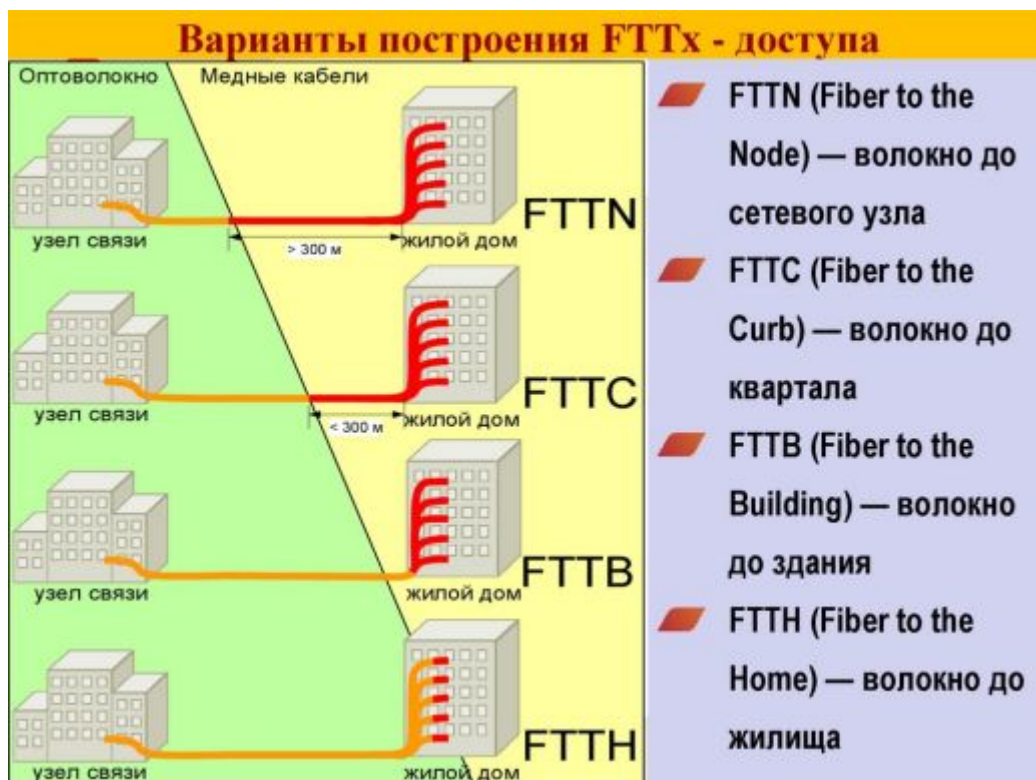


Рис.1.10. Варианты оптических сетей доступа FTTx

Варианты построения оптических сетей доступа имеют стандартизацию на уровне рекомендаций ITU-T, IEC и IEEE. В стандартах отражены физические параметры (типы волоконных световодов, характеристики интерфейсов, и т.д.) и протокольные решения второго уровня L2 для организации передачи данных на основе ATM, Ethernet, SDH, протоколы управления передачей и динамического управления скоростью или полосой частот DBA (Dynamic Bandwidth Allocation), применения спектрального мультиплексирования DWDM/CWDM и технологиями (протоколами) защиты информационных сообщений (шифрованием).

Для предоставления услуги корпоративным клиентам, оборудование доступа должно поддерживать технологии 2-го уровня QinQ, VPLS (Virtual Private LAN Service), E-Line и E-LAN в соответствии со спецификациями MEF (Metro Ethernet Forum).

Для защиты трафика оптических сетей доступа используется шифрование открытыми ключами, например, PON — это технология с общей средой передачи, то необходимо шифрование всех потоков данных на всех скоростях передачи (от 1 Гбит/с до 100 Гбит/с) (рис.1.11). В технологии GPON проводится шифрование AES с 256-разрядными ключами только нисходящего потока MACsec. Однако использование стандарта AES снижает производительность сети, т.к. при шифровании необходима передача существенного объема служебной информации вместе с каждым пакетом. Также трафик может шифроваться и IPsec. Сравнительная оценка эффективности применения различных технологий шифрования приведена на рис.1.12.

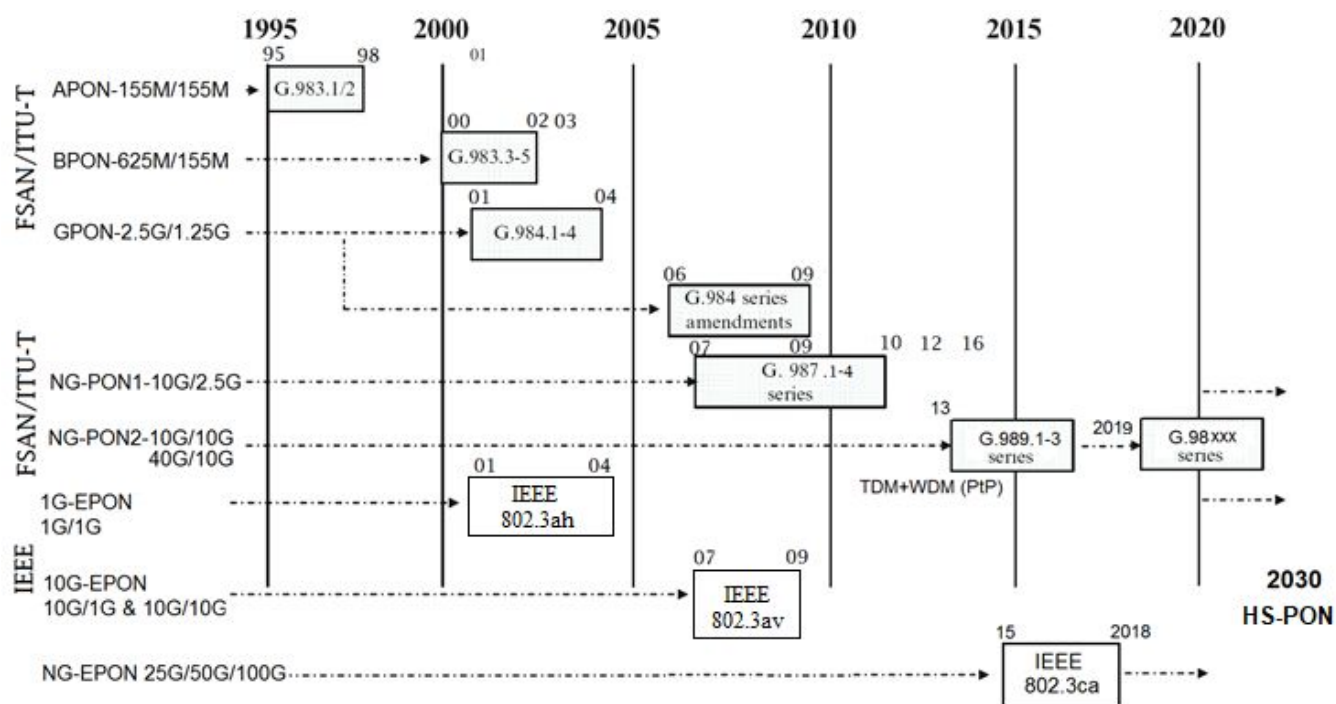


Рис.1.11. Развитие технологий пассивных оптических сетей в стандартизации

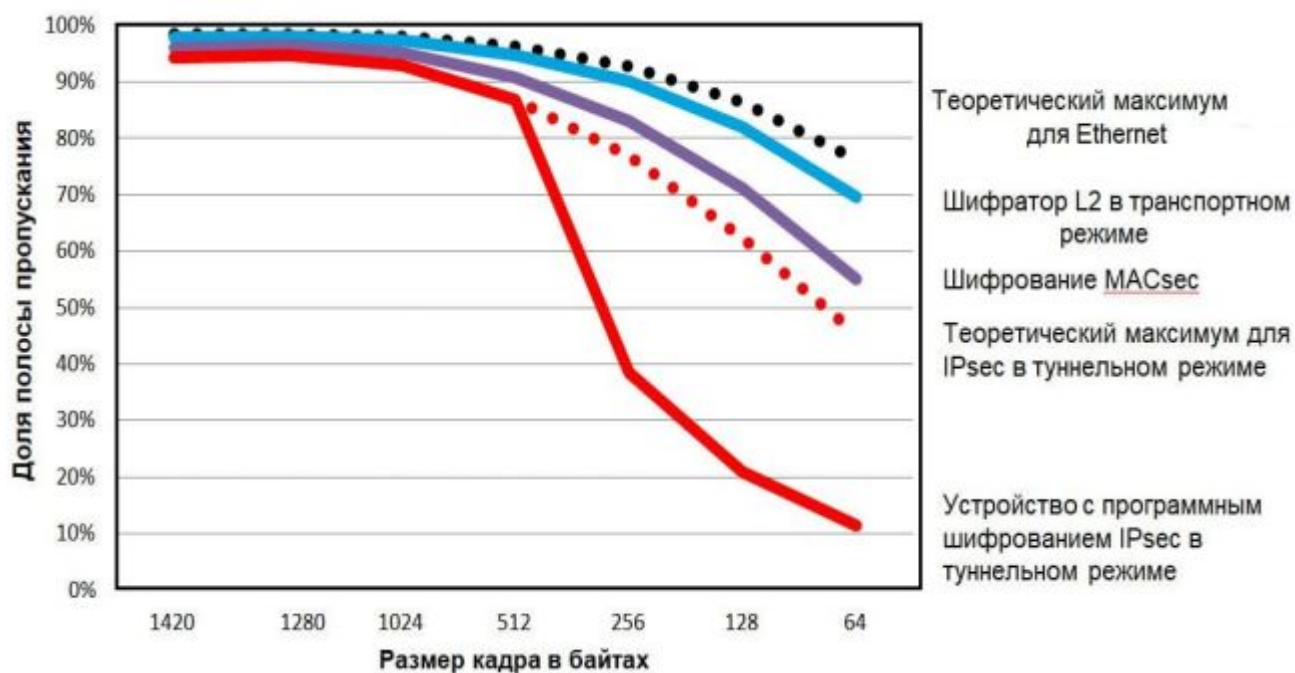


Рис.1.12. Эффективность применения шифрования в технологиях сетей доступа

1.5. Физическая защита в волоконно-оптических системах передачи и оптических сетях

1.5.1. Перехват трафика в волоконно-оптических соединениях. Основные понятия

Перехват трафика или информации - неправомерное получение информации с использованием технических средств, осуществляющего обнаружение, прием и обработку информативных сигналов, т.е. сигналов, по параметрам которых может быть определена защищаемая информация.

Оптический кабель является эффективной распределенной измерительной системой, который позволяет проводить измерение различных физических полей.

Физическая защита оптического кабеля – самый простой подход к защите конфиденциальных данных. Но такую защиту бывает сложно реализовать. Для предотвращения неправомерного использования информации законными пользователями сети, а также внешними хакерами необходимо обеспечить безопасность сетевой инфраструктуры, управляемый доступ к сети и средства контроля доступа привилегированных пользователей.

Для перехвата трафика возможен сбор специальной информации по воздействию на оптическое волокно: акустические поля; распределение температур; электромагнитные поля; радиационные излучения; другие поля.

НСД (несанкционированный доступ) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам.

НСИ (несанкционированный съём информации) или перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

ТСР (технические средства разведки) - совокупность разведывательной аппаратуры, предназначенной для обнаружения демаскирующих признаков, предварительной обработки, регистрации перехваченной информации и ее передачи через каналы передачи информации в центры сбора и обработки информации. (Подробно смотреть: <http://www.fstec.ru>)

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте.

Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Сигнал утечки информации — информативный сигнал в техническом канале утечки информации.

Модель угроз информации (техническими средствами) — формализованное описание технических каналов утечки, сведения о методах и средствах осуществления угроз информации.

Сценарий угрозы информации — последовательность действий нарушителя, направленная на получение, искажение, уничтожение конфиденциальной (защищаемой) информации с применением специальных технических средств.

Этапы перехвата информации.

Перехват информации в оптической системе передачи – сложный процесс, требующий последовательного выполнения ряда операций, которые могут быть объединены в следующие этапы:

- Поиск места перехвата информации;
- Доступ к оптическому кабелю и волокну;
- Обнаружение оптического сигнала;
- Спектральный анализ оптического сигнала;
- Структурирование зарегистрированного сигнала;
- Расшифровка структурированного сигнала.

На рис.1.13-1.17 иллюстрируются угрозы несанкционированного доступа к передаваемой информации. На рис.1.18 представлена наиболее полная классификация способов (методов) сбора или съёма оптических сигналов, которая необходима для понимания реальных угроз утечки информации.

Объект информатизации с волоконно-оптическими коммуникациями (соединениями)

A – волоконно-оптические коммуникации;

B – контролируемая зона объекта с выделенным помещением;

I – угроза трафику локальной сети

II – угроза конфиденциальной информации (переговорам)

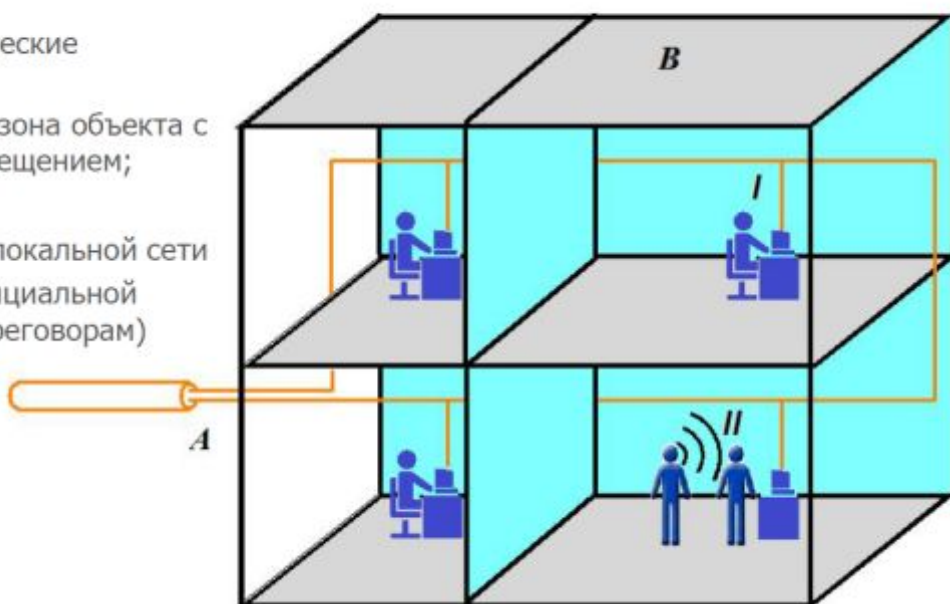
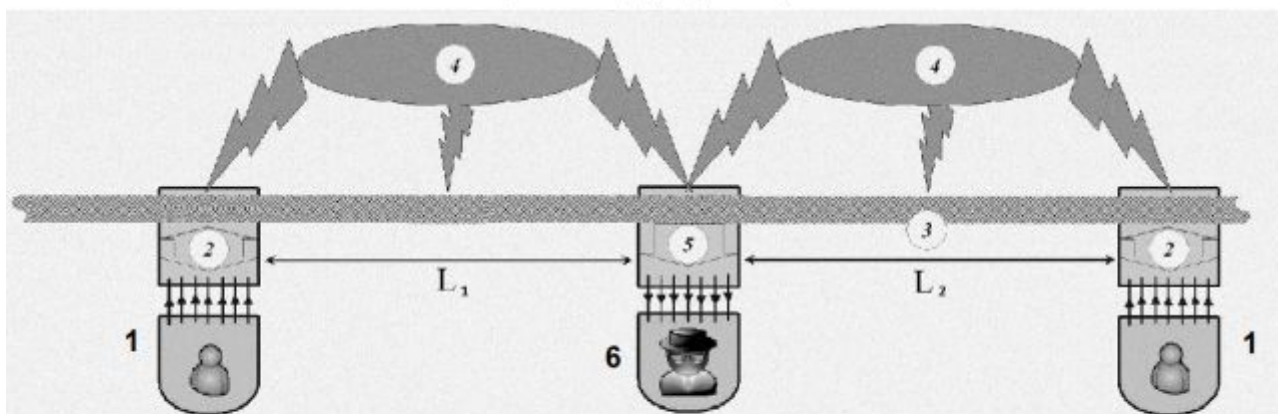


Рис.1.13. Угрозы перехвата информации в оптической сети

Выявление угроз информации. Этап выявления топологии (структуры) оптической сети и её особенностей. Определение места перехвата.

Перехват внутреннего/внешнего трафика — утечка информации, циркулирующей в компьютерной или иной оптической сети объекта информатизации, за пределы контролируемой зоны, осуществляемая внутренним нарушителем путем НСД / внешним нарушителем путем НСИ, соответственно;

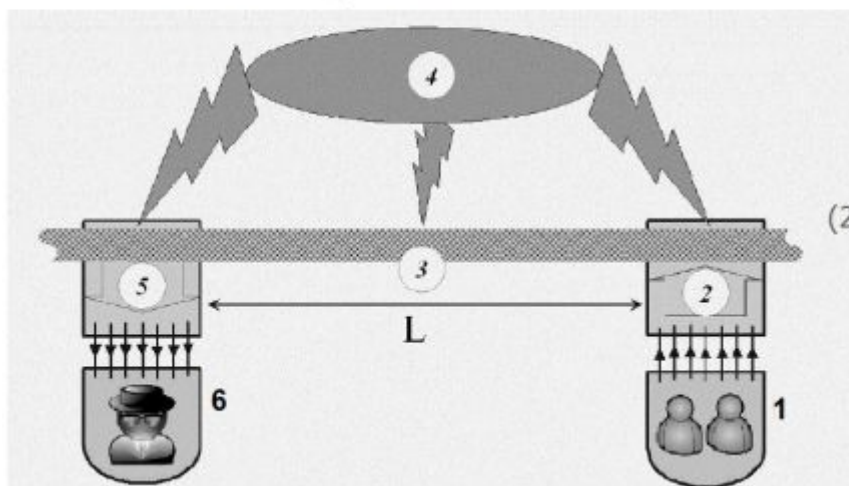
Обобщенная структура перехвата



(1) источники-абоненты, (2) штатный приемопередатчик, (3) канал связи длиной $L_1 + L_2$, (4) помехи, (5) приемник ТСП, (6) злоумышленник.

Рис.1.14. Перехват внутреннего и внешнего трафика

ТКУИ через волоконно-оптические коммуникации — утечка информации, циркулирующей на объекте информатизации, путем использования волоконно-оптических коммуникаций объекта для скрытного получения доступа к ней с помощью ТСП и использования измерительных возможностей волоконно-оптических коммуникаций.



Обобщенная структура ТКУИ:

(1) источники,
(2) нештатный преобразователь,
(3) канал утечки длиной L ,
(4) помехи, (5) приемник ТСП,
(6) злоумышленник.

Рис.1.15. Технический канал утечки

Принципиальные условные схемы перехвата трафика (I) и подслушивания конфиденциальных переговоров (II) вне контролируемой зоны (B) внешним нарушителем X, путем несанкционированного съема информации (НСИ) с волоконно-оптических коммуникаций (A) на основе технологии PON.

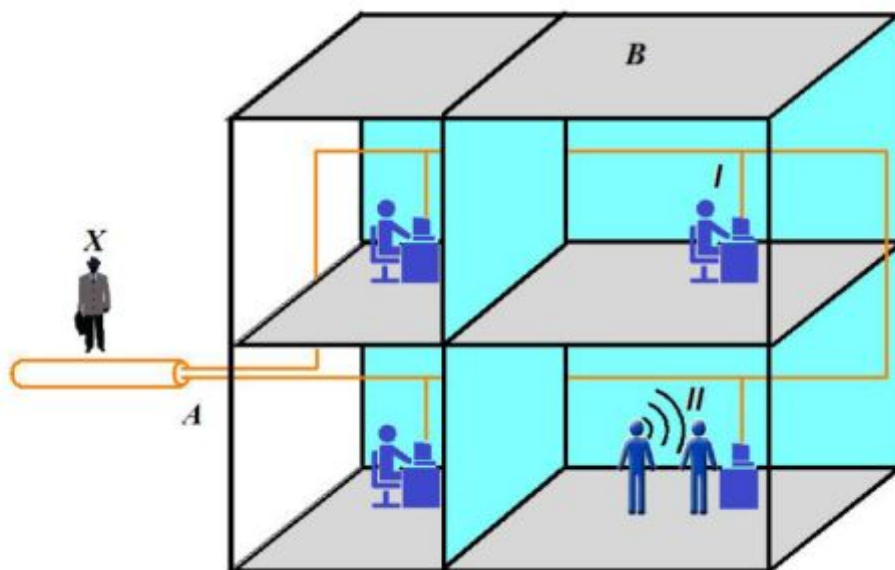


Рис.1.16. Перехват трафика в волоконно-оптических соединениях. Схема перехвата и подслушивания 1

Принципиальные условные схемы перехвата трафика (I) и подслушивания конфиденциальных переговоров (II) в контролируемой зоне (B) внутренним нарушителем X, путем несанкционированного доступа (НСД) к волоконно-оптическим коммуникациям (A) на основе технологии PON.

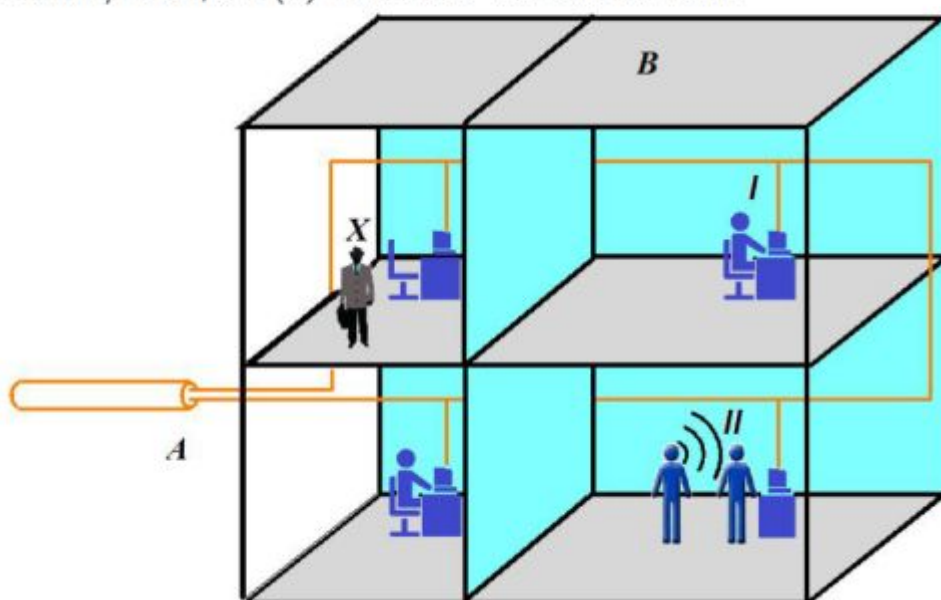


Рис.1.17. Перехват трафика в волоконно-оптических соединениях. Схема перехвата и подслушивания 2

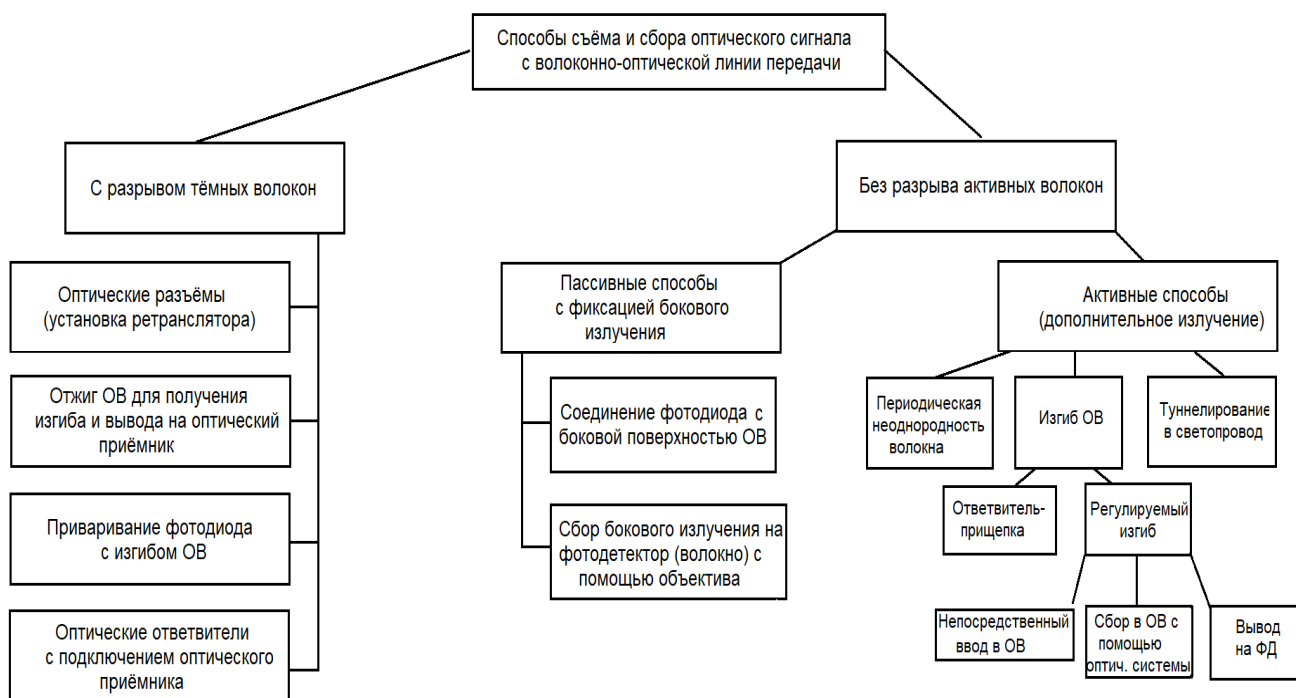


Рис.1.18. Классификация способов доступа к информации в волоконно-оптических системах и сетях

Волоконно-оптическая линия связи. Доступ к оптическому кабелю и волокну.

- Кабель внешней прокладки (между объектами информатизации):
в конструкции присутствуют металлические усиливающие и защищающие элементы;
специальный кабель может быть полностью диэлектрическим;
прокладка – подземная, подвесная и подводная;
возможно использование городских и междугородных коммуникаций;
для соединения используются соединительные муфты, регенераторы и усилители.
- Кабель внутренней прокладки (внутри объекта информатизации):
в конструкции присутствие металлических элементов не обязательно;
кабель полностью диэлектрический;
прокладка – внутри здания вертикальные колодцы и горизонтальные короба, лотки и т.д.;
прокладка – между зданиями подземные, подвесные, в коммуникационные колодцы;
для распределения абонентам используются коммутационные шкафы, боксы и т.д.

Выявление угроз информации и этап несанкционированного подключения к волоконно-оптическому каналу (волокну) иллюстрируют рис.1.19-1.22.

Сценарии перехвата трафика из волоконно-оптических коммуникаций (1) нарушителем (2)

КОНТАКТНЫЕ МЕТОДЫ:

A – контактный перехват с разрывом оптоволокна и вставкой;

B – контактный перехват с прямым доступом к волокну;

ДИСТАНЦИОННЫЕ МЕТОДЫ:

C – дистанционный перехват на основе параметрических методов;

D – дистанционный перехват с регистрацией побочных излучений.

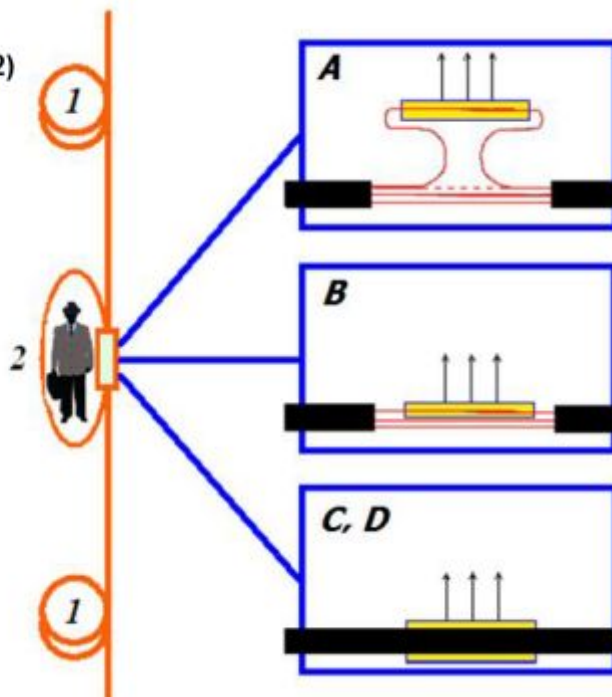


Рис.1.19. Сценарии перехвата трафика в оптической линии

Контактный способ с разрывом оптоволокна и подключением оптоволоконной вставки

Оптоволоконная вставка – устройство отвода оптического излучения из оптоволокна с минимальными возвратными и прямыми потерями, включаемое в штатную оптическую линию путем его разрыва и замыкания оптического канала через вставку.



Рис.1.20. Контактный способ с разрывом волокна

Наиболее опасные для перехвата по типу А и В участки структурированной кабельной системы:

1 – защитные оптические муфты для сварных соединений, 2,3 – коммутационно-распределительные устройства (оптические кросс-панели, стойки).

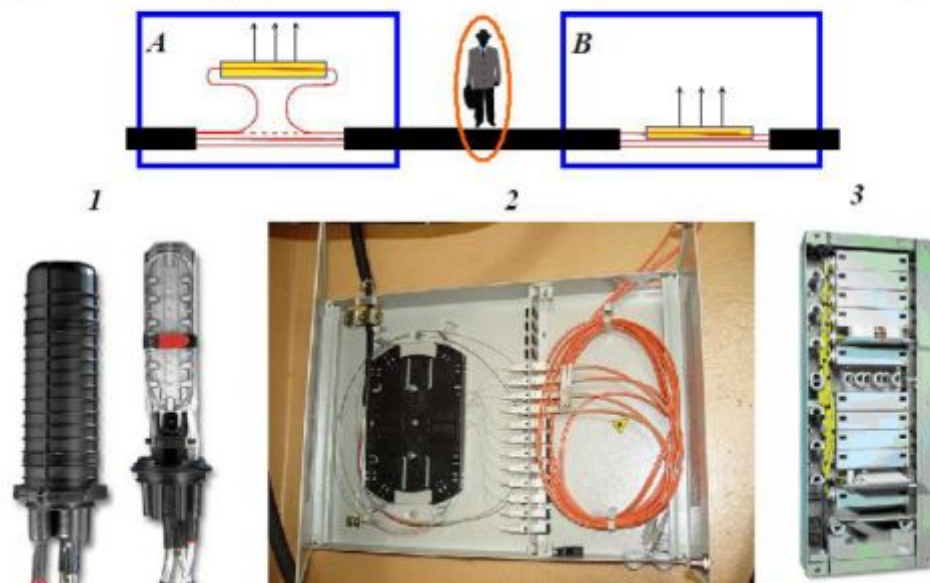


Рис.1.21. Наиболее опасные способы перехвата в волокне

Дистанционный способ съёма информации:

характерные неоднородности оптической структурированной кабельной системы, места соединения и коммутации - оптические кроссы и муфты



Места соединения с активным оборудованием, скрутка кабеля



Рис.1.22. Дистанционный способ съёма информации в различных пассивных устройствах

Сценарии перехвата трафика на основе мероприятий по повышению эффективности перехвата трафика. Для этого нужно изменение параметров оптического кабеля внешним воздействием:

изгиб, скрутка, петля, пережим кабеля;
воздействие на кабель внешнего физического поля (например, источник радиации вблизи кабеля увеличивает локальные потери, аналогично источник тепла, вода);
повреждение оболочки кабеля использование не декларируемых и не выявленных свойств оптического кабеля;
не сертифицированный на специальные свойства и воздействия кабель;
длинные скрученные «хвосты» кабеля;
другое.

Всё это может быть использовано в кабельных колодцах канализации; в подвесных муфтах на различных опорах (ЛЭП, контактная сеть ЖД и города, отдельные опоры, подводная прокладка и т.д.).

Как можно зарегистрировать утечку информации в оптической линии? Вариант представлен на рис. 1.23 для приёмного оптического модуля.

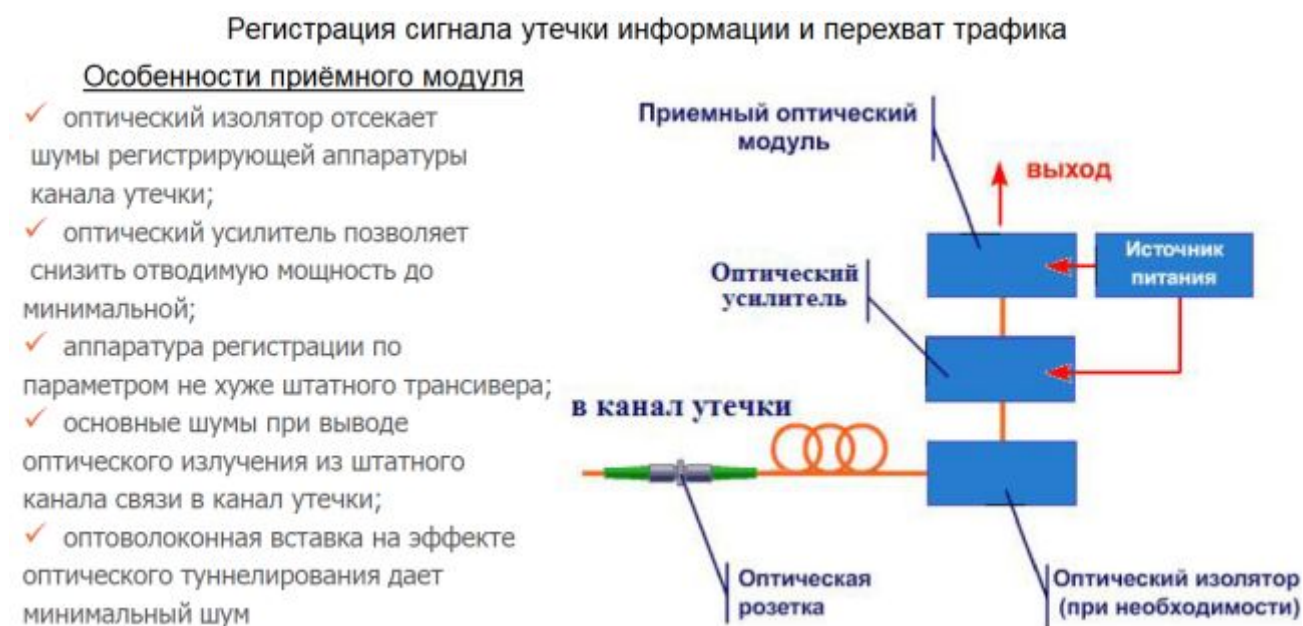


Рис.1.23. Нарушение уровня приёма оптического сигнала в модуле

Подключение в локальной сети или в помещениях может осуществляться непосредственно к оборудованию (рис.1.24). Кроме того возможен сценарий скрытой передачи трафика за пределы контролируемой зоны через СКС и PON.

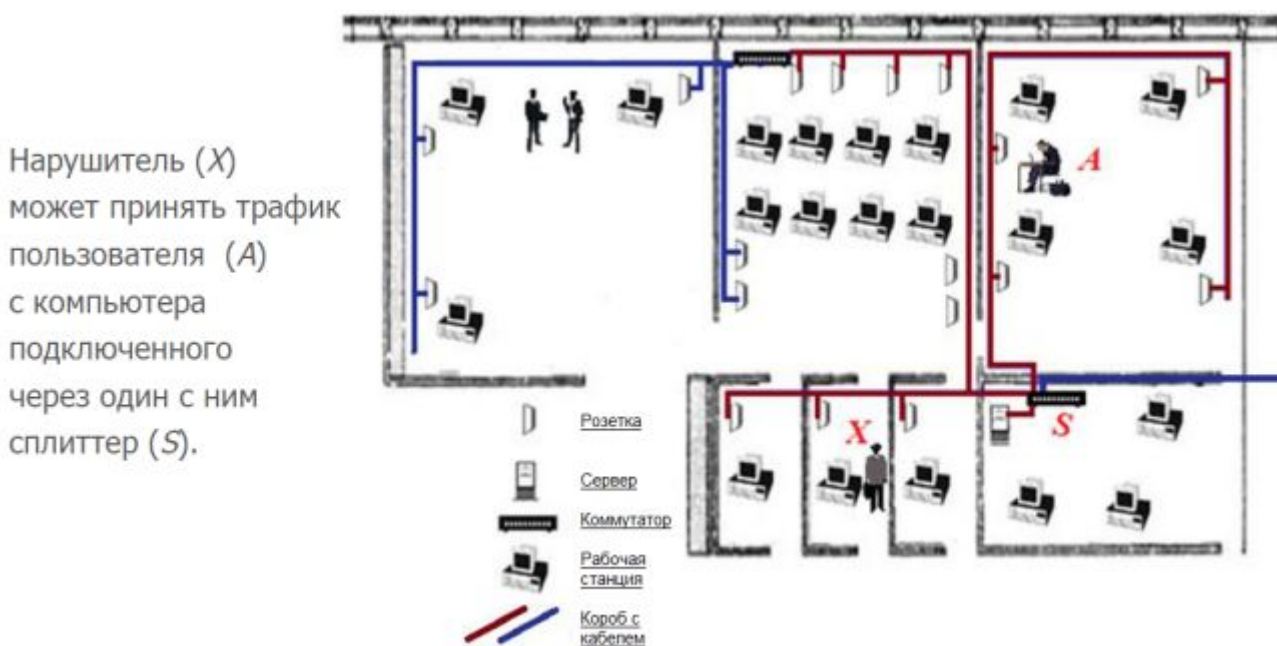


Рис.1.24. Сценарий перехвата трафика путём несанкционированного доступа к абонентским линиям СКС, PON и оборудованию

ВЫВОДЫ: волоконно-оптические телекоммуникации, локальные сети, системы передачи данных могут быть подвержены угрозе перехвата передаваемой информации; технология защиты трафика требует анализа технических возможностей поиска и подсоединения к волоконно-оптическому каналу; защита трафика зависит от технических и организационных возможностей нарушителя.

Что необходимо знать и уметь специалисту по предотвращению утечки информации?

Надо знать возможные технические средства перехвата, к которым относятся многие решения, рассматриваемые техническими средствами разведки: штатные средства монтажа, наладки и эксплуатации волоконно-оптических и систем передачи информации.

Надо знать - технические средства разведки для перехвата:

- техника поиска оптического кабеля;
- техника отвода оптического излучения;
- техника регистрации параметров проходящего по оптическому волокну излучения.

ГЛАВНАЯ ОПАСНОСТЬ пути формирования сигнала утечки информации:

- отвод части оптического излучения;
- регистрация побочных оптических излучений, сопровождающих информационный сигнал и их инициализация;
- регистрация побочных неоптических излучений, сопровождающих информационный сигнал и их инициализация;

- регистрация вызываемых информационным сигналом изменений параметров оптического волокна и их инициализация.

Отвод части оптического излучения методом нарушения полного внутреннего отражения при внешнем воздействии, т.е. изменение угла падения представлено на рис.1.25. при внешнем воздействии: радиационным излучением, электрическим и магнитным полем, нагревом и акустическим воздействием

Использование внешнего воздействия для уменьшения угла падения до величины меньшей значения φ_0 - угла полного отражения

Способы изменения угла падения

Механическое воздействие:

изгиб волокна;
кручение волокна;
растяжение волокна.

Воздействие физического поля:

акустического;
электромагнитного;
радиационного;
теплого.

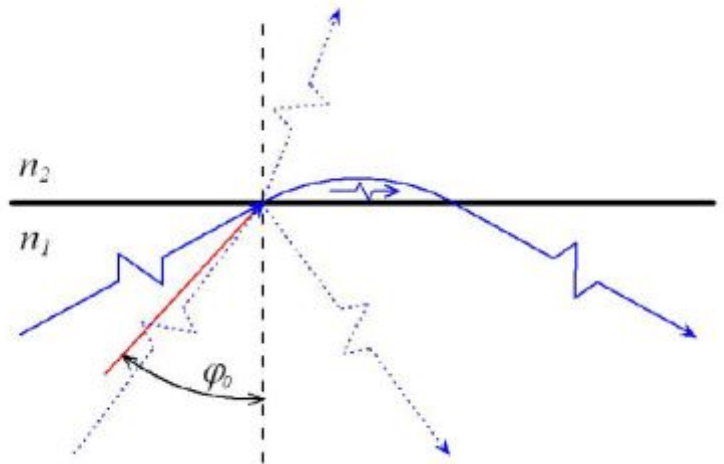


Рис.1.25. Отвод части оптического излучения нарушением полного внутреннего отражения

Наиболее простым способ отвода части оптического излучения можно считать изгиб волокна (рис.1.26).

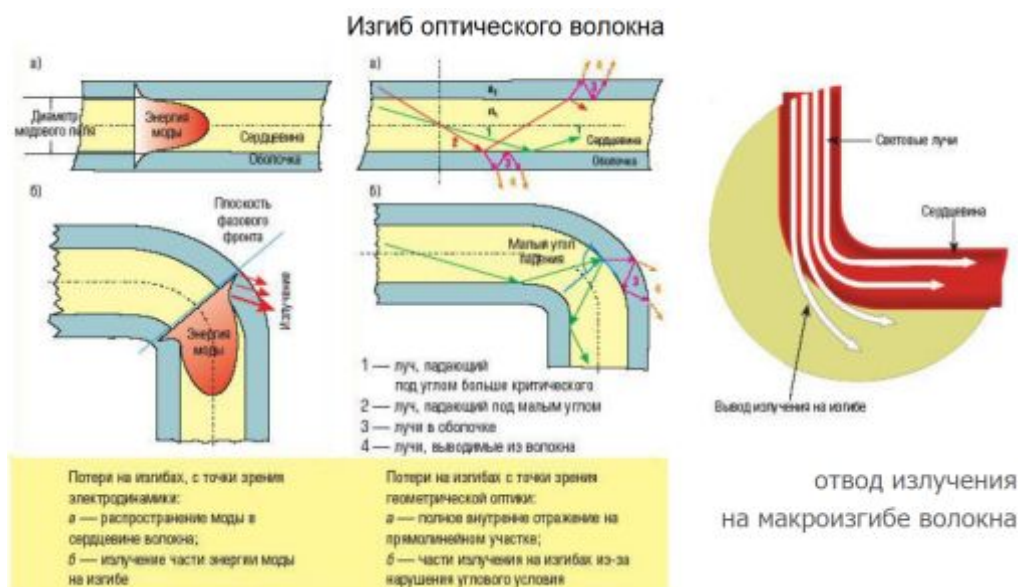


Рис.1.26. Отвод части оптического излучения изгибом волокна

Учитывая, что часть оптического излучения распространяется и в оболочке оптического волокна, возможно отведение методом туннелирования (рис.1.27).

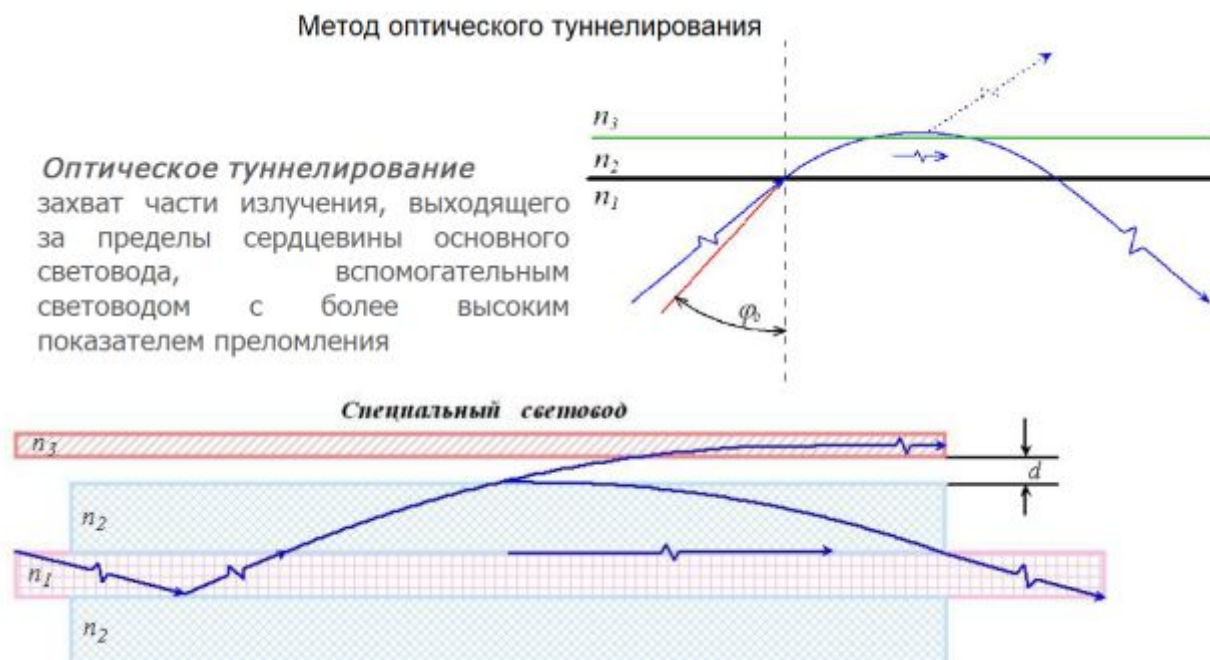


Рис.1.27. Туннелирование части излучения в накладываемое волокно

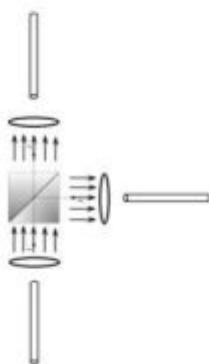
Там где возможно подключение к активному или пассивному оборудованию ВОСП возможно отводить часть оптического излучения методом деления (рис.1.28).

Метод деления оптического потока

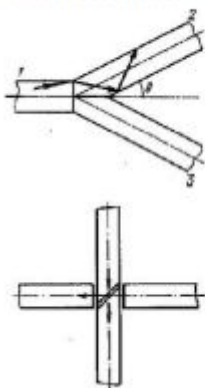
Светоделитель :

деление оптической мощности на два и более потока в требуемом соотношении микро-оптическими, волоконно-оптическими и интегрально-оптическими методами

микро-оптические



волоконные



на градах

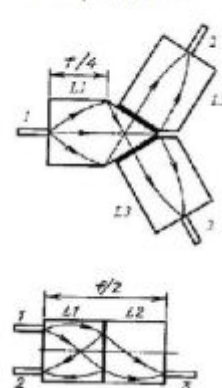
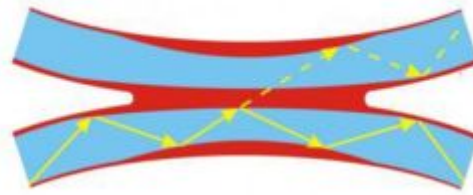


Рис.1.28. Метод деления оптического потока в различных устройствах

Таковыми устройствами могут быть сплиттеры различных конструкций (рис.1.29) для различных коэффициентов деления.

» **Сплиттеры:** выполненные по сплавной технологии Fused Biconic Tapered (FBT)

волокна скручиваются и свариваются



» **Сплиттеры:** выполненные по планарной технологии Planar Lightwave Circuit (PLC)

изготавливаются по
толсто пленочной технологии
на кремниевой подложке

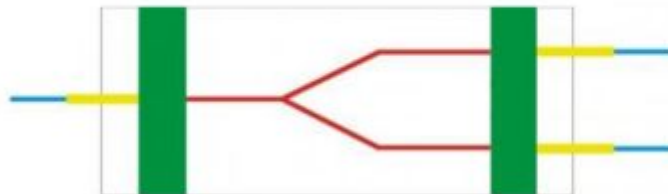


Рис.1.29. Конструкции сплиттеров по технологиям сваривания и PLC

Метод рассеяния оптического потока на неоднородностях оптического волокна также подходит для съёма части информационного сигнала (рис.1.30), который реализуется путём воздействия на оптическое волокна без разрушения его целостности тепловым полем, радиационным полем и др.

Метод рассеяния оптического потока

Рассеяние света

отклонение распространяющегося в среде светового пучка во всевозможных направлениях на неоднородностях среды, на частицах и молекулах, при этом меняется пространственное распределение интенсивности, частотный спектр, поляризация света.

Рассеяние света зависит от частоты света, размера рассеивающих частиц.

Усиление эффекта рассеяния внешним воздействием

- ✓ теплового поля
- ✓ радиационного поля
- ✓ другие поля

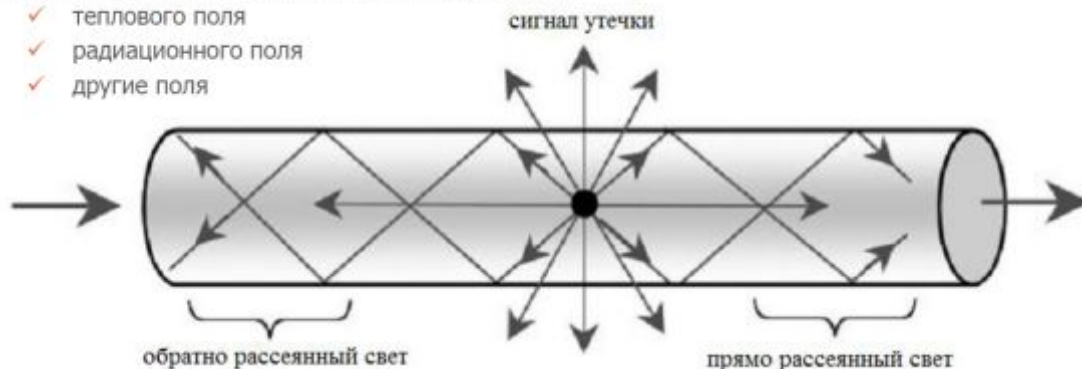


Рис.1.30 Метод рассеяния оптического потока

Если сравнить рассмотренные методы, то можно сказать следующее.

Особенности сигнала утечки информации при оптическом туннелировании: отсутствие обратного рассеянного и отраженного излучений; возможность регулирования мощности утечки; наиболее эффективен при промышленном изготовлении.

Особенности сигнала утечки информации на макроизгибе и ответвителе: простота и надежность реализации; дешевое исполнение, возможна

реализация кустарным способом; присутствие значительного рассеянного и отраженного излучений.

Для дистанционного решения по доступу к информационным сигналам в оптическом волокне подходит использование распределённой неоднородности (рис.1.31).

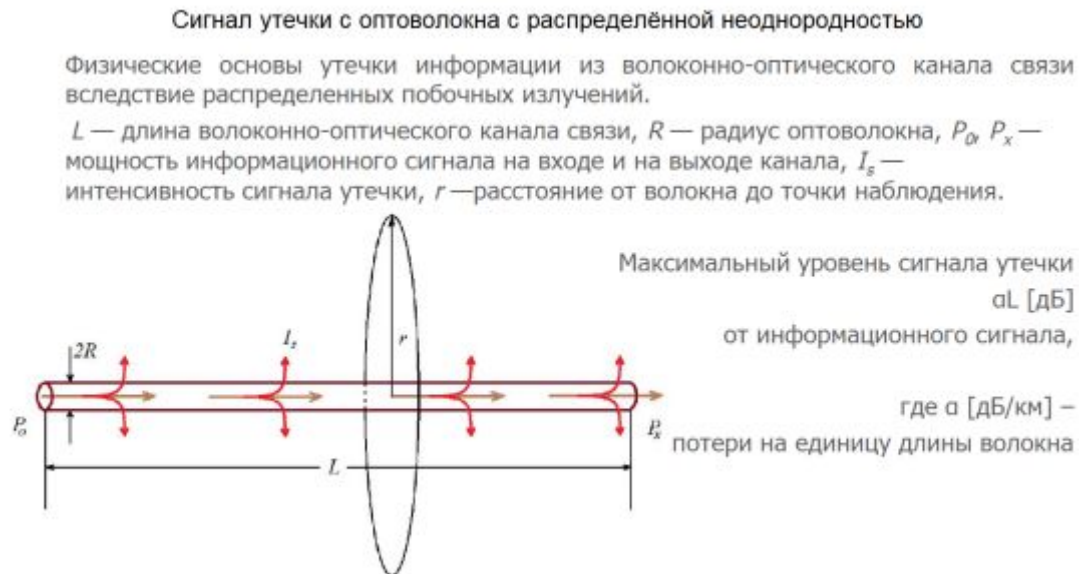


Рис.1.31. Волокно с распределённой неоднородностью и утечка сигнала

ПРИБОРНЫЕ ПОДКЛЮЧЕНИЯ С РАЗРЫВОМ И БЕЗ РАЗРЫВА ВОЛОКНА

Подключение к волокну с разрывом предполагает, как правило, краткий временной отрезок разрыва с подключением сплиттеров с оконцеванием разъёмами (рис.1.32) или вваривание волокон при монтаже оптических волокон.



Рис.1.32. Контактное подключение для отвода части оптического излучения

Подключение к волокну без разрыва стандартными приборами, например прищепками или измерителями оптической мощности (рис.1.33, 1.34).



Рис.1.33. Контактное приборное подключение к оптоволокну

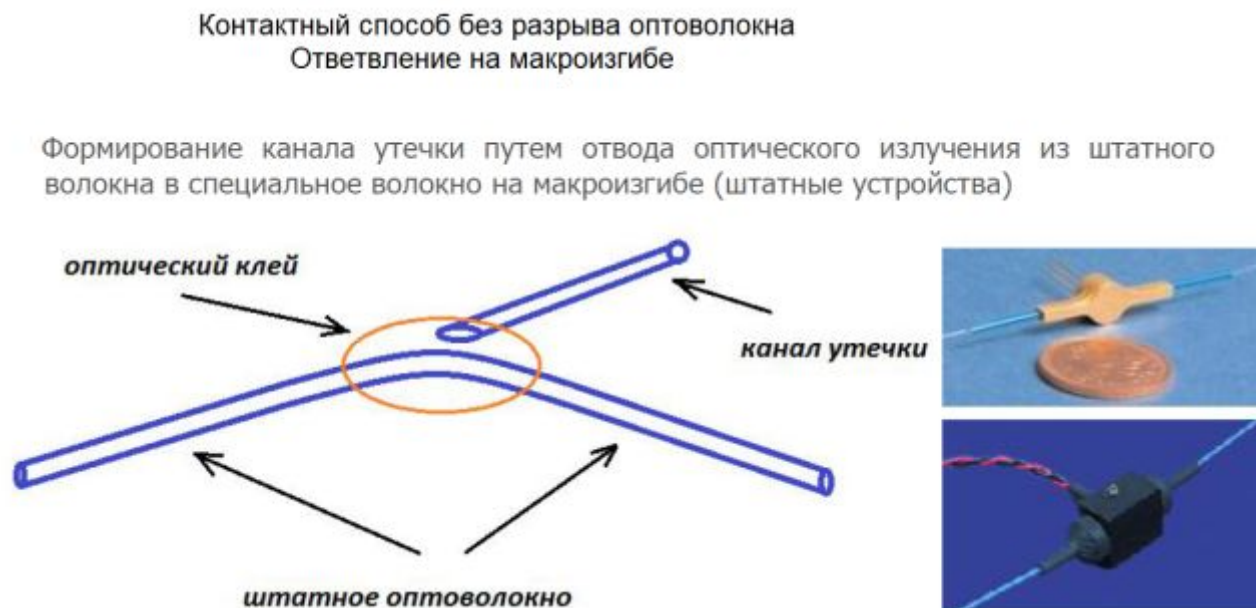


Рис.1.34. Контактное приборное подключение к оптоволокну на макроизгибе

Также контактное без разрыва подключение с возможностью туннелирования реализовано в приборных устройствах (рис.1.35, 1.36, 1.37).

Контактный способ без разрыва оптоволоконна

оптическое туннелирование

интегрально оптический ответвитель на основе оптического туннелирования

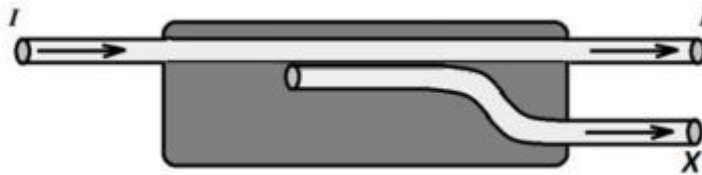
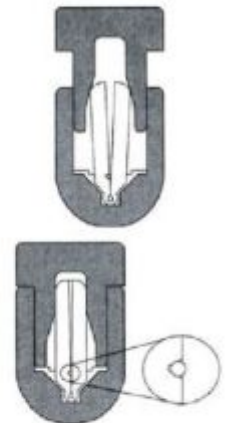


Рис.1.35. Контактное подключение без разрыва волокна

Контактный способ без разрыва оптоволоконна – **оптическое туннелирование**

Формирование сигнала утечки путем оптического туннелирования излучения из волокна в специальное волокно механически сцепленные боковыми поверхностями

Основные элементы Fibrlok™ II 2539



использование для бокового соединения
механического соединителя оптических волокон
типа FibrLok



Рис.1.36. Прибор для контактного подключения к волокну с туннелированием части оптического сигнала

Контактный способ без разрыва оптоволоконна

оптическое туннелирование

Формирование сигнала утечки путем оптического туннелирования излучения из волокна в охватывающую жидкую среду с показателем преломления выше волокна и отводящую его на регистрирующий элемент

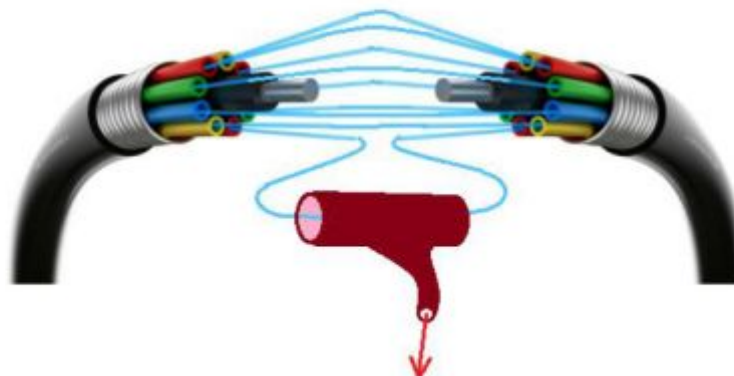
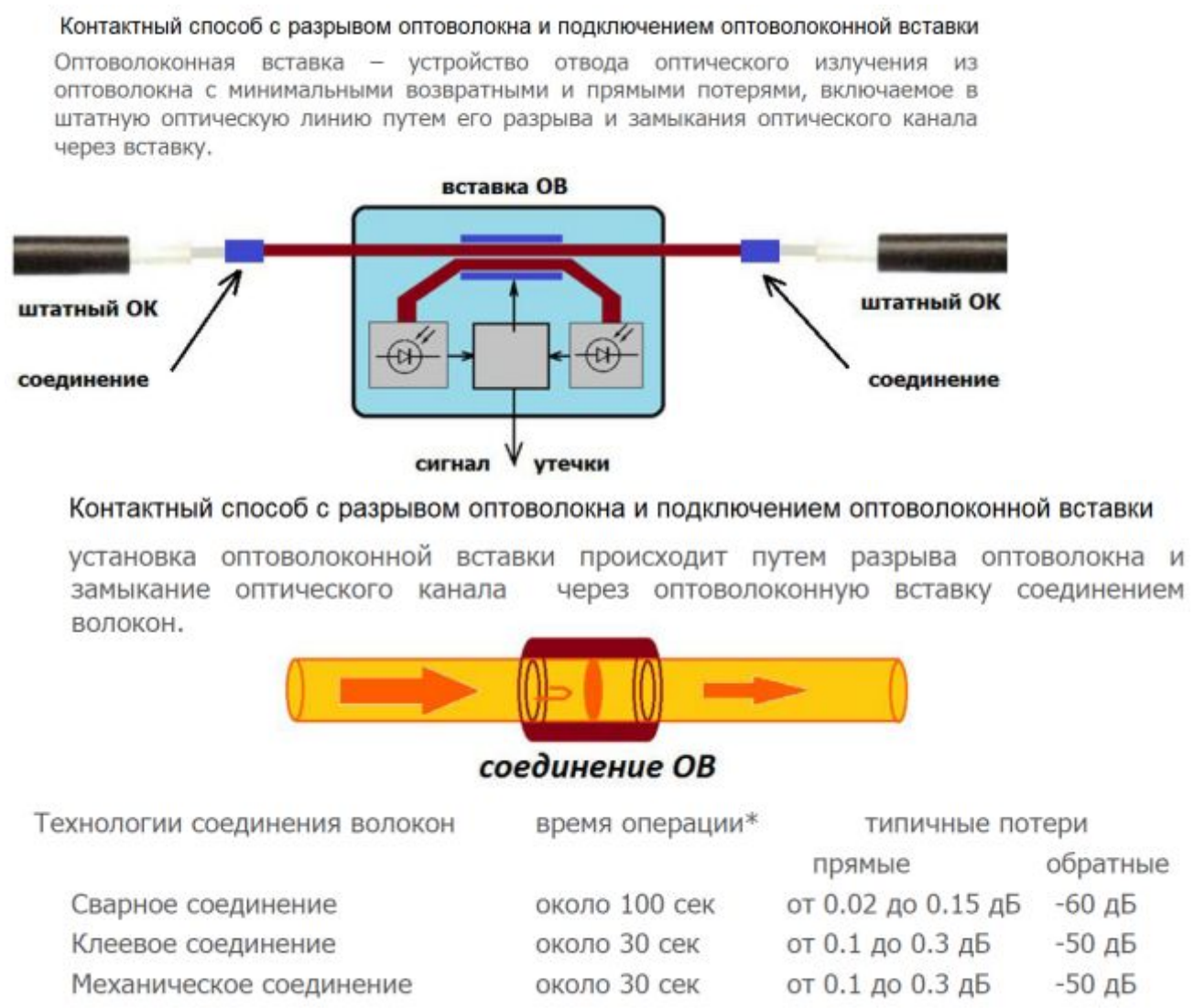


Рис.1.37. Оптическое туннелирование в жидкую среду

Выше рассмотренные технические решения предполагают доступ к среде с одним или множеством спектральных каналов передачи информации. Для доступа к оптической среде с одним каналом также возможны варианты реализации устройств съёма сигнала с штатными приборами (приёмными оптическими модулями) с разрывом и без разрыва волокна (рис.1.38).



*время операции без учета времени подготовки волокон

Рис.1.38. Контактный съём оптического сигнала с разрывом

Для установки устройства в виде вставки пригодны штатные коннекторы (рис.1.39).

Установка оптоволоконной вставки в линию со штатным разъёмным соединением

установка оптоволоконной вставки происходит путем размыкания штатного соединения оптоволоконна и замыкание оптического канала через оптоволоконную вставку соединением волокон через штатные разъёмы.

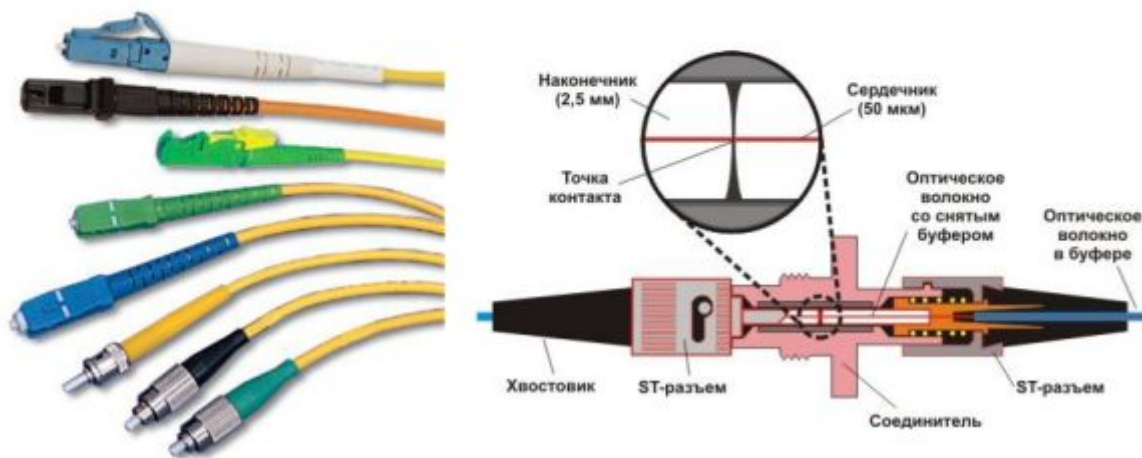


Рис.1.39. Вставки со штатными разъёмами

Вставки разрывом оптоволоконна в оборудовании и без разрыва с подключением к стороне передатчика возможны в кроссовом оборудовании (рис.1.40).

Установка оптоволоконной вставки в линию со штатным разъёмным соединением

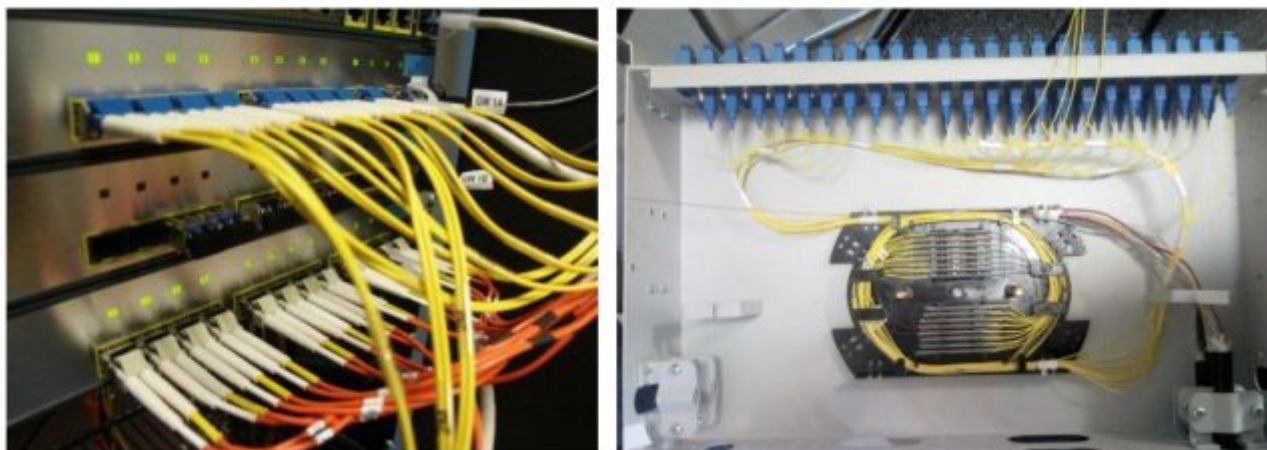


Рис.1.40. Места установки вставок с разрывом и без разрыва линии

Кратко выводы по подключениям.

Перехват трафика возможен с внутренних и внешних волоконно-оптических коммуникаций (кабеля и оборудования) с использованием штатных технических устройств; возможности нарушителя определяются доступом к волоконно-оптическим коммуникациям и его уровнем технической подготовки; наиболее опасным является подсоединение к оптическому каналу и отвод излучения методом оптического туннелирования, в том числе штатными средствами. Физические принципы не исключают возможности дистанционного перехвата трафика.

Как обнаружить технические средства перехвата информационных сигналов в оптических каналах ВОСП?

Наиболее точно и реально обнаружить перехват методами оптической рефлектометрии (<https://lenlasers.ru/novosti-i-stati/reflektometriya-opticheskikh-volokon/>):

импульсная рефлектометрия (optical time domain reflectometer, OTDR);

частотная рефлектометрия (optical frequency domain reflectometer, OFDR);

бриллюэновская рефлектометрия (Brillouin optical time domain reflectometer, BOTDR);

когерентная рефлектометрия (coherent optical time domain reflectometer, C-OTDR);

поляризационная рефлектометрия (polarization optical time domain reflectometer, P-OTDR).

Анализ рефлектограммы оптического кабеля позволяет обнаружить и измерить все **основные параметры и события в кабеле**, в том числе:

определить длину оптического кабеля (начало и конец линии);

определить местонахождение и качество сварных соединений (предельно допустимые значения потерь на сварке зависят от типа сети, для городских ВОЛС обычно не более 0,2 дБ);

определить местонахождение и качество оптических коннекторов (предельные значения допустимых величин отражения и потерь зависят от типа сети, типа коннектора и полировки ферулы; обычно отражения не более – 45 дБ, потери не более 0,2 дБ);

определить наличие и местоположение трещин, макроизгибов, обрывов;

измерить потери и отражения на основных событиях;

измерить суммарные потери на линии;

и другие события.

ПОЧТИ ВСЕ современные программно-аппаратные комплексы мониторинга волоконно-оптических линий используют рефлектометрию!

Контрольные вопросы

1. Что входит в понятие современных оптических сетей связи?
2. В чём состоят задачи современных оптических сетей связи?
3. Чем оценивается качество передачи информации в оптических сетях?
4. Почему необходимо защищать информацию, передаваемую в оптических сетях?
5. Откуда происходит угроза безопасности ТК сети?
6. Что такое квантовые коммуникации?
7. Для чего нужна квантовая криптография?
8. Для чего нужны квантовые сети связи?
9. Что является основой квантовой сети?
10. Что такое квантовые технологии и как они связаны с квантовыми коммуникациями?

11. Для каких протокольных уровней семиуровневой модели предназначены стандартизированные средства защиты информации в транспортной сети и сети доступа?

12. Какой подход к безопасности ТК сети самый простой?

13. Чем обусловлена эффективность криптозащиты информации на уровнях L1/L2 в телекоммуникационной сети?

14. Что есть перехват трафика в волоконно-оптических соединениях?

15. Что обозначают стандартизированные сокращения: НСД, НСИ, ТСР, ТКУИ?

16. Что такое сценарий угрозы информации?

17. Какие виды угроз рассматриваются в ТК?

18. Где может произойти утечка информации в ТК сети?

19. Где выявляются угрозы утечки информации в ТК сети?

20. Какими методами можно снять информацию в оптической ТК системе?

21. Как можно подключиться к волоконно-оптическому каналу?

22. В каких частях волоконно-оптической системы наиболее вероятен НСД?

23. Как можно воздействовать на изменение параметров волоконно-оптического кабеля?

24. Как можно зарегистрировать утечку информации в волоконно-оптической системе?

25. Где можно перехватить трафик в ВОСП?

26. Какие технические средства можно применить для перехвата трафика в ВОСП?

27. Как можно отвести часть оптического излучения из оптического волокна?

28. Что такое оптическое туннелирование?

29. Какими штатными оптическими приборами можно обеспечить утечку информации из ВОСП?

30. Где в оборудовании ВОСП можно подключить устройство утечки информации?

31. Что представляет собой оптоволоконная вставка?

32. Как можно подключиться к оптическому волокну без разрыва?

33. Что может показать рефлектограмма при проверке волоконно-оптической линии?

34. Какие из определений в разделе «1.3 Терминология...» не относятся к квантовым коммуникациям?

35. В чём состоят задачи проектов квантовых сетей связи?

36. Какой протокол распределения квантовых ключей был разработан первым и когда?

37. Чем отличаются друг от друга функции кодирования, шифрования и хеширования?

38. Для чего нужен квантово-криптографический шифратор?

39. Что такое кубит?

40. Что такое квантовая запутанность?

Задача 1.

В волоконно-оптической линии длиной L (рис.1.) организован квантовый канал передачи ключа шифрования с защитой сигнала в виде предискажения этого сигнала волокном с положительной дисперсией, растягивающей оптические импульсы формата NRZ на скорости V на 100%. Используя данные табл. 1 и 2 рассчитать необходимую длину волокна с положительной дисперсией, подключаемого к передатчику оптического сигнала, передаваемого на скорости V , и компенсирующего волокна с отрицательной дисперсией, подключаемому к оптическому приёмнику, учитывая при этом и дисперсию, вносимую в протяженной оптической линии L . Рассчитать необходимое усиление оптического усилителя на приёмной стороне, если известно: минимальная чувствительность оптического приёмника S ; удельное затухание предискажающего волокна на передаче, компенсирующего волокна на приёме и линейного оптического волокна стандарта G.652d. Уровень оптической мощности на выходе передатчика 0 дБм. Затухание разъёмных и сварных стыков оптических волокон не учитывать.

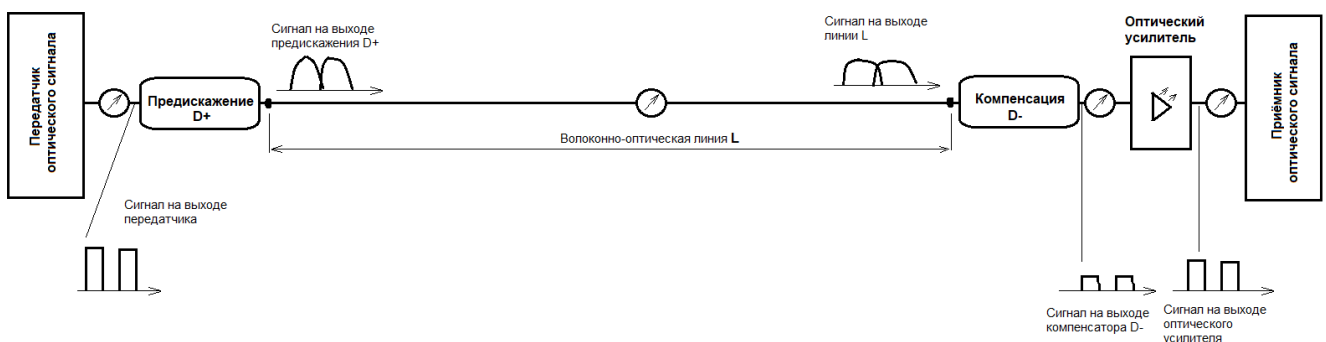


Рис.1. Схема волоконно-оптической линии связи с защитой квантового канала

Таблица 1. Исходные данные для расчёта по варианту, соответствующего предпоследней цифре номера студенческого билета или номера пароля

Номер варианта	0	1	2	3	4	5	6	7	8	9
L , км	60	70	80	90	100	110	120	65	75	85

Таблица 2. Исходные данные для расчёта по варианту, соответствующего последней цифре номера студенческого билета или номера пароля

Номер варианта	0	1	2	3	4	5	6	7	8	9
Скорость передачи, V , Гбит/с	1,25	2,5	5	10	20	1,25	2,5	5	10	20
Чувствительность, S , дБм	-24	-22	-21	-20	-25	-26	-27	-28	-29	-30
Удельная дисперсия, $D+$, пс/нм×км	60	65	70	75	80	85	90	95	100	105

Удельная дисперсия, D-, пс/нм×км	-65	-70	-75	-80	-85	-90	-95	-60	-55	-50
Удельное затухание ОВ G.652d, α, дБ/км	0,19	0,2	0,21	0,22	0,23	0,24	0,25	0,26	0,27	0,28
Удельная дисперсия ОВ G.652d, σ, пс/нм×км	15	16	17	18	19	20	21	22	23	24

Примечание: удельное значение затухания волокон предискажения и компенсации считать равным 0,2 дБ/км.

Методические указания к решению задачи 1.

1. По заданной скорости определить длительность оптического импульса в формате NRZ, т.е. импульс затянута на весь тактовый интервал, рассчитываемый делением $1/V$. Пример: $1/1\text{Гбит/с}=1\text{нс}$.

2. Импульс после предискажения увеличивается в 2 раза (100%), т.е. длина волокна D_+ определяется делением величины уширения на удельное значение с учётом, что ширина спектра сигнала передатчика равна 1нм. Пример: $1\text{нс}/50\text{пс/нм}\times\text{км}=20\text{км}$.

3. Вычисляем совокупную дисперсию предискажения D_+ и линии L . Пример:

$$D_{\Sigma} = D_+ + \sigma \times L = 1\text{нс} + 20\text{пс/нм}\times\text{км} \times 50\text{км} = 2\text{нс}.$$

4. Для компенсации всех дисперсионных искажений вычисляем длину волокна D_- . Пример: $D_{\Sigma}/D_{\text{уд}} = 2\text{нс}/-50\text{пс/нм}\times\text{км}=40\text{ км}$.

5. Вычислить требуемое усиление оптического усилителя на входе приёмника оптического сигнала. Для этого необходимо определить уровень оптической мощности на входе оптического усилителя

$$P = P_{\text{пер}} - A_{\Sigma} = P_{\text{пер}} - (A_{D_+} + A_L + A_{D_-}) = 0\text{дБм} - (20\text{км}\times 0,2\text{дБ/км} + 100\text{км}\times 0,2\text{дБ/км} + 40\text{км}\times 0,2\text{дБ/км}) = -32\text{ дБм}.$$

При минимальной чувствительности приёмника -20 дБм потребуется оптический усилитель с минимальным коэффициентом 12 дБ.

Сделать выводы по результату решения задачи!

2. Оптические транспортные сети и сети доступа с физической защитой информационных соединений и защитой на основе криптографии в интерфейсах

2.1. Классификация защиты оптических соединений

Защита информации при передаче в оптической системе или сети может осуществляться различными способами, каждый из которых имеет свои преимущества и недостатки (рис.2.1).

Все способы защиты информации от утечки по оптическому каналу (волокну) делятся на две группы: **способы защиты сигналов** и **способы защиты каналов (волоконных соединений)**. Способы защиты сигналов не обеспечивают защитой канал (волоконное соединение) от несанкционированных подключений, съёма и ввода-вывода сигналов или иных воздействий; они только затрудняют (в пределе делают невозможной) обработку перехваченных сигналов: структурирование и расшифровку.

Способы защиты канала (волокна) также не в состоянии предотвратить подключение к каналу за пределами контролируемой зоны кабельной линии, но позволяют затруднить доступ, либо обнаружить попытку несанкционированного подключения и прервать или переключить передачу сигналов. Тем самым кроме защиты канала (волокна) защищается и передача сигнала.

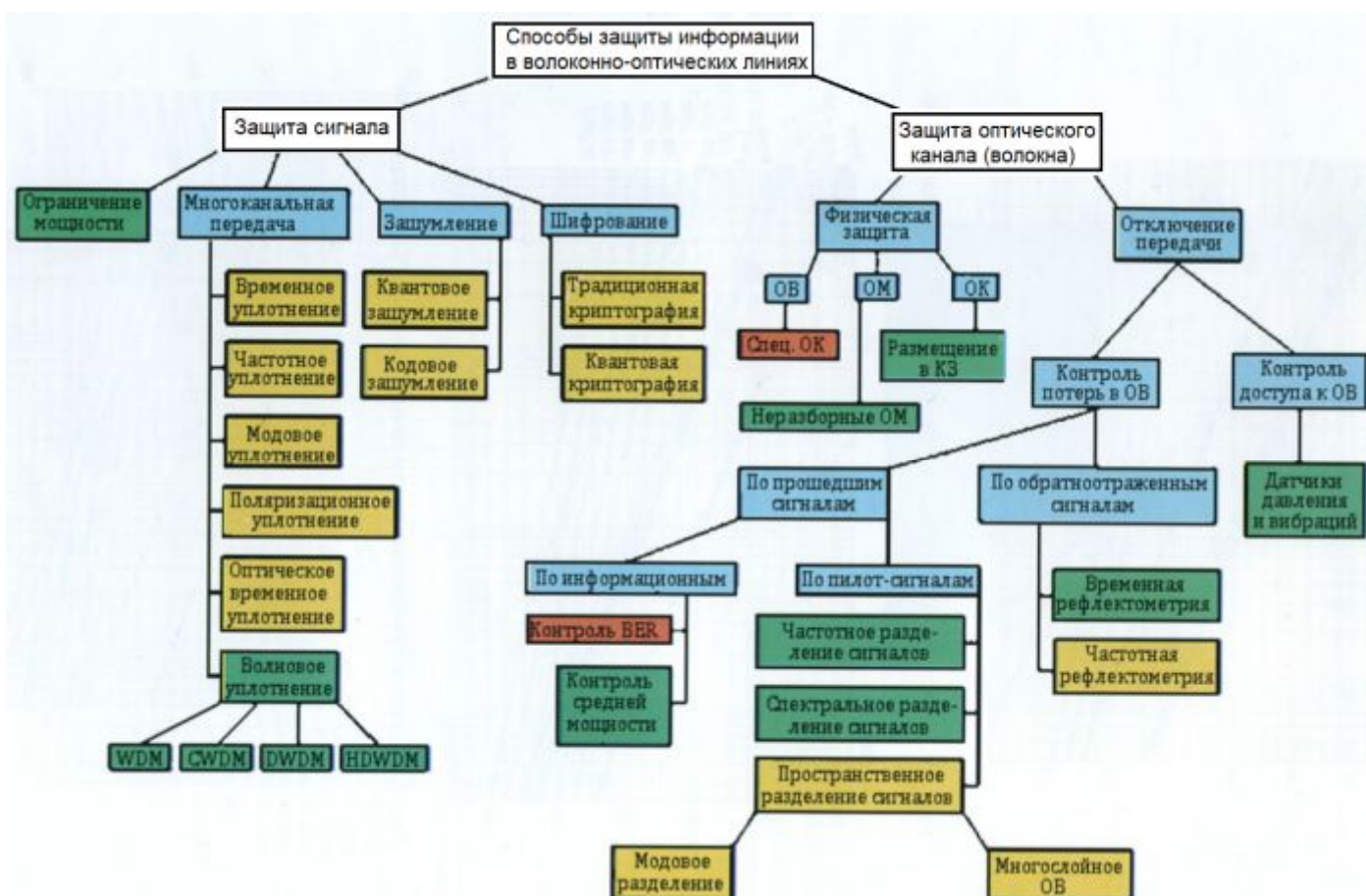


Рис.2.1. Общая классификация способов защиты информации в ВОЛС

2.2. Технические средства физической защиты оптических соединений и информации

Построение Технических Средств Физической Защиты Информации (ТСФЗИ) от перехвата в ВОСП основано на анализе возможностей нарушителя и физико-технических особенностях волоконно-оптических каналов связи: преимущества оптического волокна и кабеля как транспортной среды для информации связаны с возможностью построения транспортной среды из полностью диэлектрических материалов и отсутствие металла, который легко обнаруживается; высокой скоростью передачи информации при низком уровне шумов; ограниченностью дистанционных методов съема информации; возможностью объединения транспортных и контрольно-измерительных сетей в единую инфраструктуру; большая удаленность друг от друга активных сетевых элементов.

Оптический кабель может быть использован как среда для передачи информации оптическими сигналами и как среда для измерений воздействий и полей оптическим зондирующим излучением. Совмещение двух различных функций в одном кабеле позволяет реализовать функцию защиты от перехвата следующими способами:

- контроль намерений нарушителя по его действиям вблизи кабеля;
- контроль состояния защитных покрытий/оболочек кабеля на предмет преднамеренного разрушения;
- защита кабеля от разрушения защитных покрытий/оболочек кабеля;
- защита волокна от несанкционированных измерений путем отвода оптических излучений.

Контроль намерений нарушителя по его действиям вблизи кабеля сопровождаются вибро-акустическими сигналами, воздействующими на волокно оптического кабеля и вызывающими в нем паразитные модуляции параметров оптического излучения. На этих свойствах оптического кабеля функционируют распределенные волоконно-оптические системы охраны периметра объектов, промышленно выпускается много подобных систем, в том числе в России:

1. Волоконно-оптическая периметральная система охраны «ВОРОН™» ООО «Прикладная радиофизика» www.neurophotonica.ru
2. Волоконно-оптическая система охраны «СОВА» Инновационный центр «Оптика» www.centropic.ru
3. Оптоволоконная распределенная система вибромониторинга и охраны периметра ООО «Оптолекс» www.optolex.ru
4. Когерентный рефлектометр «Дунай» ООО «Т8» www.t8.ru

Принципы функционирования волоконно-оптических систем охраны периметра (ВОСП) основаны на регистрации виброакустических колебаний окружающей среды методами: регистрации межмодовой интерференции; регистрации спекл-структуры в оптическом волокне; двух лучевой интерференции; датчиками на брэгговских решетках; когерентной рефлектометрии.

Для защиты оптического кабеля в его структуру вводятся элементы, препятствующие разрушению и проникновению внутрь кабеля для последующего получения доступа к волокну: усиленное бронирование; защитное покрытие/оболочка с само разрушающимися при воздействии свойствами; воздействие на кабель регистрируется ТСЗИ не волоконно-оптическими методами, например, подводный кабель под высоким напряжением; защитные оболочки кабеля имеют прочную механическую защиту, содержащую металлическую оболочку; в кабеле для подводного монтажа металлическая оболочка используется для электрического питания оптических усилителей, на которую подается высокое напряжение и в зависимости от длины подводной части напряжение достигает нескольких 10 кВольт. Также созданы волокна специальных конструкций с защитой от несанкционированных измерений (рис.2.2).

Специальное волокно с защитой от несанкционированного измерения ступенчатое волокно со сдвоенными concentрическими сердцевинами для защищаемого трафика (1) и с защитным шумовым излучением (2)

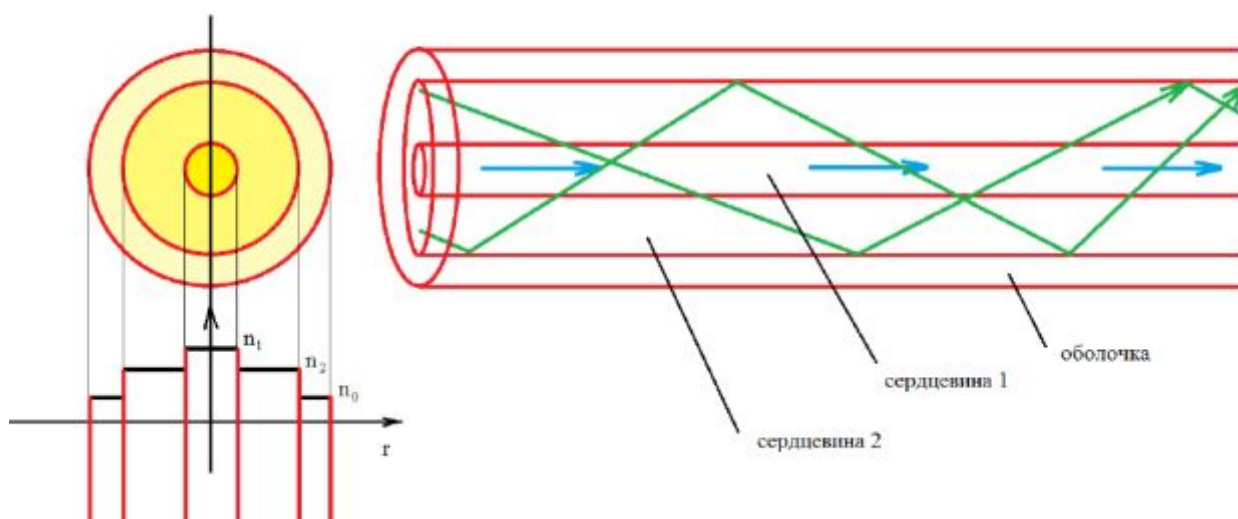


Рис.2.2. Специальное волокно с защитой от несанкционированных измерений

Краткие выводы по охране периметра оптического кабеля.

1. Охрана периметра оптической системы передачи или сети применима для защиты локальных сетей, так как охраняемый периметр ограничен дальностью действия системы;

2. Другие методы физической защиты применимы как в телекоммуникациях, так и локальной связи, но эффективность защиты связывается только со сложностью выполнения работ по нарушению защитных свойств;

3. Для защиты волокна от физического доступа могут быть использованы специальные оптические кабели с встроенными средствами защиты, когда возможны два направления защиты при вскрытии кабеля:

- воздействие на нарушителя с целью нанесения вреда его здоровью (электрическое, химическое);

- воздействие на волокно с целью его обрыва для прекращения передачи сигналов.

4. Подобные системы защиты являются неотъемлемой частью монтируемой кабельной системы и первым рубежом защиты информационного трафика.

Обнаружение «закладок» в оптическом волокне методом рефлектометрии. Подключение технических средств для отвода и регистрации оптических сигналов («закладок») можно осуществить двумя способами: **с разрывом** волокна с помощью разъёмного оптического соединителя или отводов с оптическим соединителем; **без разрыва** волокна с помощью локального изгиба волокна или путём туннелирования на протяжённом участке волокна. Любое подключение к волокну приёмника перехвата с помощью оптических соединителей неизбежно приводит к появлению в точке подключения воздушного зазора, т.е. на рефлектограмме к появлению отраженного сигнала. Если такой сигнал появляется за пределами зоны контроля линии, то это верный признак «закладки»!!! Подключение к волокну приёмника перехвата с помощью изгиба (или другого способа) без разрыва волокна приводит к тому, что появляется локальный дефект, но только с прямыми потерями без отражения. Диапазон внесённых потерь таких способов может совпадать с диапазоном прямых потерь в сварных соединениях (от 0,001 до 0,1дБ), поэтому для отделения «закладки» от сварных соединений требуются другие признаки, которые определяются из сравнения рефлектограмм с двух сторон измерения и на разных длинах волн (1310нм и 1550нм).

Спектральная зависимость (зависимость от длины волны измерения) выводимого излучения через боковую поверхность без разрыва волокна может указывать на неоднородность (накладку), т.к. на рефлектограмме для двух волн потери на сварном соединении различны в прямом и обратном направлениях измерения и в расчёт принято брать среднее значение, но при этом на разных волнах потери в одном направлении сопоставимы, а потери от изгиба или накладки для двух волн в прямом и обратном направлении одинаковы на каждой из волн, но существенно (примерно в 10 раз) различны!!! Что позволяет идентифицировать неоднородность как «закладку».

Анализ попыток съёма с помощью различных способов позволяет разделить все сигналы на три категории: быстрый вывод, плавный вывод, ступенчатый вывод. Сигналы съёма различаются по амплитуде, длительности времени вывода и форме. При использовании устройств вывода и сбора излучения типа ответвитель-прищепка осуществляется **быстрый вывод**, когда учитывается переходный процесс аппаратуры регистрации около 1с. Такой съём **преследует цель** зарегистрировать (или передать) сигнал с незащищённой ВОСП или с защищённой ВОСП, но только за время регистрации системы защиты. При **плавном выводе целью нарушителя** является сокрытие подключения, внесение минимальных потерь и регистрация перехваченного сигнала длительное время! Это способ представляет наибольшую опасность! **Ступенчатый вывод** преследует **цель** нейтрализации системы защиты, обнаруживающей плавный вывод путём многократного периодического вывода мощности сигнала на величину ниже порога обнаружения контроллера защиты.

Аппаратные средства защиты информации волоконно-оптических соединений: коммутация или переключение линий; использование режима динамического хаоса; использование кодового зашумления; применение технологии оптической CDMA; применение разно-знаковых компенсаторов дисперсии; мультиплексирование шума и сигнала на разных длинах волн; контроль уровня битовых ошибок и т.д. (см. классификацию на рис.2.1).

Пример построения коммутатора на базе MEMS приведён на рис.2.3.

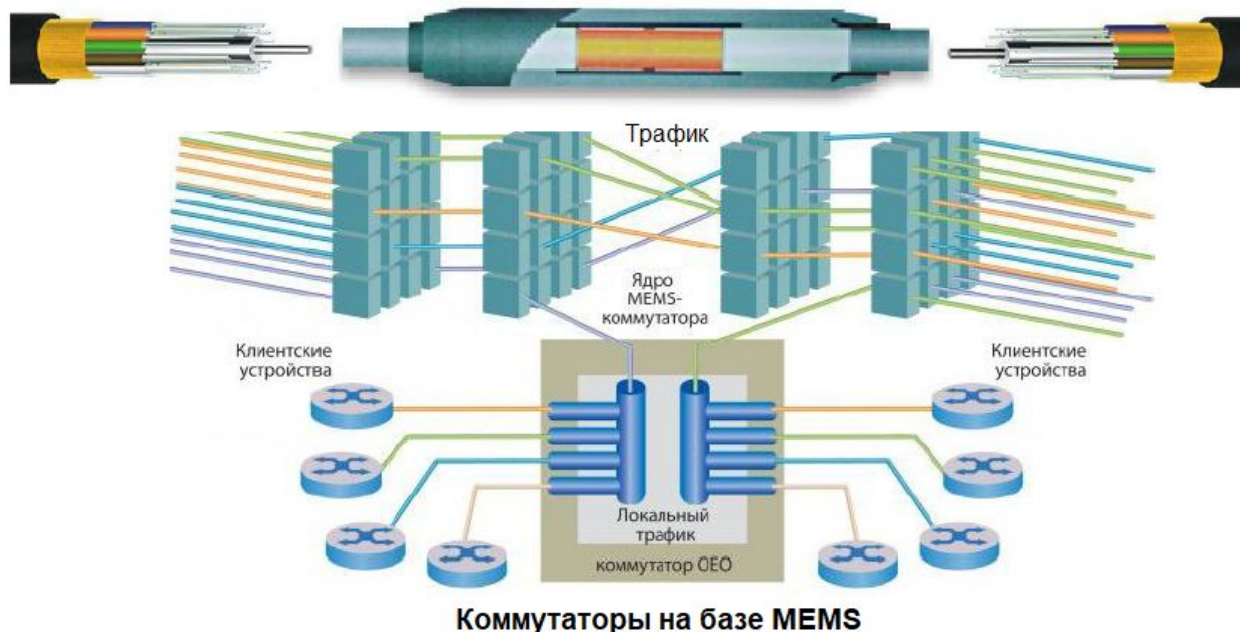


Рис. 2.3. Конструкция оптического коммутатора для управлением трафика в направлениях

Для реализации режима динамического хаоса передатчик и приемник включают в себя такие же нелинейные и линейные системы, как источник (рис.2.4). Дополнительно в передатчик включен сумматор, а в приемник вычитатель. В сумматоре производится сложение хаотического сигнала источника и информационного сигнала, а вычитатель приемника предназначен для выделения информационного сигнала. Сигнал в канале хаосоподобный и не содержит видимых признаков передаваемой информации, что позволяет передавать конфиденциальную информацию. Сигналы в точках А и А', В и В' попарно равны. Поэтому при наличии входного информационного сигнала S на входе сумматора передатчика такой же сигнал будет выделяться на выходе вычитателя приемника.

При использовании кодового зашумления (метод случайного кодирования) защита информации обеспечивается не за счет воздействия на параметры каналов утечки, а за счет вероятностного преобразования информации перед передачей по каналу связи. Невозможность восстановления информации злоумышленником основана на том свойстве, что канал утечки имеет меньшую пропускную способность, чем штатный канал пользователя. Способ кодирования выбирается так, чтобы в канале утечки количество возникающих ошибок сильно возросло,

обеспечивая эффект зашумления передаваемого сигнала, в то время как в основном канале обеспечивалась надежная связь.

Применение разнознаковых компенсаторов дисперсии для внесения искажения сигнала позволяет затруднить доступ к информационному сигналу (рис.2.5).

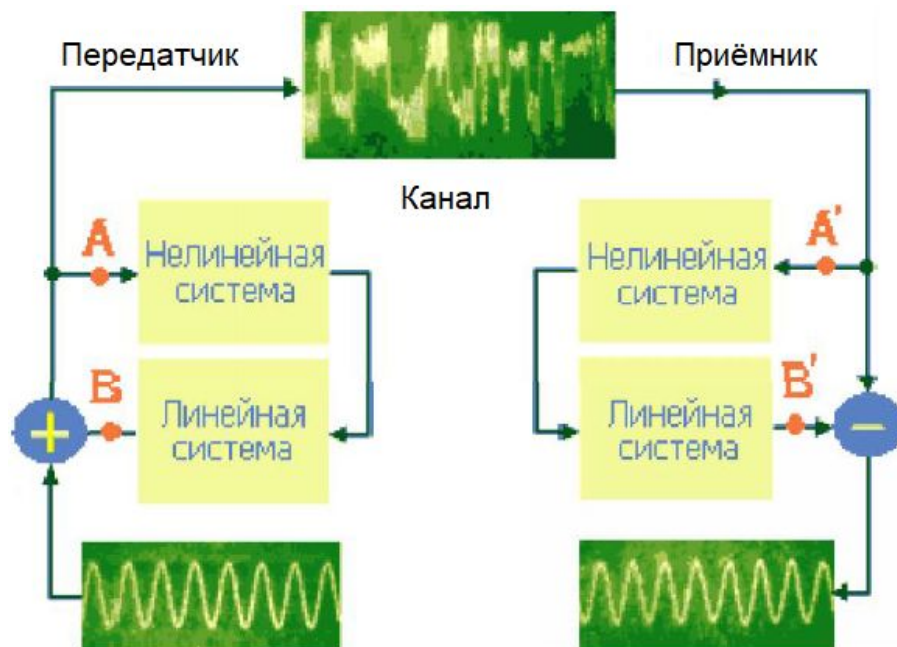


Рис.2.4. Система с динамическим хаосом

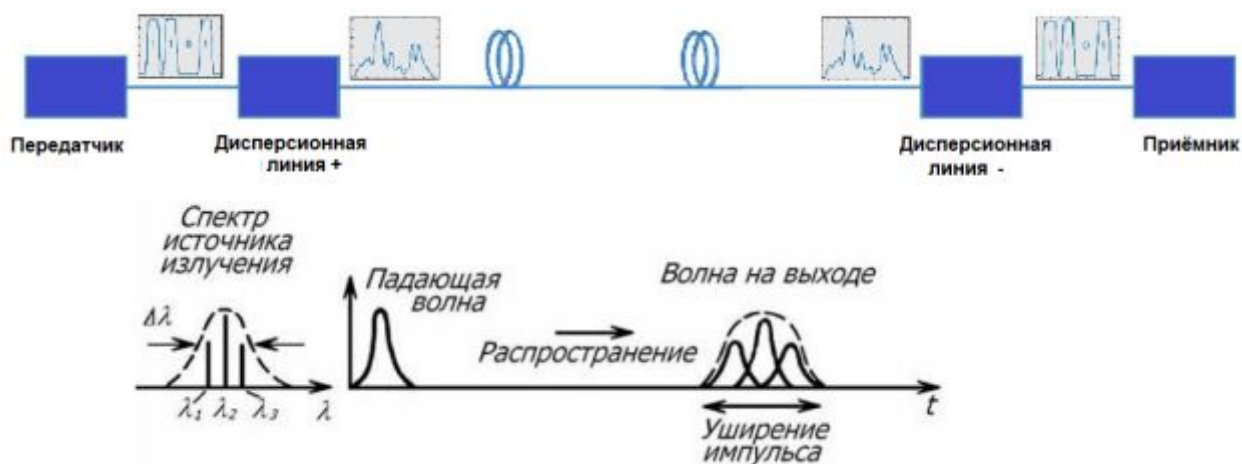


Рис.2.5. Оптическое соединение с применением разнознаковых компенсаторов дисперсии

Защита трафика на основе технологии Optical Code Division Multiple Access (OCDMA), т.е. технологией связи множественного доступа с кодовым разделением, при которой каналы передачи имеют общую полосу частот, но разную кодовую модуляцию. В отличие от других методов доступа абонентов к сети, где энергия сигнала концентрируется на выбранных частотах (Frequency

Division Multiple Access, FDMA) или временных интервалах (Time Division Multiple Access, TDMA), сигналы CDMA распределены в непрерывном частотно-временном пространстве, т.е. происходит манипуляция и частотой, и временем, и энергией (рис.2.6).

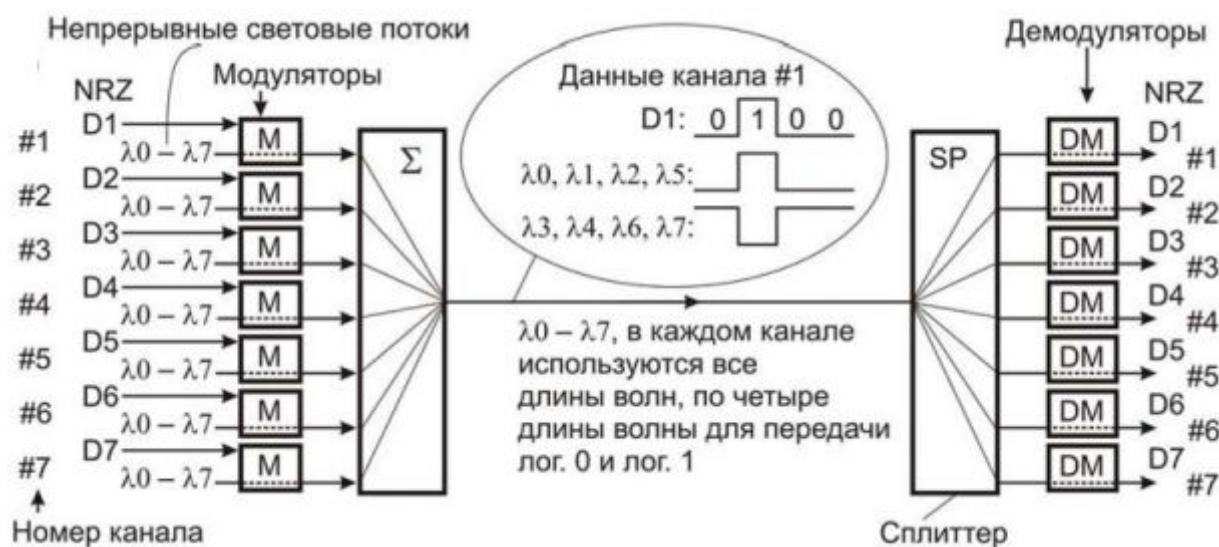


Рис.2.6. Структура системы передачи с применением CDMA

2.3. Криптография для защиты оптических соединений. Основные определения

Наукой, изучающей математические методы защиты информации путем ее преобразования, является **криптология**.

Криптология разделяется на два направления – криптографию и криптоанализ.

Криптография: Область теоретических и прикладных исследований и практической деятельности, которая связана с разработкой и применением методов криптографической защиты информации.

Криптографический анализ: Область теоретических и прикладных исследований, имеющих конечной целью получение обоснованных оценок криптографической стойкости криптографической системы в целом или отдельного криптографического механизма.

Под **криптографической защитой информации** (рис.2.7) понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий.

Целью сжатия является **сокращение объема информации**.

Сжатая информация не может быть прочитана или использована без обратного ее преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы **нельзя рассматривать как надежные средства криптографического преобразования информации**.

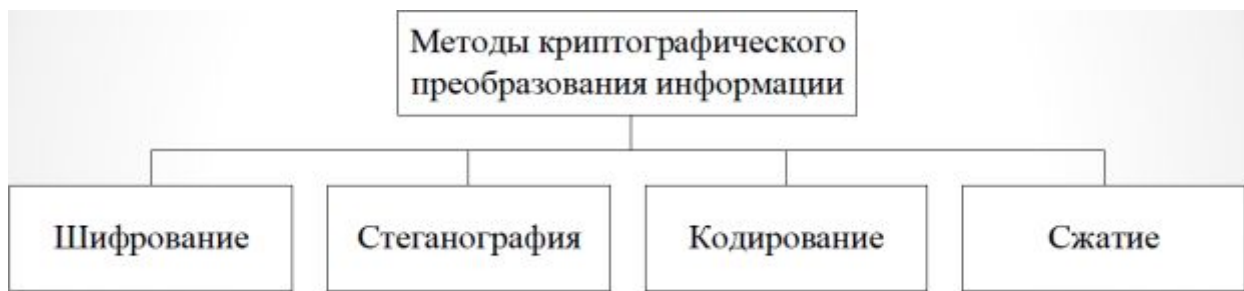


Рис.2.7. Методы криптографического преобразования информации

Содержанием процесса **кодирования информации** является замена смысловых конструкций исходной информации (слов, предложений) кодами.

Кодирование информации целесообразно применять в системах с ограниченным набором смысловых конструкций. Такой вид криптографического преобразования применим, например, в командных линиях автоматизированных систем управления. **Недостатками** кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо часто менять, чтобы избежать раскрытия кодов статистическими методами обработки перехваченных сообщений.

Под **шифрованием** понимается процесс преобразования открытой информации в зашифрованную (шифротекст) или процесс обратного преобразования зашифрованной информации в открытую.

Для шифрования информации используются **алгоритм преобразования и ключ**.

Как правило, алгоритм для определенного метода шифрования является **неизменным**. Исходными данными для алгоритма шифрования служат **информация**, подлежащая шифрованию, и **ключ шифрования**.

Методом шифрования (шифром) называется совокупность обратимых преобразований открытой информации в закрытую в соответствии с алгоритмом шифрования.

Атака на шифр (криптоанализ) – это процесс дешифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.

Процесс восстановления первоначального открытого текста на основе шифрованного без знания ключа называют дешифрованием.

Современные методы шифрования должны отвечать следующим **требованиям**:

стойкость шифра противостоять криптоанализу (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;

криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;

шифротекст не должен существенно превосходить по объему исходную информацию;

ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

время шифрования не должно быть большим;

стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

В общем, что представляют собой методы криптографической защиты информации?

Криптографические методы защиты информации - это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования.

Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя).

Основным достоинством криптографических методов защиты информации является то, что они обеспечивают высокую гарантированную стойкость защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей).

К числу основных недостатков криптографических методов можно отнести следующие:

- большие затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации;

- высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены;

- необходимость защиты открытой информации и ключей от несанкционированного доступа (НСД).

При этом важнейшее решение по защите информации возлагается на телекоммуникационные системы, которые позволяют преодолеть в значительной степени выше указанные недостатки и особенно в высокоскоростных транспортных соединениях на основе оптических каналов 1/10/100 Гбит/с.

Шифрование может применяться для физических и виртуальных соединений в сетях связи и вообще могут быть построены сети с полностью защищаемыми каналами. Всё, что связано с защитой соединений является предметом стандартизации и сертификации, всё есть предмет детального изучения в правовой плоскости, в идеологии защиты и её реализации на основе конкретных устройств (оборудование, интерфейсы, протоколы и т.д.).

2.4. Нормативное регулирование средств криптографической защиты информации в каналах связи, основанное на Федеральных законах, стандартах, приказах, положениях и инструкциях

(Исходная информация в ГОСТ Р 34.10-2012, ГОСТ Р 34.11 2012, ГОСТ 28147-1989 ГОСТ Р 34.12-2015. Подробности по адресу: <https://www.securitylab.ru/blog/company/solarsecurity/347139.php>)

Предварительный национальный стандарт Российской Федерации ПНСТ 799-2022. Криптографическая защита информации. Введён в действие 1.01.23. В содержании стандарта приводятся термины и определения.

Приказами Росстандарта от 07 августа 2012 г. №№ 215-ст, 216-ст утверждены новые национальные стандарты ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (взамен ГОСТ Р 34.10-2001) и ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» (взамен ГОСТ Р 34.11-94) со вводом в действие 1 января 2013 года. Данные стандарты разработаны Центром защиты информации и специальной связи ФСБ России с участием ОАО «ИнфоТеКС».

Стандарт ГОСТ Р 34.11-2012 определяет две функции хэширования – с длинами хэш-кода 256 и 512 бит, известные также как «Стрибог-256» и «Стрибог-512». Данные хэш-функции полностью отличаются от хэш-функции, определяемой стандартом ГОСТ Р 34.11-94, при этом «Стрибог-256» отличается от «Стрибог-512» только значением инициализационного вектора и усечением хэш-кода до 256 старших бит.

Стандарт ГОСТ Р 34.10-2012 определяет ту же общую схему электронной цифровой подписи, что и ГОСТ Р 34.10-2001, но отличается от ГОСТ Р 34.10-2001 наличием дополнительного варианта требований к параметрам схемы (соответствующего длине секретного ключа порядка 512 бит) и требованием использования функций хэширования ГОСТ Р 34.11-2012: первый вариант требований к параметрам (такой же, как в ГОСТ Р 34.10-2001, соответствующий длине секретного ключа порядка 256 бит) предусматривает использование хэш-функции с длиной хэш-кода 256 бит, дополнительный вариант требований к параметрам предусматривает использование хэш-функции с длиной хэш-кода 512 бит.

Поскольку единственной отечественной стандартизированной схемой, использующей функцию хэширования, является схема ЭЦП, ограничимся рассмотрением только средств электронной (цифровой) подписи.

С 1 января 2013 года при разработке средств электронной подписи для информации, не содержащей сведений, составляющих государственную тайну, подпадающих под действие п. 3 Положения ПКЗ-2005, рекомендуется использовать криптографические алгоритмы, определяемые новыми национальными стандартами ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 (использование вариантов указанных алгоритмов, соответствующих длине

секретного ключа порядка 256 бит, является предпочтительным, поскольку обеспечивает достаточный уровень криптографической стойкости и лучшие эксплуатационные характеристики, в том числе при совместной реализации со схемой ГОСТ Р 34.10-2001). При этом предлагается сделать исключение в случаях, когда данные средства ЭП предназначены для обеспечения совместимости с действующими средствами ЭП, реализующими схему ГОСТ Р 34.10-2001, или реализуют функцию проверки ЭП, выработанной по ГОСТ Р 34.10-2001, в пределах срока действия ключа проверки ЭП. Также представляется возможным в исключительных случаях по согласованию с ФСБ России использовать алгоритмы, определяемые стандартами ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94, при модернизации средств ЭП в информационных системах с большим количеством пользователей (при условии использования в хэш-функции набора узлов замены, соответствующего разрабатываемым в настоящее время техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации» «Методическим рекомендациям по заполнению узлов замены алгоритма шифрования ГОСТ 28147-89»).

2.5. Государственное регулирование

Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей.

Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

2.3.1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления,

распространения, а также от иных неправомерных действий в отношении такой информации;

- 2) соблюдение конфиденциальности информации ограниченного доступа;
- 3) реализацию права на доступ к информации.

2.3.2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

2.3.3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных выше в пунктах 1 и 3.

2.3.4. Владелец информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

- 1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- 2) своевременное обнаружение фактов несанкционированного доступа к информации;
- 3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- 4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- 5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- 6) постоянный контроль за обеспечением уровня защищенности информации.

2.3.5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

2.3.6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

В соответствии с Федеральным законом от 03.04.1995 № 40-ФЗ «О Федеральной службе безопасности» уполномоченным органом по обеспечению

криптографическими методами безопасности информационно-телекоммуникационных систем, сетей связи специального назначения и иных сетей связи, обеспечивающих передачу шифрованной информации, на территории Российской Федерации и в её учреждениях за границей, является Федеральная служба безопасности России.

Указанным законом в обязанность органам ФСБ России вменяется организация и обеспечение безопасности в сфере шифрованной связи в Российской Федерации¹⁰.

Помимо этого, органы ФСБ наделены правом осуществлять государственный контроль за организацией и функционированием криптографической безопасности информационно-телекоммуникационных систем, сетей связи, обеспечивающих передачу информации с использованием шифров. Также за органами ФСБ закреплена функция осуществлять «...регулирование в области разработки, производства, реализации, эксплуатации, ввоза в Российскую Федерацию и вывоза из Российской Федерации шифровальных (криптографических) средств и защищенных с использованием шифровальных средств систем и комплексов телекоммуникаций, а также в области предоставления на территории Российской Федерации услуг по шифрованию информации...» (Положение о Федеральной службе безопасности Российской Федерации).

Правовое регулирование основано также на ряде инструкций, например, «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», которая утверждена Приказом ФАПСИ при Президенте РФ от 13.06.2001 № 152.

Инструкция содержит разделы:

II. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

III. Порядок обращения с СКЗИ и криптоключами к ним. Мероприятия при компрометации криптоключей.

IV. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним.

V. Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации - государственный контроль осуществляет ФСБ России. В ходе государственного контроля изучаются и оцениваются:

организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации;

достигнутый уровень криптографической защиты конфиденциальной информации;

условия использования СКЗИ.

Где необходимо использовать стандартное шифрование данных в каналах связи?

Государственные органы – министерства и органы власти.

Операторы персональных данных – почти все организации в стране.

Электроэнергетика – генерирующие и сетевые компании.

Финансы – банки и страховые компании.

Предприятия критической инфраструктуры.

Здравоохранение – больницы, клиники, аптеки.

Ответственность за закрытие каналов связи несёт оператор связи, например, Ростелеком, в распоряжении которого находится оборудование для каналообразования и защиты (рис.2.8).

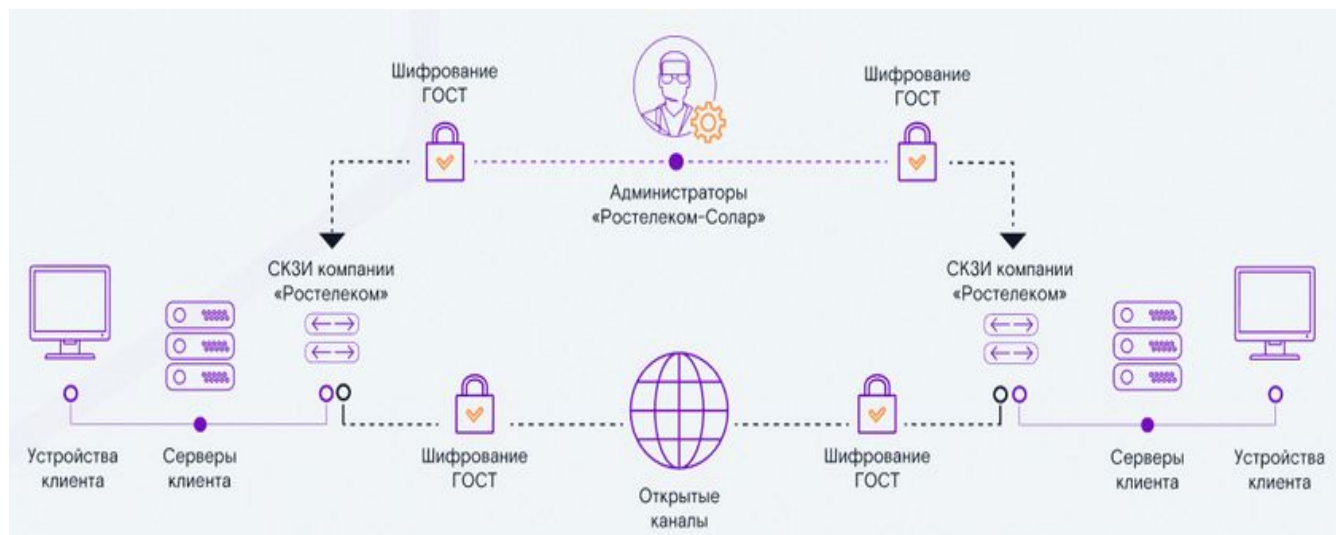


Рис.2.8. Схема организации закрытия каналов связи ОАО РОСТЕЛЕКОМ (<https://www.cnews.ru/book/Ростелеком ГОСТ VPN - CNews>)

Основные виды предприятий критической инфраструктуры, где требуется защита не только информации:

1. Энергетическая инфраструктура. Электроэнергетика: генерирующие станции, подстанции, линии электропередачи. Газоснабжение: газопроводы, компрессорные станции, газовые терминалы.
2. Транспортная инфраструктура. Дорожная сеть: автомагистрали, городские дороги, мосты, туннели. Железнодорожная инфраструктура: железные дороги, вокзалы, туннели. Авиационная инфраструктура: аэропорты, взлетно-посадочные полосы, навигационные системы. Морские и речные порты: доки, терминалы, судоходные пути.
3. Водоснабжение и водоотведение. Водозаборные сооружения: водозаборы, водонапорные башни, насосные станции. Водопроводная сеть:

водопроводные трубопроводы, водомерные сети. Канализационная система: канализационные трубопроводы, очистные сооружения.

4. Коммуникационная инфраструктура. Телекоммуникационная сеть: мобильная связь, проводные линии, оптические кабели. Интернет-инфраструктура: серверные центры, маршрутизаторы, спутниковая связь. Радио- и телевидение: телевышки, радиостанции.

5. Медицинская инфраструктура. Больницы и медицинские учреждения: госпитали, палаты, диагностические центры. Аптечные сети: аптеки, лаборатории, склады медицинских препаратов.

Защита критической инфраструктуры

Учитывая важность критической инфраструктуры, ее защита является критической задачей. Управленческие органы и операторы систем должны уделять особое внимание защите от потенциальных угроз, таких как технические сбои, природные катастрофы, террористические акты и кибератаки. Некоторые меры для обеспечения безопасности критической инфраструктуры включают:

1. Резервное питание и дублирование: установка генераторов питания и резервных источников энергии.

2. Системы мониторинга и автоматизации: использование современных технологий для постоянного мониторинга и управления системами критической инфраструктуры.

3. Физическая защита: обеспечение безопасности объектов критической инфраструктуры с помощью систем видеонаблюдения, контроля доступа и охраны.

4. Кибербезопасность: применение мер для защиты от кибератак, включая использование надежных паролей, шифрования данных и регулярные проверки безопасности.

5. Планирование чрезвычайных ситуаций: разработка и внедрение планов действий для чрезвычайных ситуаций, которые могут возникнуть в критической инфраструктуре.

6. Сотрудничество и координация: обеспечение сотрудничества между различными организациями и государственными структурами для эффективного реагирования на чрезвычайные ситуации и восстановления работы критической инфраструктуры.

2.6. Симметричные и асимметричные криптосистемы

В симметричных криптосистемах для шифрования и расшифрования используется один и тот же ключ (рис.2.9.).



Рис.2.9. Схема симметричного шифрования

К **традиционным (классическим)** методам шифрования в симметричных криптосистемах относятся: шифры перестановки; шифры простой и сложной замены; некоторые их модификации и комбинации.

Комбинации шифров перестановок и шифров замены образуют все многообразие применяемых на практике симметричных шифров.

Шифры перестановки.

При шифровании перестановкой символы шифруемого текста переставляются по определенному правилу в пределах блока этого текста.

Шифры перестановки являются самыми простыми и, вероятно, самыми древними шифрами.

Пример: *шифрующие таблицы.*

В	У	Г	Р	Н	В	Е	С
Б	С	О	С	Ы	Е	Т	П
Е	С	С	Т	Й	Р	Т	О
Л	К	У	В	У	С	Р	Р
О	И	Д	Е	Н	И	А	Т
Р	Й	А	Н	И	Т	Н	А

Шифры простой замены.

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены.

В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита по одному правилу на всем протяжении текста.

Часто шифры простой замены называют шифрами одноалфавитной подстановки. Примеры шифров простой замены:

Система шифрования Цезаря

A → D	E → H	I → L	M → P	Q → T	U → X	Y → B
B → E	F → I	J → M	N → Q	R → U	V → Y	Z → C
C → F	G → J	K → N	O → R	S → V	W → Z	
D → G	H → K	L → O	P → S	T → W	X → A	

Шифры сложной замены.

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свой шифр простой замены. Примеры: Система шифрования Вижинера; Диски Альберти, Джефферсона; Одноразовые шифры.

Система шифрования Вижинера

Ключ	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
4	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
5	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
6	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
13	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
17	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
18	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
19	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
21	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
24	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
25	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y



Рис.2.10. Диски Альберти

Американский стандарт шифрования данных DES. Стандарт шифрования данных DES (Data Encryption Standard) опубликован в 1977 г. Национальным бюро стандартов США. Предназначен для защиты от несанкционированного доступа к **важной, но не секретной** информации в государственных и коммерческих организациях США. Алгоритм DES основан на комбинировании методов подстановки и перестановки и состоит из чередующейся последовательности блоков перестановки и подстановки. DES осуществляет шифрование 64-битовых блоков данных с помощью 64-битового ключа, в котором значащими являются 56 бит (остальные 8 бит – проверочные биты для контроля на четность). Расшифрование в DES является операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности. Обобщенная схема процесса шифрования в алгоритме DES показана на рисунке 2.11.

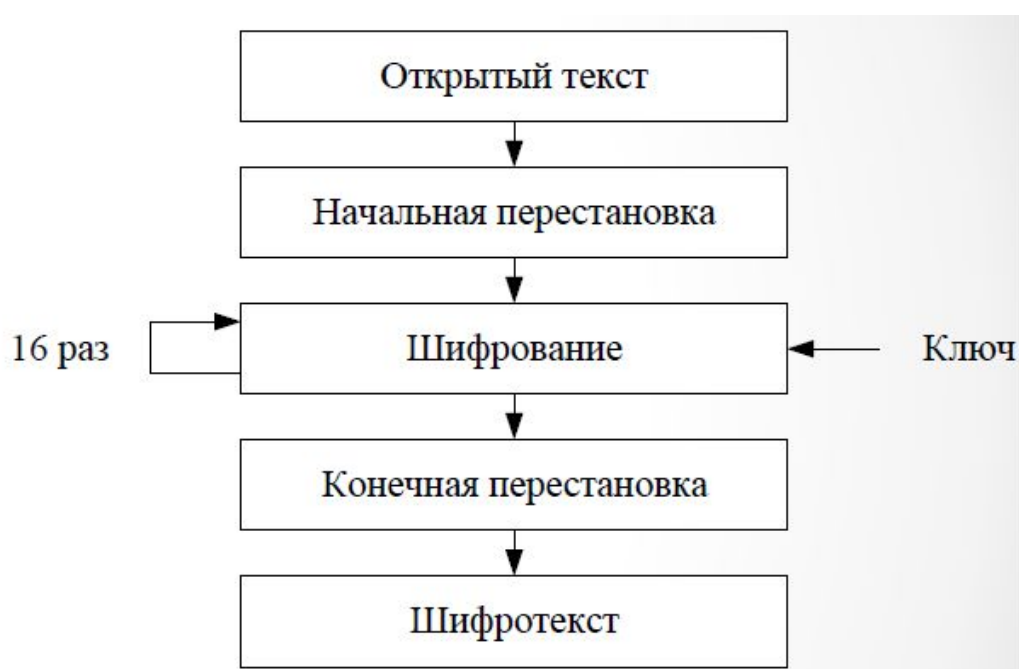


Рис. 2.11. Порядок шифрования в DES

Основные достоинства алгоритма DES: используется только один ключ длиной 56 бит; относительная простота алгоритма обеспечивает высокую скорость обработки; достаточно высокая стойкость алгоритма.

Чтобы воспользоваться алгоритмом **DES** для решения разнообразных криптографических задач, разработаны четыре рабочих режима: электронная кодовая книга **ECB (Electronic Code Book)**; сцепление блоков шифра **CBC (Cipher Block Chaining)**; обратная связь по шифротексту **CFB (Cipher Feed Back)**; обратная связь по выходу **OFB (Output Feed Back)**.

Стандарт шифрования данных (ГОСТ 28147-89). Алгоритм криптографического преобразования данных был разработан в СССР и опубликован в виде государственного стандарта ГОСТ 28147-89 в 1989 году.

Предназначен для аппаратной и программной реализации, удовлетворяет криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации. Алгоритм шифрования данных представляет собой 64-битовый блочный алгоритм с 256-битовым ключом.

Алгоритм предусматривает четыре режима работы: шифрование данных в режиме **простой замены**; шифрование данных в режиме **гаммирования**; шифрование данных в режиме **гаммирования с обратной связью**; **выработка имитовставки**.

В режиме **гаммирования** (<https://tech-geek.ru/gost-34-13/>) биты исходного текста складываются по модулю 2 с гаммой, которая вырабатывается с помощью алгоритма шифрования по ГОСТ 28147-89. То есть алгоритм шифрования по ГОСТ 28147-89 в данном **режиме** используется в качестве генераторов 64-разрядных блоков гаммы. При шифровании каждого нового блока данных гамма, использованная на предыдущем шаге, зашифровывается и используется уже как "новая" гамма. Перед шифрованием открытые данные разбивают на блоки одинаковой длины, обычно по 64 бита. Гамма шифра вырабатывается в виде последовательности аналогичной длины. Процесс расшифрования сводится к повторной генерации гаммы шифра и наложению этой гаммы на принятые данные.

В **асимметричных криптосистемах** используются два ключа – открытый и секретный, которые математически связаны друг с другом (рис.2.12). Первый ключ является открытым и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифрование данных с помощью открытого ключа невозможно.

Для расшифрования данных получатель зашифрованной информации использует второй ключ, который является *секретным*. Разумеется, ключ расшифрования не может быть определен из ключа зашифрования. Схема передачи данных между двумя субъектами (А и Б) с использованием открытого ключа выглядит следующим образом: Субъект А генерирует пару ключей, открытый и закрытый (публичный и приватный). Субъект А передает открытый ключ субъекту Б. Передача может осуществляться по незащищенным каналам. Субъект Б шифрует пакет данных при помощи полученного открытого ключа и передает его А. Передача может осуществляться по незащищенным каналам. Субъект А расшифровывает полученную от Б информацию при помощи секретного, закрытого ключа.

В такой схеме перехват любых данных, передаваемых по незащищенным каналам, не имеет смысла, поскольку восстановить исходную информацию возможно только при помощи закрытого ключа, известного лишь получателю и не требующего передачи.

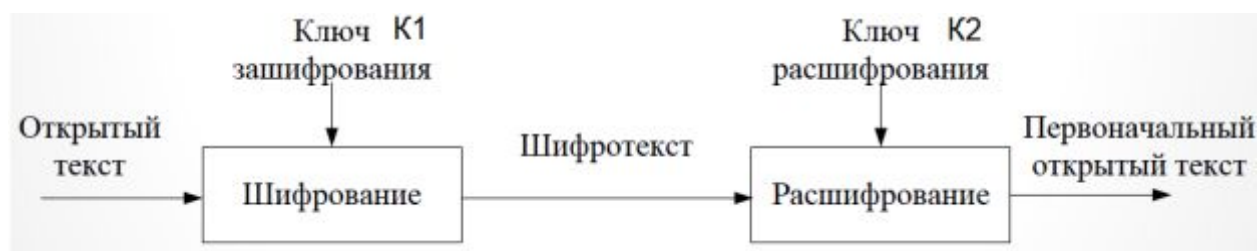


Рис.2.12. Асимметричная схема шифрования

В алгоритмах асимметричного шифрования используется схема обмена ключами Диффи — Хеллмана, изобретённая в 1976 году Уитфилдом Диффи и Мартином Хеллманом под влиянием работ Ральфа Меркле (*Ralph Merkle*), которая стала первым практическим методом для получения общего секретного ключа при общении через незащищенный канал связи. Годом позже был изобретен первый алгоритм асимметричного шифрования RSA, который решил проблему общения через незащищённый канал кардинально, уже не требуя, чтобы каждая сторона имела копию одного и того же секретного ключа.

Наиболее распространенные алгоритмы асимметричного шифрования:

RSA (аббревиатура от Rivest, Shamir и Adelman, фамилий создателей алгоритма) — алгоритм, в основе которого лежит вычислительная сложность факторизации (разложения на множители) больших чисел. Применяется в защищенных протоколах SSL и TLS, стандартах шифрования, например в PGP и S/MIME, и так далее. Используется и для шифрования данных, и для создания цифровых подписей.

DSA (Digital Signature Algorithm, «алгоритм цифровой подписи») — алгоритм, основанный на сложности вычисления дискретных логарифмов. Используется для генерации цифровых подписей. Является частью стандарта DSS (Digital Signature Standard, «стандарт цифровой подписи»).

Схема Эль-Гамала — алгоритм, основанный на сложности вычисления дискретных логарифмов. Лежит в основе DSA и устаревшего российского стандарта ГОСТ 34.10–94. Применяется как для шифрования, так и для создания цифровых подписей.

ECDSA (Elliptic Curve Digital Signature Algorithm) — алгоритм, основанный на сложности вычисления дискретного логарифма в группе точек эллиптической кривой. Применяется для генерации цифровых подписей, в частности для подтверждения транзакций в криптовалюте Ripple.

ВНИМАНИЕ!!! Секретность алгоритмов шифрования и аппаратной реализации не определяют стойкость криптосистемы

Стойкость криптосистемы определяется лишь секретностью ключа!!!!

Управление криптографическими ключами: генерация, хранение и распределение ключей

Как бы ни была сложна и надежна сама криптосистема, она основана на использовании ключей. Если для обеспечения конфиденциального обмена

информацией между двумя пользователями процесс обмена ключами тривиален, то в системе, где количество пользователей составляет десятки и сотни управление ключами, – это серьезная проблема.

Под ключевой информацией понимается совокупность всех действующих в системе ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации.

Управление ключами – информационный процесс, включающий в себя три элемента: генерацию ключей; накопление ключей; распределение ключей.

Откуда брать секретные ключи?

Доверенный курьер доставляет ключи из ключевого центра или ключи вычисляют при условии двухсторонней аутентификации

Генерация ключей. В реальных системах используются специальные аппаратные и программные методы генерации случайных ключей. Как правило, используют датчики случайных чисел. Однако степень случайности их генерации должна быть достаточно высокой. Идеальными генераторами являются устройства на основе “натуральных” случайных процессов. Например, генерация ключей на основе белого радишума. Другим случайным математическим объектом являются десятичные знаки иррациональных чисел, например π или e , которые вычисляются с помощью стандартных математических методов.

В системах со средними требованиями защищенности вполне приемлемы программные генераторы ключей, которые вычисляют случайные числа как сложную функцию от текущего времени и (или) числа, введенного пользователем.

Накопление ключей. Под накоплением ключей понимается организация их хранения, учета и удаления.

Поскольку ключ является самым привлекательным для злоумышленника объектом, открывающим ему путь к конфиденциальной информации, то вопросам накопления ключей следует уделять особое внимание.

Секретные ключи никогда не должны записываться в явном виде на носителе, который может быть считан или скопирован.

В достаточно сложной системе один пользователь может работать с большим объемом ключевой информации, и иногда даже возникает необходимость организации минибаз данных по ключевой информации. Такие базы данных отвечают за принятие, хранение, учет и удаление используемых ключей.

Каждая информация об используемых ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие ключевую информацию называются мастер-ключами. Желательно, чтобы мастер-ключи каждый пользователь знал наизусть и не хранил их вообще на каких-либо материальных носителях.

Очень важным условием безопасности информации является периодическое обновление ключевой информации в системе. При этом переназначаться должны как обычные ключи, так и мастер-ключи. В особо ответственных системах обновление ключевой информации необходимо производить ежедневно.

Вопрос обновления ключевой информации связан и с третьим элементом управления ключами – распределением ключей.

Распределение ключей. Распределение ключей – самый ответственный процесс в управлении ключами. К нему предъявляются два требования:

- оперативность и точность распределения;
- скрытность распределяемых ключей.

В последнее время заметен сдвиг в сторону использования криптосистем с открытым ключом, в которых проблема распределения ключей отпадает. Тем не менее распределение ключевой информации в системе требует новых эффективных решений.

Распределение ключей между пользователями реализуются двумя разными подходами:

1. Путем создания одного или нескольких центров распределения ключей. Недостаток такого подхода состоит в том, что в центре распределения известно, кому и какие ключи назначены, и это позволяет читать все сообщения, циркулирующие в системе. Возможные злоупотребления существенно влияют на защиту.

2. Прямой обмен ключами между пользователями системы. В этом случае проблема состоит в том, чтобы надежно удостовериться подлинность субъектов.

В обоих случаях должна быть гарантирована подлинность сеанса связи. Это можно обеспечить двумя способами:

1. Механизм запроса-ответа, который состоит в следующем. Если пользователь А желает быть уверенным, что сообщения, которые он получает от пользователя В, не являются ложными, он включает в посылаемое для В сообщение непредсказуемый элемент (запрос). При ответе пользователь В должен выполнить некоторую операцию над этим элементом (например, добавить 1). Это невозможно осуществить заранее, так как не известно, какое случайное число придет в запросе. После получения ответа с результатами действий пользователь А может быть уверен, что сеанс является подлинным. Недостатком этого метода является возможность установления, хотя и сложной, закономерности между запросом и ответом.

2. Механизм отметки времени. Он подразумевает фиксацию времени для каждого сообщения. В этом случае каждый пользователь системы может знать, насколько “старым” является пришедшее сообщение.

В обоих случаях следует использовать шифрование, чтобы быть уверенным, что ответ послан не злоумышленником и штампел отметки времени не изменен.

При использовании отметок времени встает проблема допустимого временного интервала задержки для подтверждения подлинности сеанса. Ведь сообщение с отметкой времени в принципе не может быть передано мгновенно. Кроме этого, компьютерные часы получателя и отправителя не могут быть абсолютно синхронизированы.

Для обмена ключами можно использовать криптосистемы с открытым ключом, используя тот же алгоритм RSA.

Но весьма эффективным оказался алгоритм Диффи-Хеллмана (рис.2.13), позволяющий двум пользователям без посредников обменяться ключом, который может быть использован затем для симметричного шифрования.

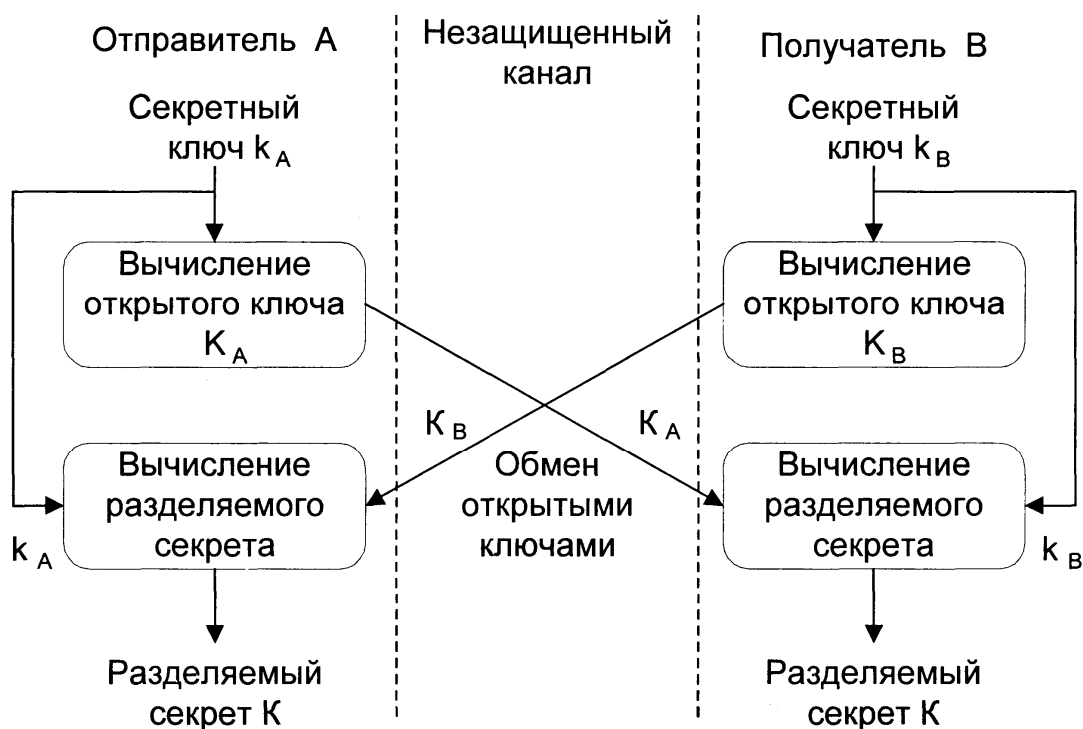


Рис.2.13. Схема алгоритма Диффи-Хеллмана

Проблемы всех классических механизмов распределения ключей: не обеспечивается безусловная секретность ключей; дорогостоящие организационно-технические меры; всегда есть «человеческий фактор»; создание квантового компьютера приведет к компрометации всех асимметричных криптографических алгоритмов и протоколов на их основе (DH, RSA, ECDSA TLS/SSL, HTTPS, IPsec, X.509).

Зачем нужна быстрая смена ключей?

Для конкретного алгоритма шифрования в конкретном режиме работы для конкретного варианта реализации СКЗИ имеется предельное количество данных, которые допустимо зашифровать на одном ключе – **нагрузка на ключ**.

Пример – Алгоритм блочного шифрования по ГОСТ 28147-89

- Размер блока $n = 64$
- Предельная теоретическая нагрузка $2^{64/2} = 2^{32}$ блоков шифротекста, или 256 Гбит данных
- Шифратор на скорости 10 Гбит/с израсходует ключ за 25 секунд.

2.7. Алгоритм шифрования с симметричным ключом, получивший наибольшее распространение

AES, или Advanced Encryption Standard, - это алгоритм шифрования с симметричным ключом. Это одно из самых универсальных и наиболее любимых технических решений в сфере криптографии.

В основе AES лежит блочный шифр, который использует 128-битный размер блока и 128, 192 или 256-битные ключи для шифрования данных. AES256 - это версия стандарта с 256-битными ключами. Этот стандарт широко считается самым безопасным стандартом цифровой криптографии, который обычно используется для наиболее надежной сквозной шифрованной связи на высоких скоростях передачи.

AES был разработан двумя бельгийскими криптографами: Джоаном Деменом и Винсентом Риджменом и был принят в качестве официального стандарта в 2001 году Национальным институтом стандартов и технологий США. Такое достижение свидетельствует о широком признании, которое получил стандарт. Уже более 20 лет AES256 и шифрование AES в целом является одним из наиболее предпочтительных решений для разработчиков, желающих создать систему, в которой коммуникации хорошо защищены от постороннего или внешнего влияния и утечек. Вот упрощенная схема того, как это работает.

Насколько безопасно шифрование AES-256?

Алгоритм AES пользуется высоким доверием и надежностью. Национальный институт стандартов и технологий высоко оценил AES, назвав его "невзламываемым", а правительство США использует его для защиты секретной информации с 2001 года.

Как и в любой технологии безопасности, всегда существуют потенциальные уязвимости, которые могут быть обнаружены и использованы в будущем. Однако на данный момент их нет. Существуют только уязвимости боковых каналов, но от них можно защититься, если разработчики программного обеспечения будут разумно и безопасно применять стандарт.

Как уже упоминалось ранее, AES имеет три различных *личности* (128, 192 и 256 бит). 256-битная версия имеет самый длинный ключ для шифрования, и поэтому хакер должен потратить больше всего времени, пытаясь расшифровать сообщение. Если вы хотите узнать, сколько усилий для этого требуется, то ни один обычный компьютер или даже квантовый компьютер не сможет сделать это за разумное время. Все еще не поняли масштаба? Ну, это 2^{256} . Это также намного больше, чем общее количество атомов (да, атомов) во всей наблюдаемой Вселенной. А только в вашем теле насчитывается около 7 октиллионов атомов (7×10^{27}). Масштабы колоссальны, и никакие современные технологии не в состоянии охватить этот масштаб.

Помимо количества возможных вариантов расшифровки, AES 256 также реализует 14 раундов шифрования. Таким образом, ключ для его расшифровки автоматически становится длиннее, чем при использовании других технологий

шифрования. Чем длиннее ключ, тем сложнее его взломать. Скорость также не является проблемой. Алгоритм Advanced Encryption Standard - AES не слишком требователен к оперативной памяти системы, поэтому он не сильно нагружает системы и серверы.

Если вы хотите узнать, сколько времени потребуется для взлома зашифрованного AES-256 содержимого - мы не можем точно сказать, что произойдет на практике, поскольку это еще не было сделано. Но теоретически для взлома потребуются миллиарды лет. Подходы к тому как выработать ключи шифрования различаются, но в общем это выглядит так как иллюстрируется на рис.2.14. На пути к новому, пятому поколению информационных систем, предпочтение в квантовой криптографии отдаётся симметричному шифрованию (рис.2.15).



Рис.2.14. Подходы к выработке ключей шифрования



Рис.2.15. Переход к пятому поколению информационных систем

Пример для алгоритма Диффи-Хеллмана (Diffie-Hellman, DH) формирования и распределения секретного ключа с использованием незащищенного канала.

1. Алгоритм Диффи-Хеллмана не применяется для шифрования сообщений или формирования электронной подписи. Его назначение – в распределении ключей.
2. Он позволяет двум или более пользователям обменяться без посредников ключом, который может быть использован затем для симметричного шифрования. Это была первая криптосистема, которая позволяла защищать информацию без использования секретных ключей, передаваемых по защищенным каналам.
3. Алгоритм построен на простой формуле: $A = G^a \bmod P$
4. В приведенном далее расчете, **модификация** означает операцию по модулю. По сути, это расчеты, чтобы **выяснить остаток** после деления левой части на правую.

В качестве примера: $15 \bmod 4 = 3$

Остаток от деления по модулю означает следующее: мы делим одно число на другое с остатком. Целую часть выкидываем, а остаток — это то, что нам нужно. Обозначается такое деление словом **mod**.

Например, $12 \bmod 5 = 2$, потому что $12 = 2 \times 5 + 2$

$13 \bmod 4 = 1$, потому что $13 = 4 \times 3 + 1$

$10 \bmod 2 = 0$, потому что $10 = 2 \times 5 + 0$

В криптографии деление по модулю применяется часто, потому что зная два исходных числа найти остаток очень легко, а вычислить первое число, зная второе и остаток — невозможно.

Если $X \bmod 5 = 1$, то X может быть равен 6, 11, 16, 21 и так далее — остаток от деления каждого из этих чисел по модулю 5 равен одному. Поэтому пересылать остаток от деления по модулю можно, а первое число — нет.

Итак, пусть Алиса и Боб решили обмениваться шифрованными сообщениями, но в их распоряжении имеется только незащищенный открытый канал связи, при этом никаких возможностей встретиться или передать секретный ключ через кого-нибудь другого у них нет. В соответствии с алгоритмом Диффи—Хеллмана для успешного решения задачи Алиса и Боб должны выполнить следующие действия.

Прежде всего они открыто договариваются о том, что будут использовать одностороннюю функцию $Y = D^x \bmod P$. Затем они договариваются о значениях параметров D и P . Пусть, например, они договорились, что $D = 7$ и $P = 13$, то есть функция имеет вид $Y = 7^x \bmod 13$. Еще раз подчеркнем, что в соответствии с алгоритмом Диффи—Хеллмана вся эта информация не является секретной, и даже если переговоры будут подслушаны Евой, это не даст ей возможности прочитать сообщения Алисы и Боба.

1	Алиса секретным образом выбирает произвольное число A (закрытый ключ Алисы)	Пусть, например, $A = 2$	Боб также секретно выбирает произвольное число B (закрытый ключ Боба)	Пусть, например, $B = 4$
2	Алиса вычисляет значение a односторонней функции Y , используя в качестве аргумента свое секретное число A : то есть $a = D^A \bmod P$ (открытый ключ Алисы)	$a = 7^2 \bmod 13 = 10$	Боб также вычисляет значение b односторонней функции Y , используя в качестве аргумента свое секретное число B : $b = D^B \bmod P$ (открытый ключ Боба)	$b = 7^4 \bmod 13 = 2401 \bmod 13 = 9$
3	Алиса посылает Бобу свой открытый ключ a	10	Боб посылает Алисе свой открытый ключ b	9
4	Алиса, получив от Боба число b , вычисляет по формуле $K = b^A \bmod P$ (разделяемый секретный ключ)	$K = 9^2 \bmod 13 = 81 \bmod 13 = 3$	Боб, получив от Алисы число a , вычисляет по формуле $K = a^B \bmod P$ (разделяемый секретный ключ)	$K = 10^4 \bmod 13 = 10000 \bmod 13 = 3$

2.8. Применение криптографии в каналах оптических сетей связи

2.8.1. Протокол IPsec

IPsec — это набор протоколов (protocol suite), созданный The Internet Engineering Task Force (IETF) для обеспечения безопасности в IPv4 и IPv6. IPsec стал стандартом реализации VPN-решений во всём мире, и его используют ведущие зарубежные и отечественные разработчики. IPsec имеет три протокола (англ. «sub protocols») (рис.2.16):

АН, Authentication Header (аутентификационный заголовок). Обеспечивает аутентификацию источника и контроль целостности пакета.

ESP, Encapsulating Security Payload (шифрование данных). Обеспечивает конфиденциальность и, опционально, аутентификацию источника контроль, целостности пакета.

IKE, Internet Key Exchange Protocol (протокол согласования ключей). Обеспечивает аутентифицированное согласование ключей.

АН и ESP — протоколы непосредственной защиты данных. Роль IKE совсем другая — он не занимается непосредственно защитой данных пользователя, но обеспечивает АН и ESP аутентифицированными ключами.



Рис.2.16. Набор протоколов IPsec

Основное назначение – для организации соединений виртуальных частных сетей VPN (Virtual Private Network). IPsec представлено серией стандартов RFC (RFC2401- RFC2412, Request for Comments – запрос на изменение), разработанных советом по архитектуре Интернета IAB (Internet Architecture Board) (рис.2.17).

Протоколы IPsec могут функционировать в двух режимах: транспортном и туннельном (рис.2.18). В транспортном шифруются (защищаются) только данные IP- пакета, а исходный заголовок сохраняется. Транспортный режим, как правило, используется для установления соединения между хостами, т.е. окончательными устройствами, предоставляющими услуги типа «клиент-сервер». Он может также использоваться между шлюзами для защиты туннелей, организованных каким-нибудь другим способом, например протоколом сеансового уровня (L5) L2TP (Layer 2 Tunnelling Protocol).

Т.о., L2 TP/IPsec — это тип протокола VPN, который сочетает в себе протокол туннелирования уровня 2 (L2TP) и протокол безопасности интернет-протокола (IPsec) для создания безопасного и зашифрованного соединения между двумя устройствами через Интернет.

В туннельном режиме шифруется весь исходный IP-пакет: данные, заголовок, маршрутная информация, а затем зашифрованный пакет вставляется в поле данных нового пакета (инкапсуляция). Туннельный режим может использоваться для подключения удалённых компьютеров к виртуальной частной сети или для организации безопасной передачи данных через открытые каналы связи между шлюзами.

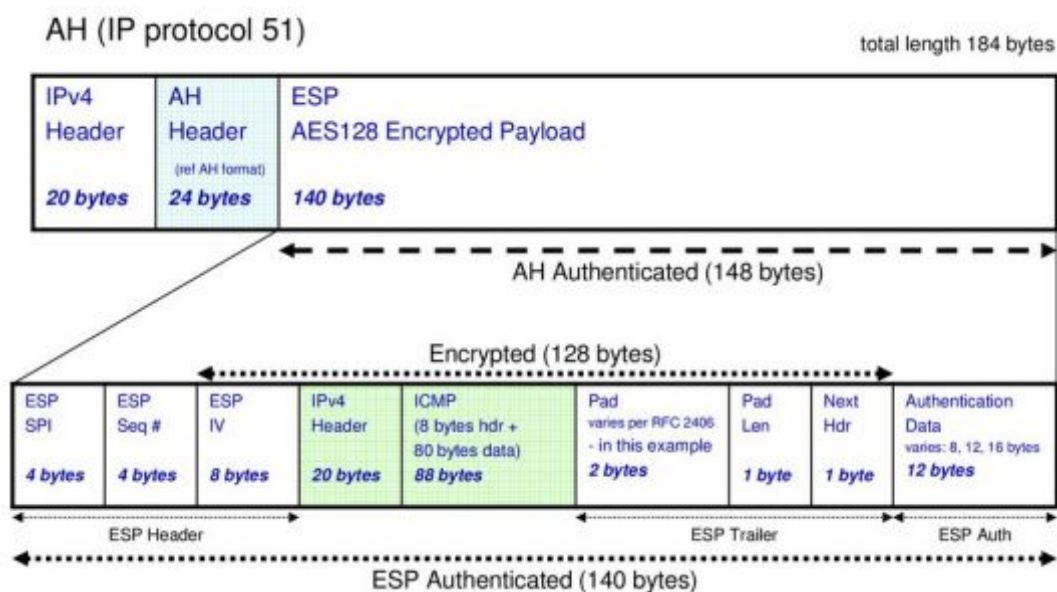


Рис.2.17. Пример структуры IP пакета с решением IP sec (AH, ESP)

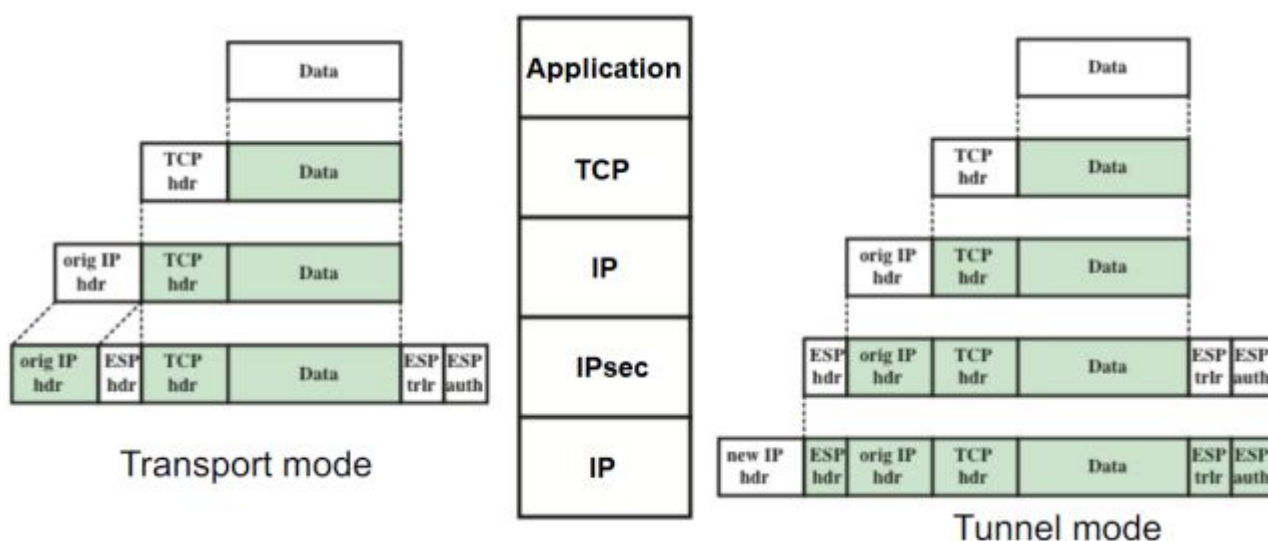
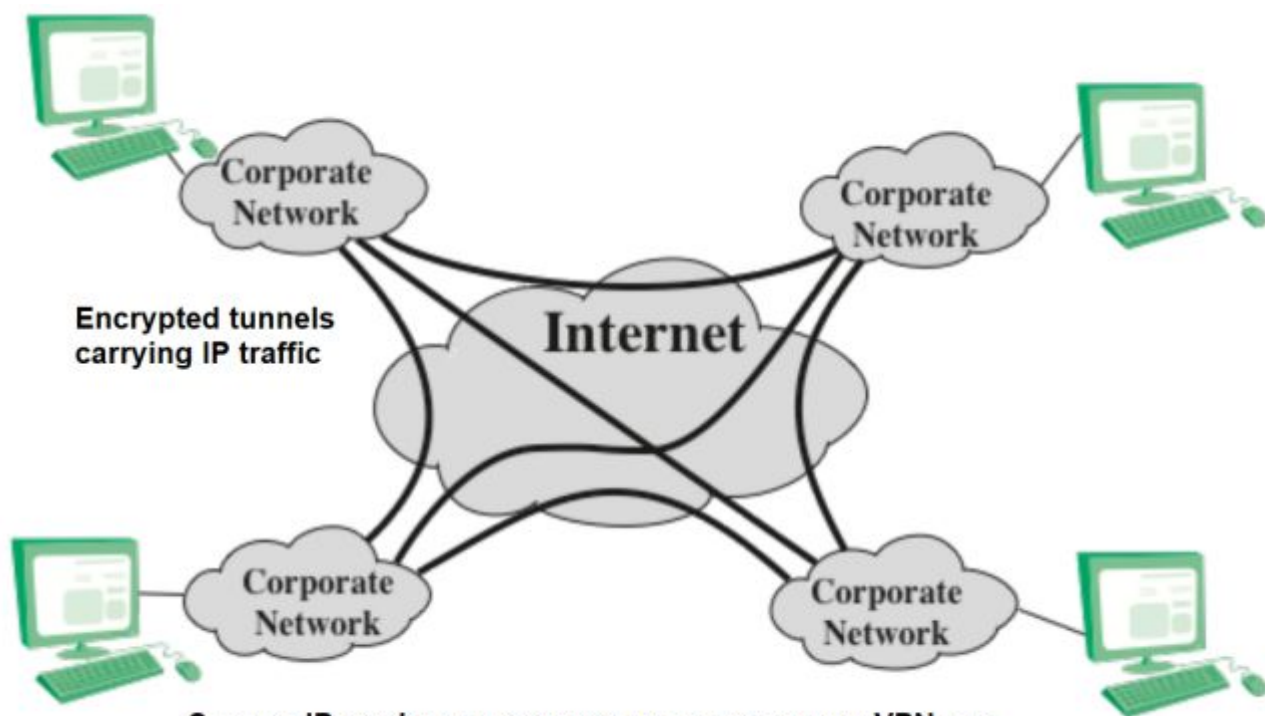


Рис.2.18. Транспортный и туннельный режимы протокола



Защита IP трафика в режиме туннелирования VPN для корпоративной сети

Рис.2.19. Пример схемы с защитой информации в туннельном режиме для корпоративной сети

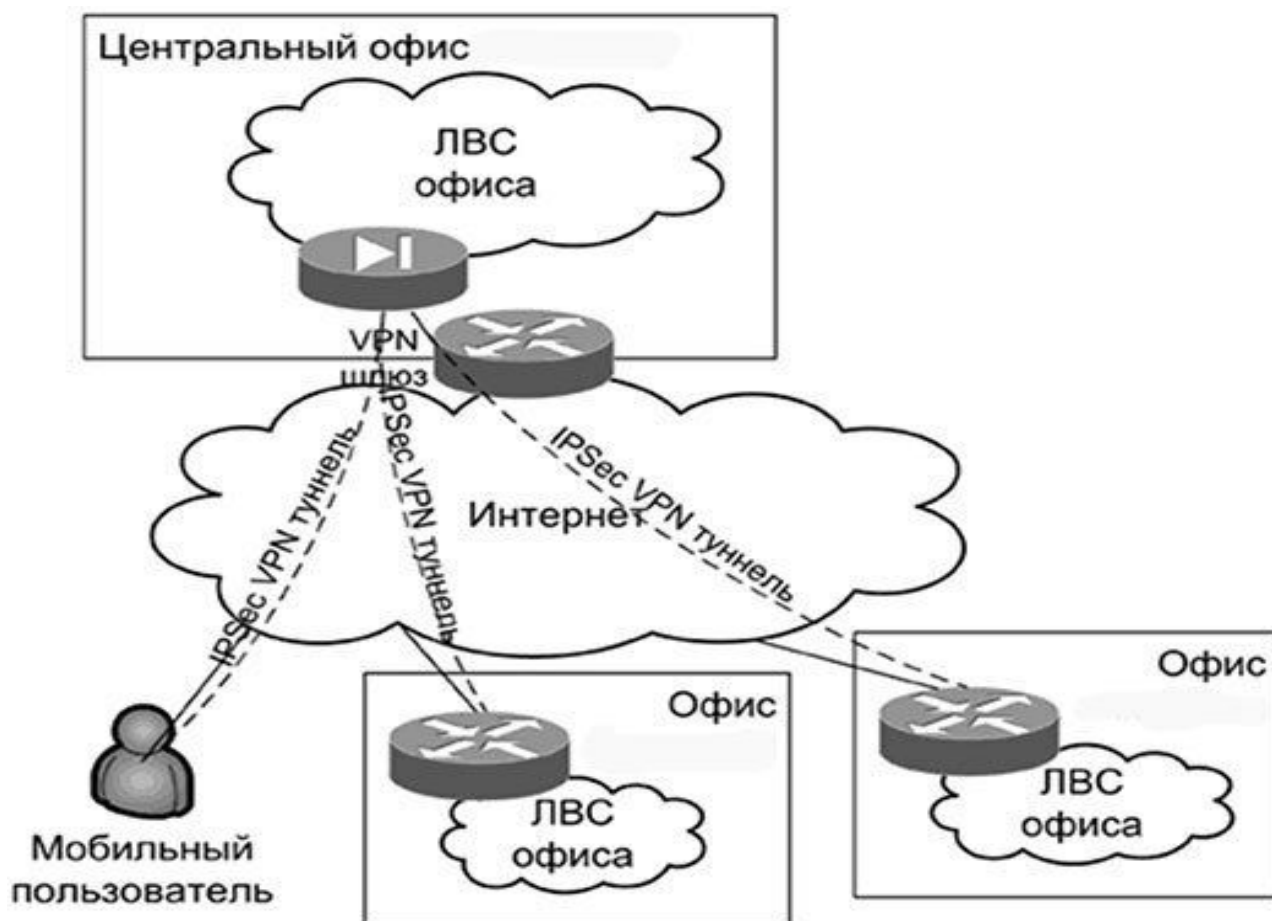


Рис.2.20. Пример схемы с защитой трафика в туннельном режиме с использованием шлюзов защиты

Обмен ключами шифрования поддерживает протокол Internet Key Exchange (IKEv2) protocol, базирующийся на алгоритме Diffie-Hellman (DH).

IKE или Internet Key Exchange - это протокол туннелирования на основе IPSec, который обеспечивает безопасный канал связи и определяет автоматические средства согласования и аутентификации для сопоставлений безопасности IPSec защищенным способом. Первая версия протокола (IKEv1) была представлена в 1998 году, а вторая (IKEv2) вышла 7 лет спустя. Между IKEv1 и IKEv2 существует ряд различий, одним из которых является уменьшение пропускной способности IKEv2.

IKE обеспечивает взаимную аутентификацию сторон и организует защищенную связь IKE (SA), включающую общую секретную информацию, которая может использоваться для эффективной организации защищенных связей для ESP или AH, а также задаёт набор криптоалгоритмов, который будет использоваться защищенными связями для передачи трафика между сторонами.

Возможности протокола IKEv2 VPN:

256-битное шифрование данных;

реализация IPSec для обеспечения безопасности;

стабильное и согласованное соединение;

поддержка MOBIKE (протоколы для мобильных и многосетевых устройств) для обеспечения лучшей скорости.

Безопасность. IKEv2 использует проверку подлинности сертификата сервера, что означает, что он не будет выполнять никаких действий, пока не определит личность запрашивающей стороны. Благодаря этому количество атак «человек посередине» и DoS атак значительно уменьшается.

Надежность. В первой версии протокола, при подключении к другому интернет соединению при включенном VPN, например, при переходе с домашней Wi-Fi сети к мобильному интернету, требовалось переподключение. Это имело некоторые нежелательные последствия, такие как снижение производительности и изменение предыдущего IP адреса. В версии протокола IKEv2, эта проблема была исправлена. В IKEv2 VPN протоколе реализована технология MOBIKE, которая позволяет использовать этот протокол мобильным и много сетевым пользователям.

Скорость. Продуманная архитектура и эффективная система обмена сообщениями протокола IKEv2 обеспечивают лучшую производительность.

IKEv2 работает в два этапа.

На первом этапе два устройства устанавливают безопасный канал, используя протокол Internet Security Association и Key Management Protocol (ISAKMP). На втором этапе два устройства согласовывают параметры туннеля IPsec, включая алгоритмы шифрования, методы аутентификации и группы Диффи-Хеллмана.

Обмен IKEv2.

IKEv2 использует серию обменов для установления и поддержания безопасного канала между двумя устройствами.

Обмены включают в себя:

Инициатор отправляет предложение: инициатор отправляет ответчику предложение, которое включает в себя используемые алгоритмы шифрования и аутентификации.

Ответчик отправляет предложение: ответчик отправляет инициатору предложение, включающее собственные алгоритмы шифрования и аутентификации.

Обмен Диффи-Хеллмана: два устройства обмениваются открытыми ключами Диффи-Хеллмана, чтобы установить общий секрет.

Обмен аутентификацией: два устройства аутентифицируют друг друга, используя выбранный ими метод аутентификации.

Создание туннеля IPsec: два устройства создают туннель IPsec, используя согласованные параметры.

ПРЕИМУЩЕСТВА IKEv2

- Одним из ключевых преимуществ IKEv2 является его способность поддерживать несколько ключей шифрования, включая 256-битное шифрование. Это гарантирует, что данные, передаваемые через VPN, защищены надежным шифрованием и не подвержены перехвату или прослушиванию.
- IKEv2 также использует сертификаты X.509 для аутентификации, либо предварительно общие, либо распространяемые с помощью DNS, и обмен ключами Диффи-Хеллмана для установки безопасного канала между клиентом и сервером. Это гарантирует, что доступ к VPN предоставляется только авторизованным пользователям, а все передаваемые данные зашифрованы и защищены.

Дополнительные возможности протокола IKE рассмотрены в документах:

RFC4555, IKEv2 Mobility and Multihoming Protocol (MOBIKE).

RFC6311, Protocol Support for High Availability of IKEv2/IPsec.

RFC5685, Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2).

RFC5723, Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption.

RFC6290, A Quick Crash Detection Method for the Internet Key Exchange Protocol (IKE).

2.8.2. Протокол MACsec

Протокол MACsec описывается стандартом IEEE802.1AE и служит для шифрования пакетов между двумя совместимыми устройствами. Шифруется весь поток данных, скрыт отправитель и получатель, порты их приложений, а так же вся служебная информация (рис.2.21). Здесь предусмотрена возможность шифрования с использованием ключа МКА (MACsec Key Agreement), как между коммутаторами (Switch-to-Switch), так и между коммутатором и конечными устройствами (Switch-to-Client). Это обеспечит шифрование трафика на L2 уровне при помощи алгоритма AES-128 или AES-256.

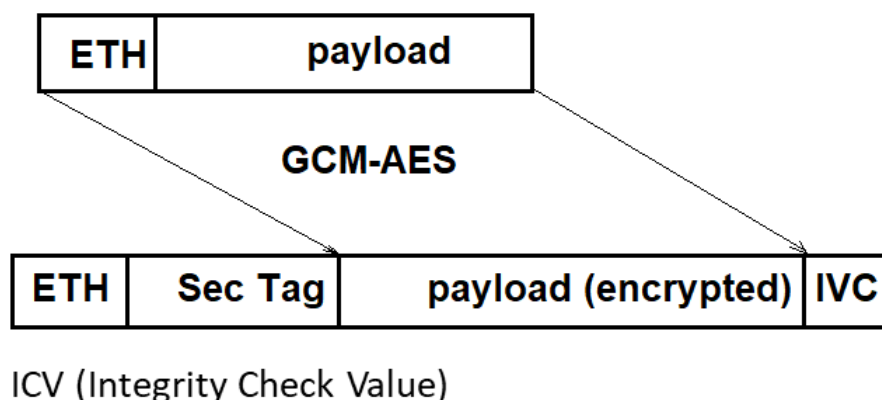


Рис.2.21. Шифруемая часть кадра Ethernet

Большой плюс этого решения в том, что криптография происходит на **аппаратном уровне**, и ресурсы процессоров сильно экономятся. Алгоритм GCM-AES (Galois/Counter Mode - Advanced Encryption Standard) один из самых универсальных и популярных алгоритмов шифрования с симметричным ключом в сфере криптографии. В его основе лежит блочный шифр, который использует 128-битный размер блока и 128, 192 или 256-битные ключи для шифрования данных. AES 256 - это версия стандарта с 256-битными ключами. Этот стандарт широко считается самым безопасным стандартом цифровой криптографии, который обычно используется для наиболее надежной сквозной шифрованной связи, в том числе для высокоскоростных оптических каналов.

Стандарт 802.1AE определяет реализацию MAC Security Entities (SecY), которую можно рассматривать как часть станций, подключенных к той же локальной сети, обеспечивающую защищенное MAC обслуживание клиента.

Стандарт определяет:

Формат фрейма (кадра) MACsec, который похож на Ethernet-фрейм, но включает в себя дополнительные поля (рис.2.22):

Метка безопасности, которая является расширением поля EtherType 16 байт MACsec tag (SecTAG)

- Код проверки подлинности сообщения (Message authentication code, ICV) 16 байт Integrity Check Value (ICV)

Ассоциации защищённого подключения (Security Connectivity Associations), которые представляют собой группы станций, подключенных через однонаправленные защищённые каналы (Secure Channels).

Ассоциации защиты (Security Associations) в пределах каждого канала. Каждое объединение использует свой ключ (SAK). Допускается больше одного соединения в контексте одного канала в целях внесения ключевого изменения без прерывания трафика (стандарт требует от устройства поддержку как минимум двух объединений).

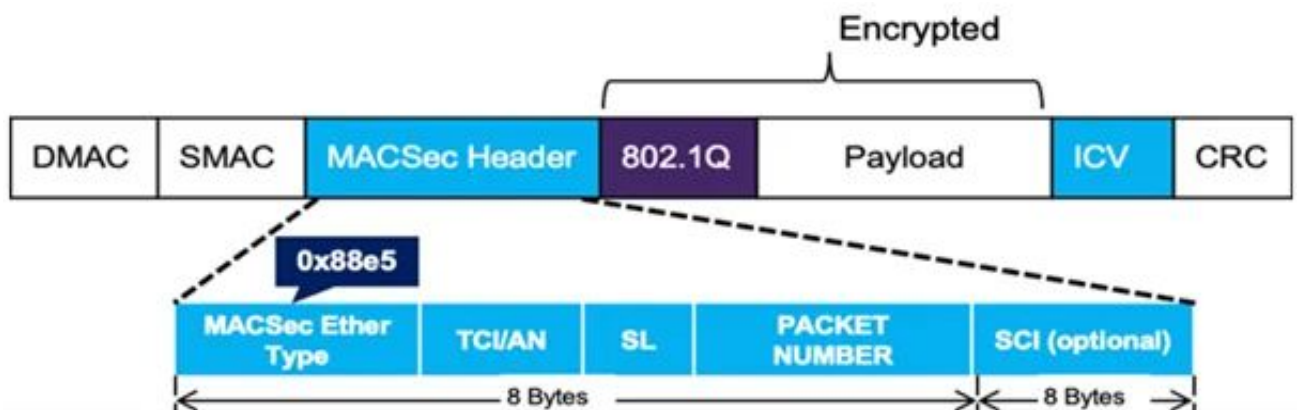


Рис.2.22. Структура кадра Ethernet с полем MACsec

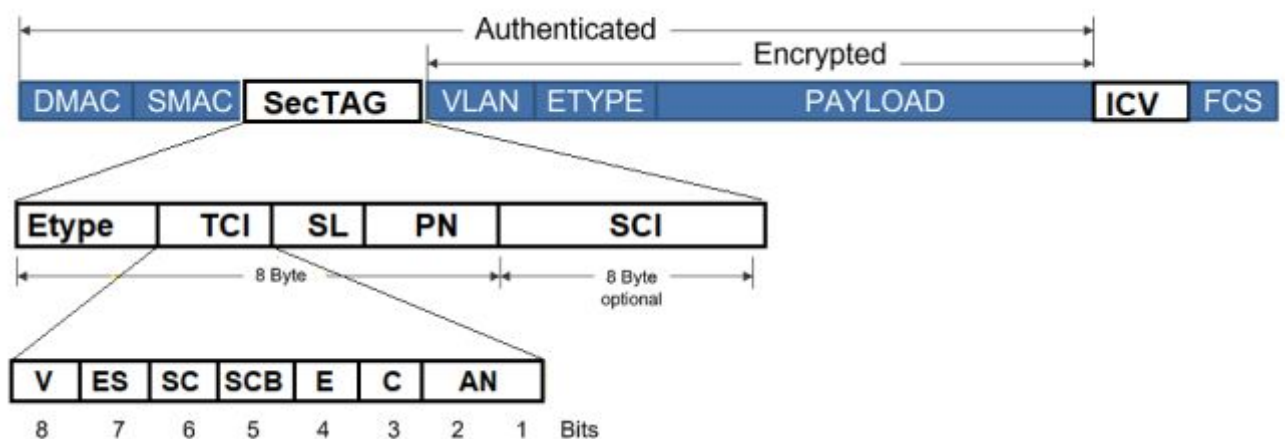


Рис.2.23. Детализация метки TCI

ETYPE – The MACsec Ethertype is 2 bytes long, like the normal Ethertype field. But it has a fixed value of 0x88e5 to indicate that this frame is a MACsec frame. Указание на тип протокола Ethernet и фиксированная индикация принадлежности кадра MACsec.

TCI – Is a 1 byte field of TAG Control Information (TCI) that contains several pieces of information. Version number (V), End Station (ES), SCI present (SC), Single Copy Broadcast (SCB), Encrypted payload (E), Changed Text (C), and Association

Number (AN). Байт метки информации управления с номером версии, конечной станции, представлением в настоящем, простой копией расширения, типом кодирования нагрузки, изменённым текстом и номером ассоциации.

SL – Is indicating a short length frame; the field is 6 bits long and indicates the bytes between the last byte of the SecTAG and the first byte of the ICV, if that number is less than 48. Otherwise, SL is set to zero. The bit 7 and 8 of this byte is always zero.

Индикатор длины кадра. 7 и 8 биты всегда ноль.
PN – The Packet Number (4byte) is mainly used to protect against replay attacks. In each MACsec frame the PN is unique, usually an increasing number. The PN is also used as Initial Value (IV) for the Cipher Suite. Номер пакета в 4 байта используется для исключения атак изменения. Каждый кадр MAC sec имеет нарастающий уникальный номер.

SCI – The 8 byte secure channel identifier can be used to identify to which security association the traffic belongs. 8 байт используются для безопасности идентификатора канала, который принадлежит к безопасной трафиковой группе.

ICV – The integrity check value is attached to each MACsec frame and ensures the integrity of data. The length of ICV depends on Cipher Suite and is between 8 to 16 bytes. Интегрированная метка в каждом кадре MAC sec указывает на целостность данных кадра в объёме от 8 до 16 байт.

На рис.2.24 представлены графики, показывающие ограничение для использования IP sec и преимущество MAC sec при увеличении скорости передачи в оптическом канале.

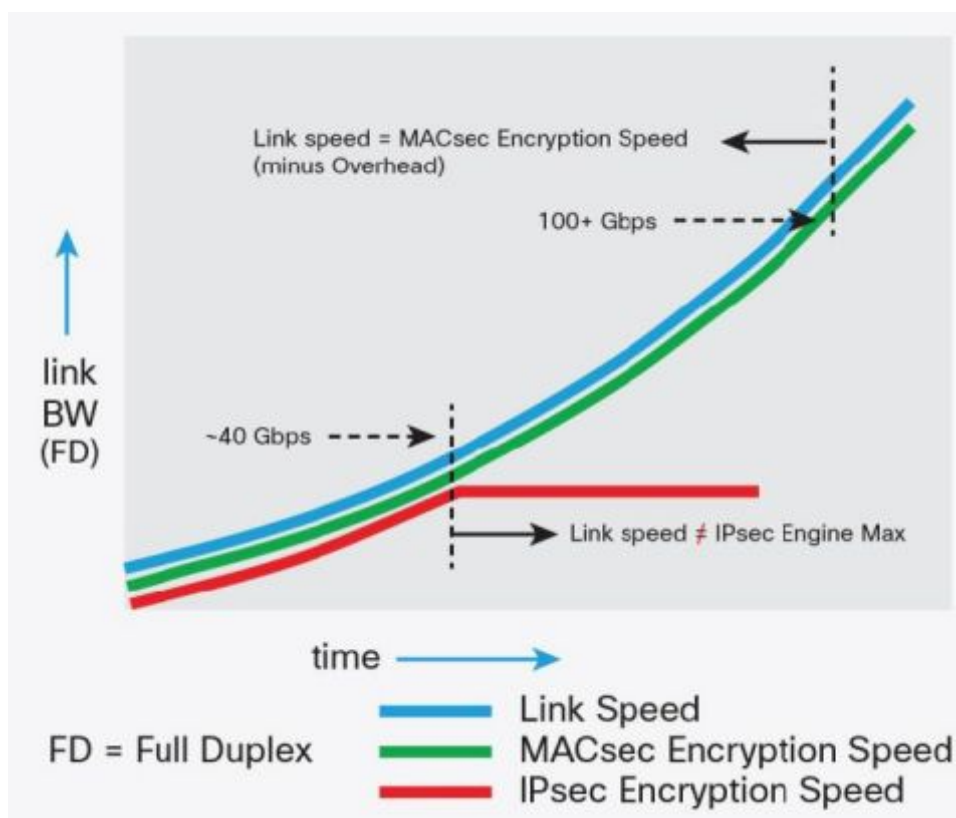


Рис.2.24. Зависимость скорости передачи зашифрованного трафика от применяемой технологии IPsec и MACsec

Проблемы использования криптозащиты информации на уровнях L2/L3.

Шифрование на L2 может быть реализовано в разных режимах передачи. В транспортном режиме защищается только поле данных, а заголовки остаются незашифрованными, поэтому кадры можно передавать через коммутируемую сеть, а накладные расходы (избыточность) из-за шифрования остаются умеренными. В туннельном режиме кадр целиком шифруется и инкапсулируется в блок данных другого пакета, в том числе и более высокого уровня (например, UDP), благодаря чему можно маршрутизировать зашифрованный на L2 трафик через IP-сеть (правда, и накладные расходы из-за дублирования заголовков здесь велики, и особенно это заметно на коротких кадрах).

У шифрования на L2 есть два основных преимущества. Во-первых, так как полностью шифруются не только собственно пользовательские данные, но и вся адресная и служебная информация протоколов L3 и выше (а иногда и самого L2), злоумышленникам сложнее вскрыть структуру сети и реализовать атаки. Во-вторых, его можно применять там, где конечным узлам (станциям) сети нужна связность на L2, по MAC-адресам и EtherType — например, для инфраструктуры виртуальных машин или для «растягивания» VLAN между площадками. Вот почему для всех основных сценариев межсайтового шифрования (защита каналов между ЦОДами, подключение к коммерческому ЦОДу, связь между филиалами) есть большая потребность в шифровании на L2, но до последнего времени предложение отставало от спроса.

Источник: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-L2-encryption-devices-for-Ethernet-networks

При использовании L2- / L3-устройств для защиты данных в оптических каналах существует ряд проблем:

- снижение пропускной способности (высокие накладные расходы на шифрование);

- низкая скорость шифрования (не поддерживается шифрование на скорости линии);

- негативное влияние на характеристики и качество сети (вносимая задержка и её изменение (вариация), потери пакетов и кадров);

- отсутствие приоритета шифрования трафика между сервисами;

- вносение изменений в служебную информацию (влияние на QoS, trunk);

- влияние на архитектуру сети при интеграции в неё устройств шифрования.

2.8.3. Практическая реализация IPsec и MACsec

На рис.2.25 представлена **блок-схема микросхемы BCM85344 Dual 800G MACsec/IPsec Retimer PHY** с поддержкой функций IP sec, MAC sec, FEC и восстановлением синхронизации для скоростей от 100 Гбит/с до 800 Гбит/с Ethernet.

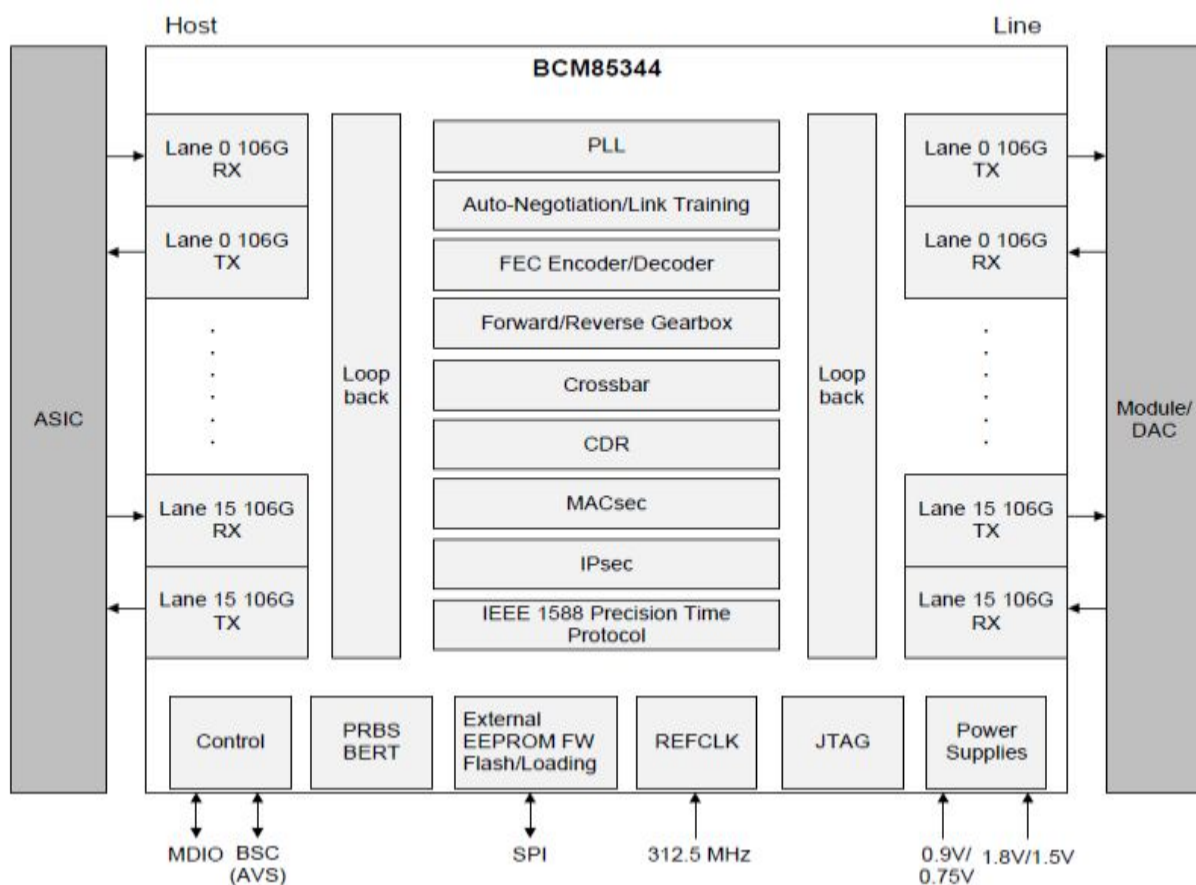


Рис.2.25. Блок-схема микрочипа BCM85344 Dual 800G MACsec/IPsec Retimer PHY

Сокращения в обозначениях для схемы BCM85344:

CDR, clock and data recovery, восстановление тактов и данных

PRBS, pseudorandom binary sequence, псевдослучайная последовательность

BERT, bit error rate tester, тестирование ошибок

JTAG, Joint Test Action Group; произносится «джей-таг» — название рабочей группы по разработке стандарта IEEE 1149. JTAG - это аппаратный интерфейс для программирования, тестирования и отладки печатных плат.

PLL, phase-locked loop or phase lock loop (PLL), автоподстройка по тактовой частоте

ASIC, application-specific integrated circuit, специализированная интегральная схема

DAC, Direct Attached Cable модуль с форм-фактором SFP+, работающий по стандарту 10GBASE.

Программно-аппаратный комплекс ViPNet L2-10G – шлюз безопасности, который обеспечивает шифрование данных в канале Ethernet (темная оптика, MAN, WAN, выделенный канал). ViPNet L2-10G обладает высокой производительностью и сверхнизкой задержкой, обеспечивая защиту без снижения пропускной способности канала, что является идеальным решением для реализации защиты IT-сервисов, а также эффективным средством защиты каналов связи между сегментами IT-инфраструктуры.

(<https://infotecs.ru/resheniya/zashchita-vysokoskorostnykh-kanalov-svyazi.html>)

Производительность:

сверхнизкая задержка - менее 3 мкс;

скорость шифрования трафика - 20 Гбит/с (10 Гбит/с Ethernet в режиме дуплекс);

минимальная избыточность протокола – не более 12 байт на один Ethernet-кадр

Прозрачность для любых сервисов:

прозрачен для сетевых протоколов и приложений;

поддерживает Unicast, Multicast и Broadcast трафик.

Защищенность:

специализированная аппаратная платформа в корпусе 1U, предусматривающая защиту от вскрытия;

энергонезависимое уничтожение ключевой информации при вскрытии корпуса или по команде оператора;

шифрование с использованием алгоритмов регламентированных ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015; соответствует требованиям ФСБ России к СКЗИ класса КВ; готовность к работе с аппаратурой квантового распределения ключей шифрования.

Сценарии использования

Высокоскоростные шифраторы используются для защиты каналов связи, требующих исключить влияние защиты на скорость передачи данных, таких как:

магистральных каналов между ЦОДами;

каналов связи операторского уровня транспортных сетей.

ViPNet L2-10G может также применяться для высокопроизводительного шифрования потока данных в «облачных» технологиях при переносе IT-инфраструктуры в виртуальную среду.

2.8.4. Криптографическая защита в модулях транспондеров и мукспондеров оптических каналов транспортной сети OTUsec

Преимущества использования шифрования данных уровня L1 в каналах оптической транспортной сети OTN/OTH (ODU2, 4) для нагрузки со скоростью 10 Гбит/с и 100 Гбит/с в поле OPU2, OPU4 представлены на рис.2.26. На рис.2.27 указано место размещения схемы шифрования в оборудовании OTN.

Шифрование	IP sec	MAC sec	ODU sec
Уровень	Уровень 3 (IP)	Уровень 2 (Eth)	Уровень 1 (OTN)
Высокая производительность и низкая цена	×	✓	✓
Малое время ожидания	×	✓	✓
Заголовок протокола	Большой	Малый	Нет
Мультипротокольность	×	×	✓

ODU sec

ODU Payload (Data Plane) Encryption

- AES-256-GCM (256-bit key, Galois/Counter Mode)
- Encryption of ODU4 payload (OPU4) and ODU2 payload (OPU2)

Рис.2.26. Преимущество шифрования клиентского трафика на уровне L1



Рис.2.27. Транспондер/мукспондер с функцией шифрования L1

Преимущества использования шифрования данных в каналах оптической транспортной сети OTN Encryption при сравнительной оценке задействованных ресурсов MACsec и IPsec представлено рис.2.28.

В мире для защиты оптических каналов уже давно применяются устройства класса L1 Services Encryption. Перемещение криптографической защиты с уровней L2 / L3 на более низкий уровень L1 приводит ко предельно малому влиянию функциональности информационной безопасности на ИТ-сервисы. Для передачи данных по оптическим линиям с использованием протокола OTN L1-

шифраторы упаковывают их в специальные блоки протокола (OTUsec, ODUsec), одновременно зашифровывая. За счёт этого удаётся существенно уменьшить время затрачиваемое на шифрование данных. После передачи блоки распаковываются и расшифровываются L1-шифратором на приёмной стороне. В данном случае защищается весь направляемый в транспортную сеть трафик, включая служебную информацию вышестоящих протоколов без их изменения.

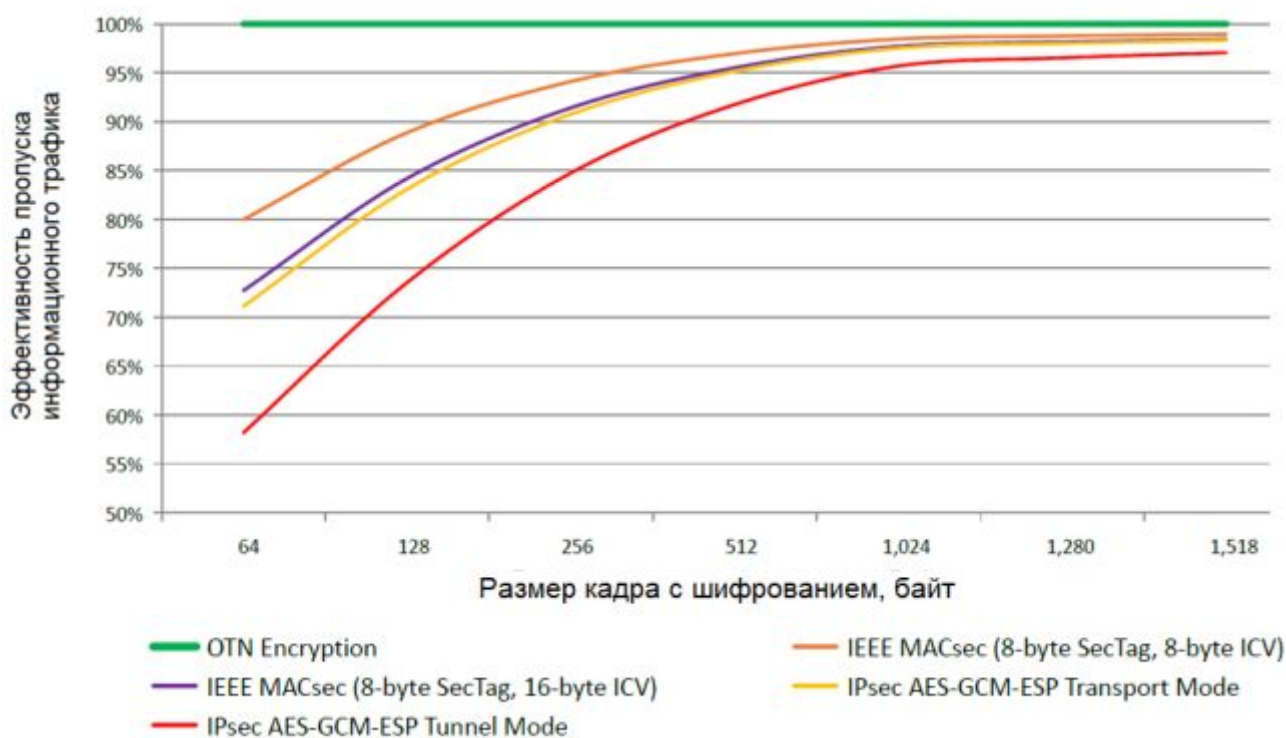


Рис.2.28. Эффективность пропуска информационного трафика в каналах оптических транспортных сетей в зависимости от размера кадра шифрования

Согласно выше представленным графикам устройствам класса L1 Services Encryption свойственны максимальная и независимая от размера пакетов пропускная способность, сверхнизкая вносимая оборудованием задержка (не зависит от загрузки канала), альтернативное соединение (для соединяемого оборудования такой канал полностью прозрачен).

При этом криптографические средства уровня L1 не стоит рассматривать в качестве конкурентов тем, которые работают на уровнях L2 / L3, поскольку у каждого из этих типов своё целевое предназначение. Устройства класса L1 Services Encryption эффективны при построении оптических каналов связи высоких скоростей передачи.

В рекомендации МСЭ-Т Sup.76 (12/2021) по защите оптических транспортных сетей OTN/OTN представлены рекомендуемые сетевые решения по защите информационного трафика пользователей оптических каналов в вариантах с использованием средств шифрования клиентов и операторов транспортных сетей. При этом допускается использование одной или двух инстанций шифрования OTN sec и клиентского шифрования уровня MAC sec (рис.2.29).

Шифрование разделяется для OTN sec на два варианта использования: в структуре ODU sec J с разделением нагрузки клиента по отдельным блокам ODUCn для структуры гибкого оптического мультиплексирования n x FlexOsec и в отдельном блоке ODUsec ODUk (k=2, 4) (рис.2.30).

Для поддержки обмена ключей шифрования используется протокол IKEv2 с датаграммой передачей PPP(point-to-point protocol) данных в отдельной сети передачи данных или в каналах GCCn (n=1,2), размещаемых в заголовках ODUk (рис.2.31). Повторяемость обмена ключами шифрования от 30 секунд до 14 суток. Для кодирования информационной нагрузки в блоках OPUk применяется AES 256-bit Galois-Counter-Mode (GCM). Структура кадра OTUk/ODUk представлена рис. 2.32.

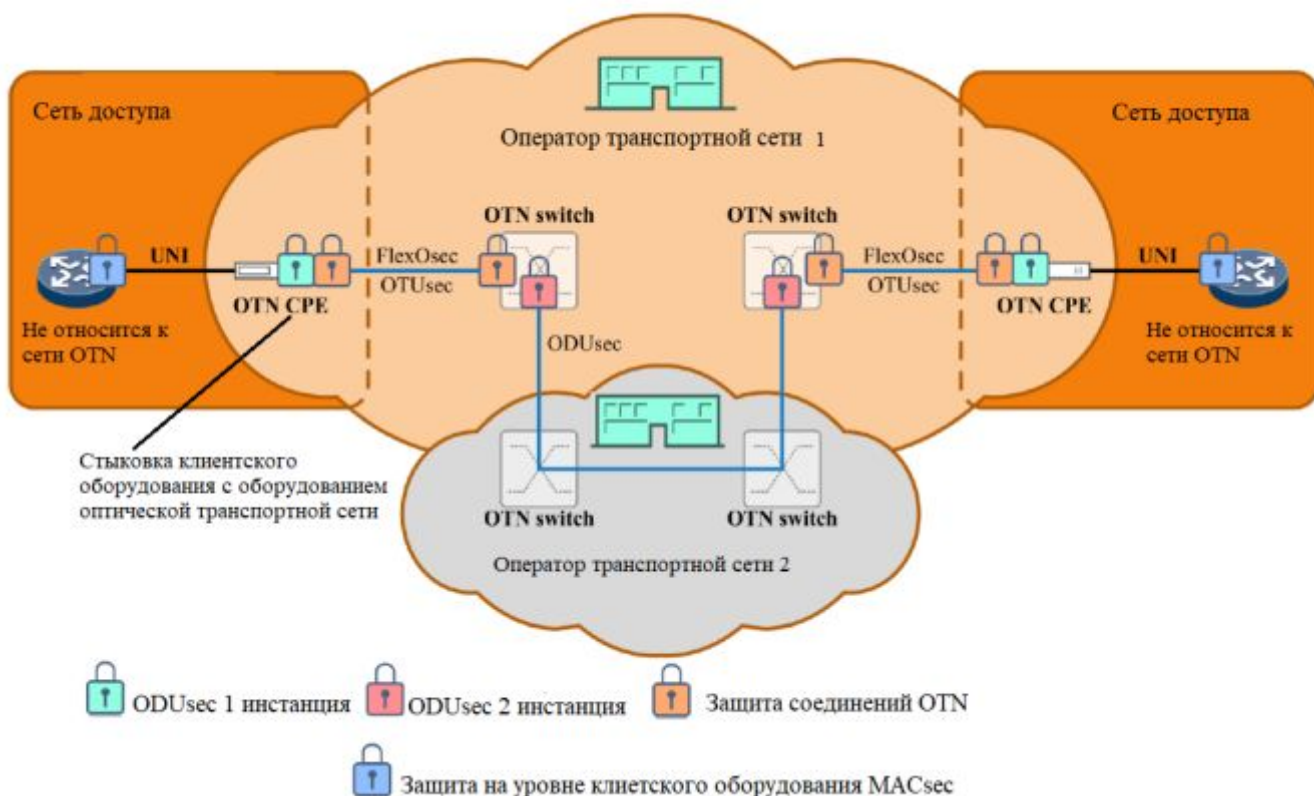


Рис.2.29. Структура транспортной сети с участками шифрования

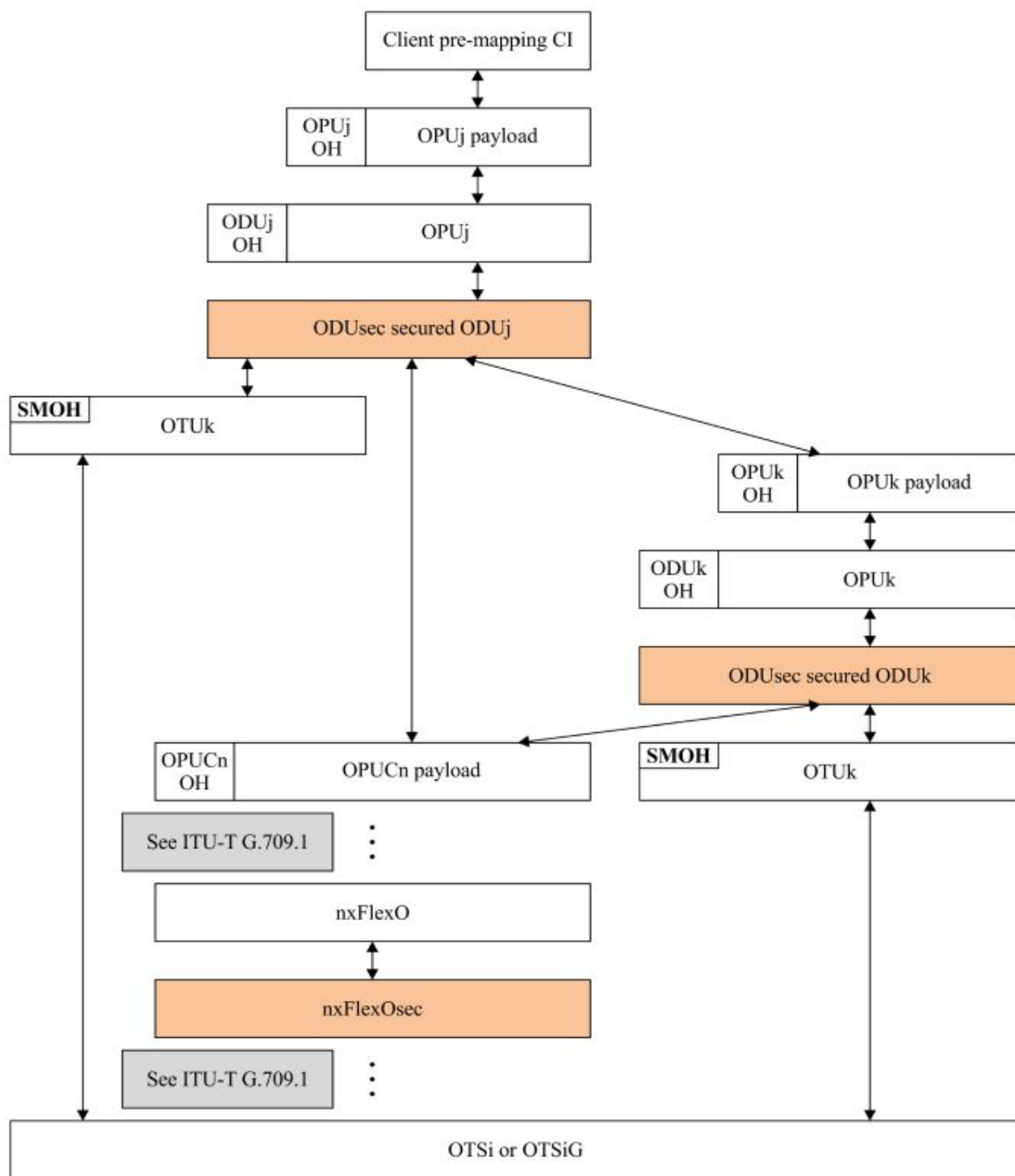


Рис.2.30. Варианты мультиплексирования информационной нагрузки клиента в защищаемый оптический канал сети OTN/OTN по рек. G.709.1

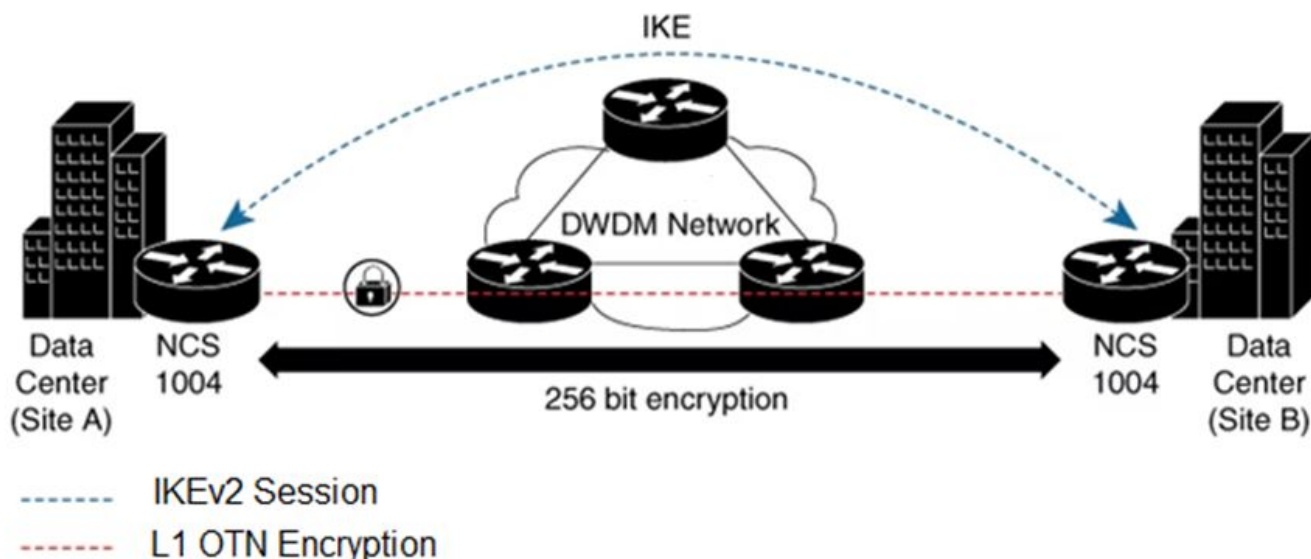


Рис.2.31. Схема взаимодействия по обмену ключами шифрования IKEv2 в канале оптической сети с оборудованием NCS 1004 (Cisco)

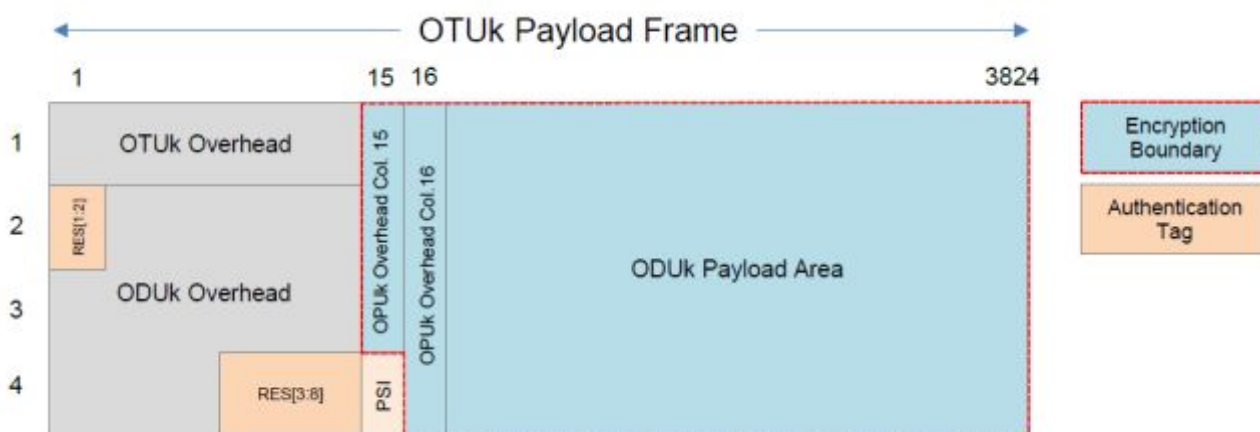


Рис.2.32. Структура кадра OTUk с шифруемым полем нагрузки OPUk и метками опознавания шифрования (Tag) и идентификации AAD

В последовательности кадров OTUk создаётся криптопакет с четырьмя полями: TAG, Encrypted OPU, ADD, IV. Порядок формирования меток представлен на рис.2.33.

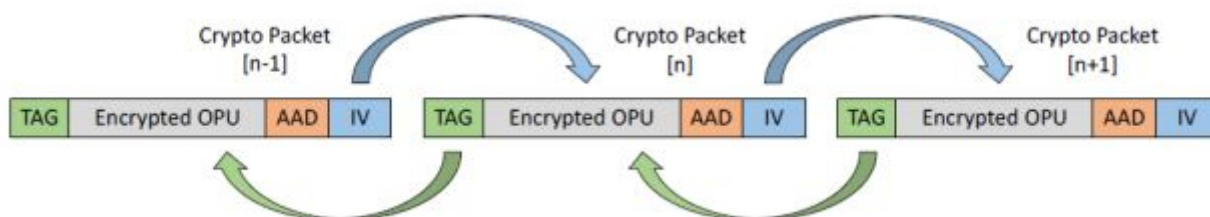


Рис.2.33. Криптопакет с четырьмя полями: TAG, Encrypted OPU, ADD, IV

Обозначение полей меток, ёмкость в байтах и исполнение (HW, аппаратное, SW, программное):

Field	Description	Size (byte)	Managed by
TAG	Message Authentication Code (MAC)	16	HW
AAD	Additional Authenticated Data	4	SW
IV	CSKS – Crypto Session Key Selection	1	SW/HW
	CSID – Crypto Session ID	4	SW
	CBID – Crypto Block ID	4	HW
	CPID – Crypto Packet ID	3	HW

AUTHENTICATION TAG, опознавательный признак –поле TAG соответствует кодексу установления подлинности сообщения (MAC), произведённого алгоритмом AES-GCM и используется приёмником. Передаётся изначально для сокращения времени ожидания-хранения-отправления в течении опознавательного процесса.

AAD, дополнительные заверенные данные 4 байта, включаемые в криптопакет. Используется оператором транспортной сети для передачи информации о мониторинге, наличии или отсутствии шифрования.

IV, вектор инициализации, построенный на основе двух полей: установления и обращения. Необходимо для выбора ключа шифрования.

Crypto Session Key Selection (CSKS), выбор ключа шифрования сессии вместе с CSID образуют пакет шифрования с уникальной различимостью в IV.

Crypto Session Identification (CSID) 4-byte number, номер идентификатора криптосессии

Crypto Block Identification (CBID) 4-byte number, указывает на размер пакета шифрования (64 пакета шифрования) в одной мультиструктуре (сверхцикле)

Crypto Packet Identification (CPID) 3-byte number, идентификация номера пакета шифрования.

Уникальность IV предусмотрена числом 2 в степени 232 и умноженное на 64, при криптопериоде 4,672мкс, т.е. длительность использования сессии шифрования 14,86 дней. Реально такой период не требуется.

Образование криптопакета с его опознанием происходит в четырёх кадрах по сверхциклам (индикация MFAS в заголовке OTUk) на позициях байт, ранее зарезервированных (RES) в заголовке ODUk (рис.2.34, 2.35).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Frame Alignment Overhead							OTUk Overhead							OPUk OH	
2	RES		PM TCM	TCM ACT	TCM6			TCM5			TCM4		FTFL			
3	TCM3			TCM2			TCM1			PM		EXP				
4	GCC1		GCC2		APS/PCC			RES								

Рис.2.34. Заголовок кадра OTUk с полями для опознавания криптопакета

MFAS [1:0]	RES (row, col)							
	(2, 1)	(2, 2)	(4, 9)	(4, 10)	(4, 11)	(4, 12)	(4, 13)	(4, 14)
0	TAG	TAG	TAG	TAG	TAG	TAG	TAG	TAG
1	TAG	TAG	TAG	TAG	TAG	TAG	TAG	TAG
2	AAD	AAD	CSKS	CSID	CSID	CSID	CSID	CBID
3	AAD	AAD	CBID	CBID	CBID	CPID	CPID	CPID

Рис.2.35. Сверхцикловая структура для байт RES с размещением меток криптопакета

Полная структура криптопакета представлена на рис.2.36.

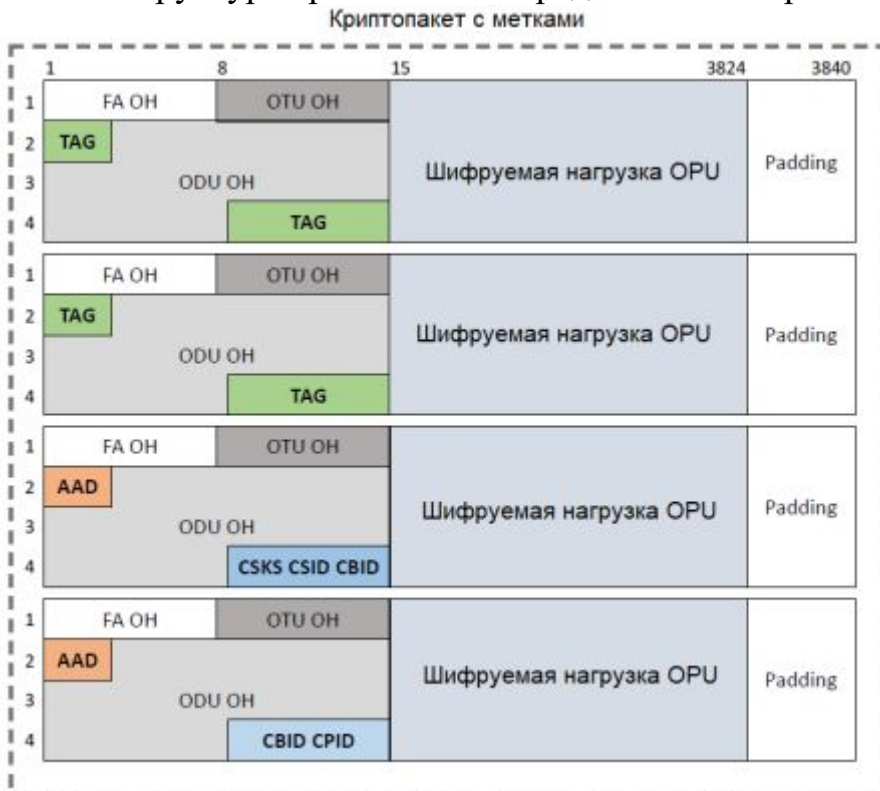


Рис.2.36. Структура криптопакета с метками

Пример реализации криптозащиты микромодулем - PM5990 DIGI-G4 в блоках OTU4 для канала на скорости 400Гбит/с представлен рис.2.37 и защищаемый участок оптической сети рис.2.38.

Single-Chip 400G OTN Line Card

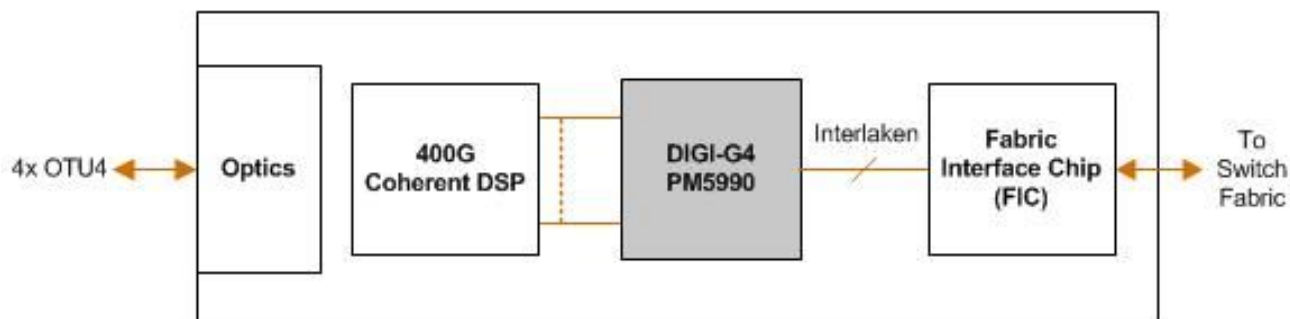


Рис.2.37. Структура модуля PM5990 DIGI-G4 <https://www.microsemi.com>

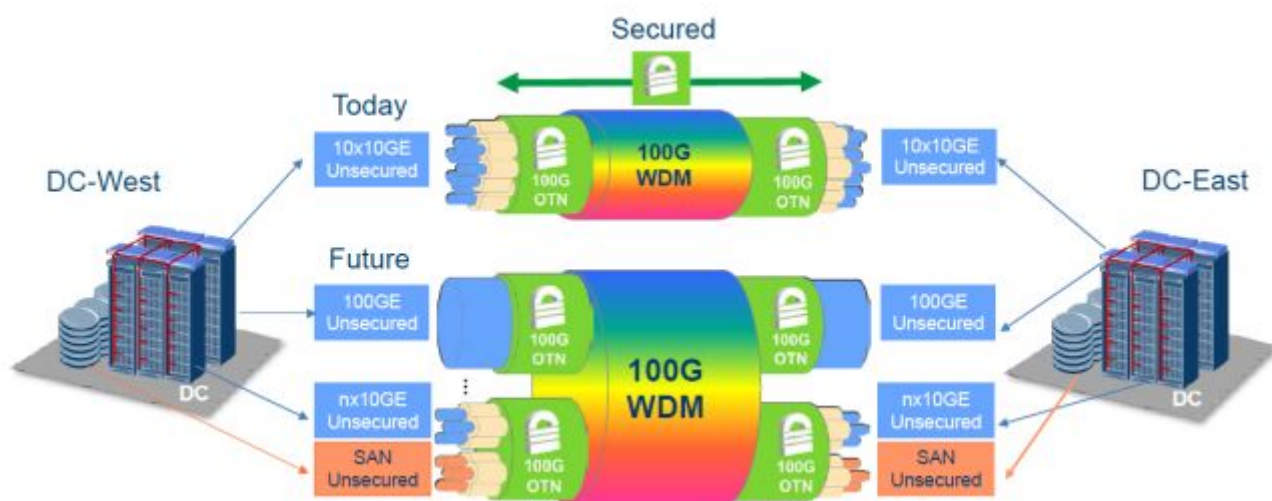


Рис.2.38. Участок оптической сети с применением криптозащиты уровня L1

2.8.5. Криптографическая защита оптических каналов связи уровня L1. Модули «Квазар» в оптической транспортной сети

Высокопроизводительные модули шифрования «Квазар» для защиты информации в оптических сетях предназначены для обеспечения конфиденциальности и целостности данных, защиты от навязывания ложного содержимого по отношению к передаваемой в сети OTN информации. Модули шифрования «Квазар» выполняют функции криптозащиты с производительностью 10 и 100 Гбит/с при передаче данных по магистральным волоконно-оптическим линиям связи между клиентским и каналообразующим оборудованием, а также могут сами выполнять роль последнего. Источник: <https://www.anti-malware.ru/reviews/Kvazar>

В России, учитывая требования действующего законодательства (152-ФЗ, 187-ФЗ, ГОСТ Р 57580.1-2017 и т. п.), необходимо применять сертифицированные в системе ФСБ России криптографические средства.

Модули шифрования «Квазар» подключаются между клиентским оборудованием и каналообразующим оборудованием сетей OTN и обеспечивают выполнение функций криптозащиты с производительностью 10 Гбит/с и 100 Гбит/с при передаче информации по магистральным волоконно-оптическим линиям связи.

Сценарии использования: Топология сети: точка-точка, кольцо.

Технические характеристики модуля Квазар

Канал: оптика, OTN с форматом кадра OTU2 (10 Гбит/с)/OTU4 (100 Гбит/с).

Клиент: оптика 10Gbit Ethernet или 8x1Gbit Ethernet.

Производительность шифрования 10/100 Гбит/с.

Алгоритм шифрования: ГОСТ Р34.12-2015 (Магма или Кузнечик). Шифр имеет 128-битный размер входного блока данных, 256-битный ключ и выполняет 10 раундов шифрования. В последнем раунде шифрования выполняется только одна операция — наложение раундового ключа.

Шифрование данных осуществляется в режиме гаммирования в соответствии с ГОСТ Р34.13-2015.

Имитозащита данных осуществляется в соответствии с ГОСТ Р34.13-2015.

Формирование и контроль имитовставки за каждый кадр OTU2.

Ключи — парные.

Коррекция ошибок FEC RS (255, 239).

СКЗИ «Квазар» — модули шифрования МШ-ТРfс и МШ-ТРfс-1U (транспондеры), МШ-MUXs и МШ-MUXs-1U (агрегирующие транспондеры), обеспечивают криптоимитозащиту и преобразование клиентского потока информации по интерфейсам 10 Gbit Ethernet или 8 Gbit Fibre Channel;

СКЗИ «Квазар-100» — модули шифрования ВМШ-ТР-1U для организации защиты высокоскоростного канала 100 Гбит/с.

Архитектура «Квазаров» спроектирована таким образом, чтобы обеспечить эффективную работу с оптической средой передачи данных без влияния на характеристики сети в целом.

Модуль шифрования «Квазар» помещает кадры клиентских протоколов L2 целиком в гораздо больший кадр протокола передачи данных по оптической сети (L1/L0) и потом шифрует его. Далее эти кадры доставляются через оптическую сеть и распаковываются устройством шифрования на другом её конце (рис.2.39, 2.40).

«Квазар» защищает весь направляемый в транспортную сеть трафик.

Линейка «Квазар» включает в себя:

СКЗИ «Квазар» — модули шифрования МШ-ТРfс и МШ-ТРfс-1U (транспондеры), МШ-MUXs и МШ-MUXs-1U (агрегирующие транспондеры);

СКЗИ «Квазар-100» — модули шифрования ВМШ-ТР-1U для организации защиты высокоскоростного канала 100 Гбит/с;

СКЗИ «Квазар-СКР» — модули шифрования с квантовой криптографической системой выработки и распределения ключей МШ-ТР-СКР;

СКЗИ «Квазар-Э» — экспортные варианты модулей шифрования МШ-ТРfc-1U и МШ-MUXs-1U.

Модули шифрования «Квазар» поддерживают формат OTU2e, а «Квазар-100» — формат OTU4, что даёт им совместимость с DWDM-системами ведущих производителей, таких как Huawei, ADVA Optical Networking, Packetlight Networks, **ООО «Т8»**, BTI (Juniper), Ciena, Infinera, Ekinops.

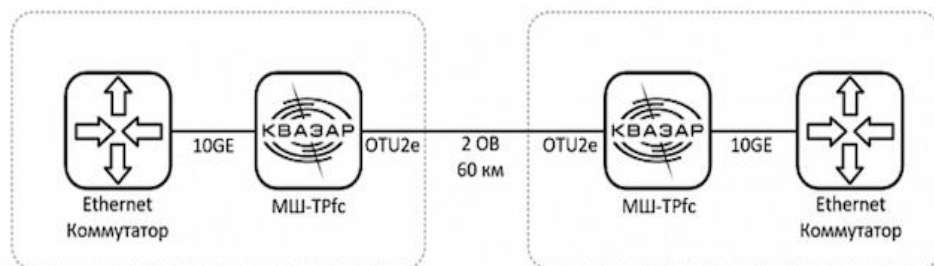


Рис.2.39. Модули Квазар для защиты соединения коммутаторов сети Ethernet

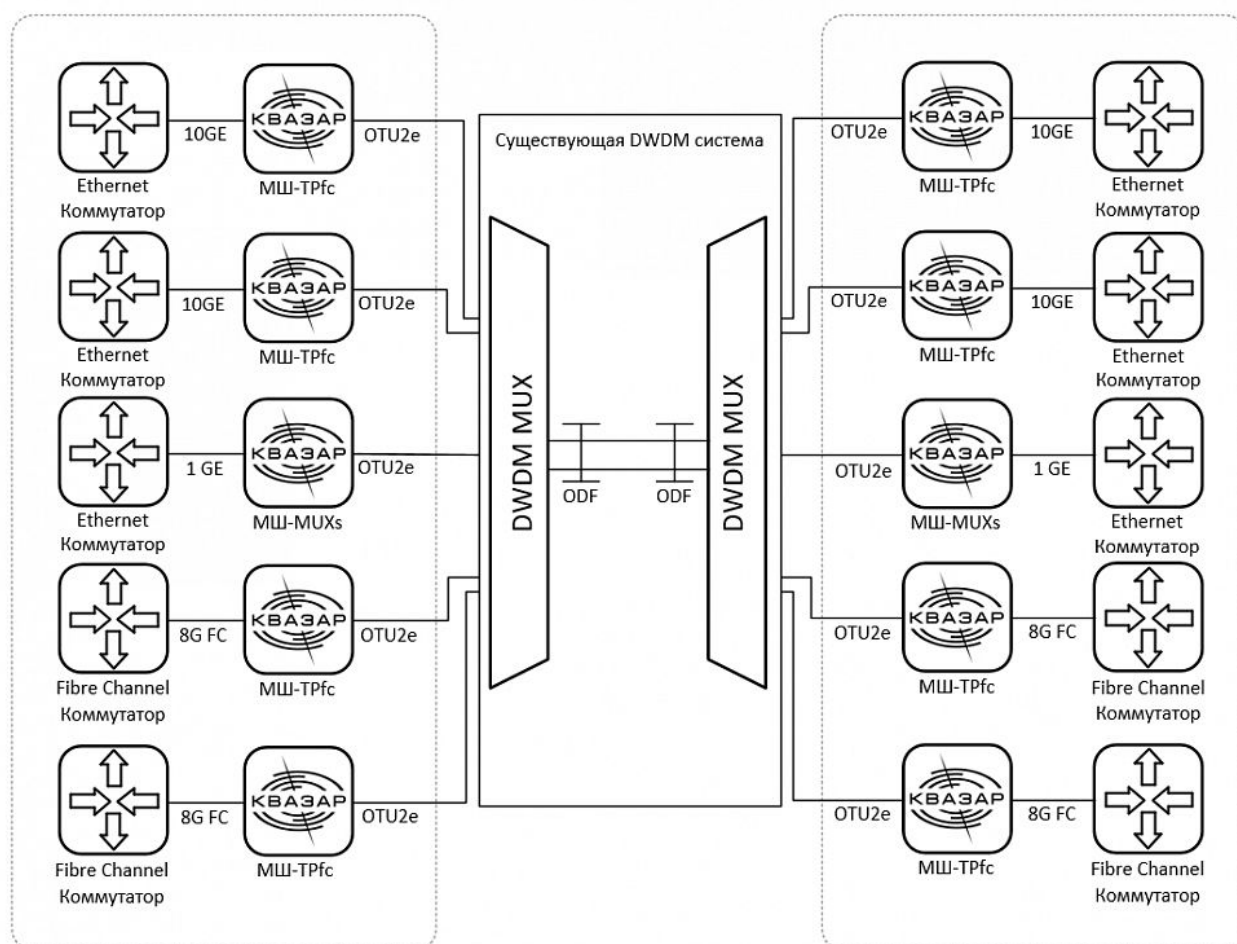


Рис.2.40. Применение модулей Квазар в оптической сети DWDM

Достоинства Квazar: отечественная разработка, L1-шифрование с применением алгоритма ГОСТ. Сертификат соответствия требованиям ФСБ России к СКЗИ по классу КСЗ. Минимальное влияние на ИТ-сервисы благодаря уникальным сетевым характеристикам, простая интеграция и внедрение без перерыва сервисов, включая интеграцию с системами мониторинга. Реальная производительность 10 и 100 Гбит/с без потерь, возможность масштабирования. При использовании дополнительного коммуникационного оборудования DWDM возможно мультиплексировать потоки нескольких СКЗИ в одно оптическое волокно, наращивая необходимую производительность по защите информации, при этом не увеличивая количество используемых оптических волокон. Защита мультисервисных сетей (потокоевое видео, ВКС, телефония, передача данных) обеспечивается без необходимости разделения потоков информации. Возможность подключения к магистральным каналам OTN, поддержка основных протоколов передачи данных (Eth 1G, 10G, 100G, 8GFC, STM 1-4-16), совместимость с любым DWDM или работа по «тёмному» волокну. Маскирование типа трафика в каналах связи. Возможность использовать в роли каналообразующего оборудования. Низкая стоимость в пересчёте на гигабит защищённой информации.

Контрольные вопросы

1. Какие протокольные уровни 7-уровневой модели ISO/OSI поддерживают функции защиты клиентской информации шифрованием?
2. В каких транспортных технологиях поддерживаются функции шифрования клиентского трафика?
3. Для чего нужны протоколы SSL/TLS?
4. Какие виды защиты соединений предусмотрены в транспортных сетях и сетях доступа?
5. Что обозначает IP sec?
6. Какие протокольные решения входят в IP sec?
7. Для чего нужны протоколы AH, ESP?
8. Чем отличаются протоколы IP sec для транспортного и туннельного режимов?
9. Для чего нужен протокол IKEv2?
10. Что такое MOBIKE?
11. Для чего нужен обмен Диффи-Хеллмана?
12. Для чего нужен протокол MAC sec?
13. Какой алгоритм шифрования используется в MAC sec?
14. Для чего предназначен стандарт IEEE802.1AE?
15. Что входит в структуру кадра MAC sec?
16. В чём состоят ограничения протокола IP sec и преимущество протокола MAC sec?
17. Какие проблемы существуют в шифровании на уровнях L2/L3 для транспортных сетей?

18. Какие сетевые транспортные функции поддерживает схема BCM85344?
19. Какое назначение у аппаратно-программного комплекса ViPNet L2-10G?
20. Где может применяться ViPNet L2-10G?
21. Какие сетевые конфигурации поддерживает ViPNet L2-10G?
22. В каком оборудовании транспортной оптической сети устанавливаются элементы криптографической защиты?
23. В чём состоят преимущества шифрования (криптозащиты) данных в каналах оптической транспортной сети OTN/OTN?
24. Где выше эффективность пропуска трафика при шифровании в OTN/OTN? В MAC sec? В IP sec?
25. Что предусмотрено рекомендацией ITU-T Sup.76?
26. Для чего нужны IKEv2?
27. Какая часть кадра OTUk подлежит шифрованию с целью защиты клиентского трафика?
28. Для чего нужны поля TAG, Encrypted OPU, ADD, IV в криптопакете?
29. Что входит в криптопакет L1?
30. Какой вид шифрования реализуется в схеме PM5990 DIGI-G4?
31. На каких участках оптической транспортной сети наиболее актуально применение шифрования?
32. Для чего предназначены модули «Квазар»?
33. Где должны применяться модули «Квазар»?
34. Какие клиентские протоколы и скоростные режимы передачи поддерживают модули «Квазар»?
35. Какой вид шифрования используется в модулях «Квазар»?
36. Что относится к линейке модулей «Квазар»?
37. С каким оборудованием транспортных сетей совместимы модули «Квазар»?
38. В чём особенность модулей СКЗИ «Квазар-СКР»?
39. Что обозначает GCM-AES-256?
40. Какая государственная структура РФ обеспечивает сертификацию защиты информации в телекоммуникациях?

Задача 2.

Используя алгоритм Диффи-Хеллмана вычислите разделяемый секретный ключ шифрования по варианту в таблицах 1, 2 и представьте его в двоичном подходящим по разряду коде.

Табл.1. Номер варианта соответствует предпоследней цифре студенческого билета или номера пароля

Вариант		0	1	2	3	4	5	6	7	8	9
Секретное число стороны А	X	2	3	4	5	6	7	6	5	4	3
Несекретные числа	D	4	5	4	6	7	3	2	3	5	8
	p	6	6	7	8	5	6	12	2	4	7

Табл.2. Номер варианта соответствует последней цифре номера студенческого билета или пароля

Вариант		0	1	2	3	4	5	6	7	8	9
Секретное число стороны Б	X	3	4	5	6	7	6	5	4	3	2
Несекретные числа	D	4	5	4	6	7	3	2	3	5	8
	p	6	6	7	8	5	6	12	2	4	7

Методические указания:

1. Для решения задачи изучите исходный материал и используйте примеры, приведённые в разделе 2.7.
2. Подробно представьте все этапы вычисления и выводы по результатам.

3. Оптические квантовые коммуникации и место применения квантово-криптографической защиты оптических сетевых соединений

В настоящее время переход к технологии, основанной на использовании квантовых эффектов, является одним из основных трендов в современных коммуникациях и высокопроизводительных вычислениях. Во всём мире в развитие квантовых методов передачи информации вкладываются большие ресурсы.

КТО ЗАНИМАЕТСЯ РАЗРАБОТКАМИ:

Российский квантовый центр

<https://www.rqc.ru/team/группа-квантовых-коммуникации>

Группа создана в 2015 году. Цель деятельности группы – выпуск коммерческого устройства квантовой криптографии (QKD312). Для достижения поставленной цели группа занимается экспериментальной квантовой оптикой, теорией квантовой информации, электроникой и разработкой программного обеспечения. Группой изучаются способы улучшения протоколов квантовой криптографии и оптических схем, для увеличения скорости работы и уменьшения габаритов устройств.

В общей сложности в России насчитывается около 850 таких организаций, в т.ч. более 80 академических институтов и научных центров (РАН и РАМН), около 150 ВУЗов и научно-технических центров при ВУЗах, около 100 отраслевых НИИ, КБ и НПО, около 60 производственных объединений и крупных предприятий, более 120 медицинских учреждений и не менее 320 малых предприятий. По территории страны они распределены весьма неравномерно. Центрами максимальной концентрации организаций и предприятий отрасли являются Москва, С. - Петербург, Московская область, Новосибирск и Поволжье.

3.1. Что такое квантовые коммуникации?

Предлагаю повторить определение по ГОСТ (*раздел оптической связи, связанный с изучением и практическим применением методов передачи информации фотонами, находящимися в неклассических (квантовых) состояниях*) начать с азов и взглянуть на само словосочетание. В нем есть слово «квант» и есть «коммуникация».

Коммуникация — набор технологий для передачи информации. В современном мире мы передаем информацию, кодируя ее в какие-либо физические сигналы: например, передавая данные в виде световых импульсов по оптоволоконному кабелю. В квантовых коммуникациях, в отличие от традиционных, в качестве носителя выступают необычные световые импульсы достаточно большой мощности, а квантовые сигналы, то есть те, которые обладают существенной квантовой природой. Оказывается, что в ряде случаев они дают возможность решать совершенно недоступные ранее задачи.

В **квантовых коммуникациях**, системах и устройствах используются принципы квантовой механики: 1) квантованность, дискретность уровней энергии, квантовый эффект Холла; 2) квантовая когерентная суперпозиция альтернативных чистых состояний систем; 3) квантовая запутанность состояний двух и больше объектов; 4) квантовое туннелирование; 5) квантовый параллелизм, позволяющий квантовым компьютерам превзойти классические по производительности; 6) принцип неопределенности Гейзенберга.

Реализации: квантовые коммуникации, квантовые сети, квантовая криптография, квантовое распределение ключей, квантовые алгоритмы, квантовая телепортация, квантовый Интернет, квантовая телефония, квантовые вычисления, квантовые компьютеры, квантовые радары, квантовые изображения, квантовая визуализация, квантовая микроскопия, квантовые сенсоры, квантовая метрология.

Наиболее развитое направление в рамках технологии — квантовая криптография, или, более точно, квантовое распределение ключей QKD (Quantum Key Distribution). Это совокупность методов, направленных на выработку между удаленными пользователями общего секретного ключа, который в дальнейшем используется для шифрования.

Еще одна задача квантовых коммуникаций — передача квантовой информации между квантовыми компьютерами. Технологии плавно идут к развитию распределенных квантовых вычислений, то есть к созданию, например, центрального квантового компьютера и множества периферийных машин, которые решают часть подзадач и передают данные друг другу. Альтернативой этому может быть набор связанных между собой удаленных квантовых процессоров. В феврале 2021 года группа исследователей из Германии продемонстрировала возможность передачи квантовой информации между двумя модульными квантовыми процессорами. Результаты эксперимента [опубликовал](#) журнал Science. Это важный шаг в развитии технологий, который показал, что увеличивать мощность квантовых вычислительных технологий возможно за счет объединения нескольких устройств в сеть.

Интересная технологическая особенность состоит в том, что если в квантовых компьютерах мы выбираем платформу, которая наиболее эффективно подойдет для решения тех или иных задач, то с обменом квантовой информацией все очевидно: лучше всего справляются фотоны, то есть частицы света. Альтернатив практически нет. Поэтому исследователи уже осознают, какой будет элементная база. Единственная сложность заключается в том, чтобы квантовую информацию, возникающую, например, в рамках работы сверхпроводникового квантового компьютера, каким-то образом транслировать в фотон, который можно передать на большие расстояния. А после снова преобразовать в ту форму, которая доступна квантовому компьютеру. Если квантовая криптография — понятный технологический фронт, который находится в очень высокой степени готовности, то область квантовых коммуникаций, связанная с обменом квантовой информацией между квантовыми компьютерами — большая задача, которая находится на достаточно ранней стадии.

В то время, как в квантовых вычислениях принято говорить о квантовом объеме — увеличении числа кубитов — квантовых бит (достижение 2048 кубитные компьютеры) и точности операций, в квантовых коммуникациях в широком контексте пока не существует единственной метрики. В квантовой криптографии ученые фокусируются на скорости генерации ключа на какое-либо расстояние. Чаще всего рассматривается скорость генерации ключа на 50 км, что позволяет сравнивать разные устройства. Порой также изучают какие-то предельные характеристики, например, максимальное расстояние для генерации ключей.

3.2. Основы физики квантовых коммуникаций

Что такое квант?

Квант — фундаментальная (минимальная и неделимая) порция энергии, а также соответствующая ей частица (например, квант света — фотон).

Обозначение кванта энергии:

$$E = h\nu$$

frequency of radiation, sometimes written as f giving expression $E = hf$.

Quantum energy of a photon.

h = Planck's constant = 6.626×10^{-34} Joule·sec = 4.136×10^{-15} eV·s

Понятие о кванте появилось в начале 20 века, когда были сформулированы фундаментальные законы квантовой физики и с ним связано определение первой квантовой революции. На основе квантовой физики были созданы приборы и устройства: генераторы оптического излучения, детекторы оптического излучения, электронные приборы (лампы, транзисторы, интегральные полупроводниковые схемы), оптические усилители и т.д. (рис.3.1)



Рис.3.1. Первая и вторая квантовые революции

С началом 21 века произошла вторая квантовая революция, с которой связано создание устройств и технологий на основе управления **отдельными квантовыми объектами** (революции в вычислениях, криптографии и метрологии!). Достижение качественно новых возможностей с помощью технологии квантовой передачи и обработки информации основано на законах квантовой физики, лежащих в их основе. В качестве примеров можно привести “мгновенную” передачу квантового состояния на расстоянии на основе принципа запутанности (квантовая телепортация), ускорение квантовых вычислений за счёт их неклассического параллелизма и обеспечение конфиденциальности данных в системах квантовой рассылки ключа, основанное на неделимости квантовых объектов и невозможности их клонирования. Устройства квантовой передачи и обработки информации используют квантовые единицы информации – кубиты, которые в отличие от классического аналога (бита) могут находиться в суперпозиции двух состояний, т.е. при измерении обнаруживаются в любом из этих состояний. Материальным воплощением кубита может быть любая микроскопическая физическая система с двумя состояниями. Кубит определяется как единица квантовой информации. Для наглядности представлен рис.3.2 пример отличий бит и кубит. Квантовая информация записывается в квантовых битах (*кубитах*).

Что такое квантовая суперпозиция?

Это суперпозиция альтернативных состояний (взаимоисключающих)!

Кубит - когерентная суперпозиция двух различных (ортогональных) квантовых состояний, например, вертикальной и горизонтальной поляризации.

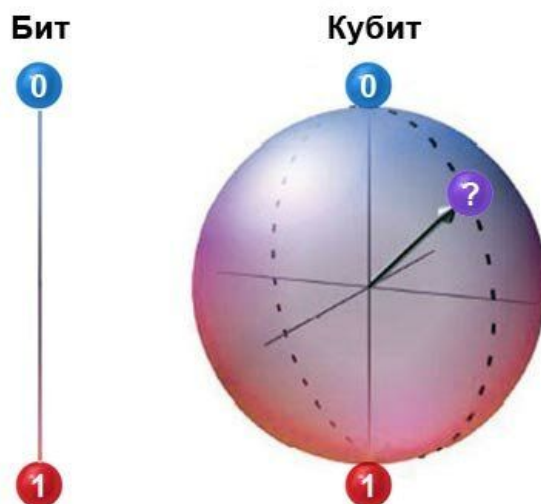


Рис.3.2. Соотношение понятий бит и кубит

Состояния кубита запутаны, т.е. невозможно до проведения измерений указать однозначно состояния «0» или «1»!

До измерения:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha^2 + \beta^2 = 1$$

После измерения: 0 или 1.

Кубиты могут быть запутаны: $|\psi_{12}\rangle \neq |\psi_1\rangle + |\psi_2\rangle$

Они становятся единой системой и измерение одного сразу же влияет на другой.

НЕОБХОДИМО принять во внимание фундаментальные свойства:

1. **Неопределённость** – чем точнее измеряется одна характеристика объекта, тем менее точно можно определить вторую (связанную с ней). Т.е. фотон может находиться в нескольких местах в один и тот же момент времени.

2. **Нереализм** – состояние квантового объекта можно определить только в процессе измерения, после которого это состояние разрушается. Т.е. фотон перестаёт существовать в одном месте и спонтанно возникает в другом без перемещения в пространстве, т.е. наблюдается квантовый переход или телепортация

3. **Нелокальность** – «запутанные» квантовые объекты могут влиять друг на друга, находясь на любом расстоянии («быстрее скорости света»). Т.е. появление одного квантового объекта, вызванное наблюдением (измерением), спонтанно влияет на связанный с ним объект-близнец, вне зависимости от того, как далеко тот находится (квантовое действие на расстоянии).

Теперь о квантах - фотонах. Фотон – это частица, у нее нет фазы, но она является частью волны. А фаза волны – это характеристика, которая показывает некоторую отстройку состояния поля электромагнитной волны. Если представить волну как синусоиду на координатной плоскости, сдвиги ее положения относительно начала координат соответствуют некоторым состояниям фазы. Фотон нельзя разделить или измерить, скопировать или незаметно отвести в сторону. Он из-за этого однозначно разрушается и не доходит до принимающей стороны (рис.3.3).

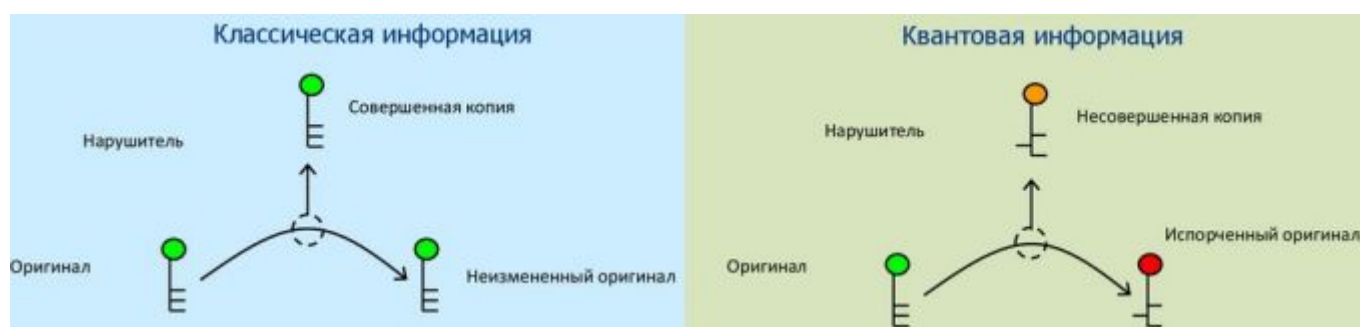


Рис.3.3. Сравнение классической и квантовой передачи информации

Квантовая физика, как основа понимания принципов работы систем квантовой связи, указывает на вероятностный характер законов природы или статистические закономерности. Результаты измерений в квантовой физике носят принципиально статистический характер.

Возможные достижения второй квантовой революции: новые материалы и новая элементная база; квантовые компьютеры; квантовая криптография; новые сенсоры (датчики) различного назначения (рис.3.4).



Рис.3.4. Предполагаемые достижения второй квантовой революции

Область квантовой передачи информации возникла на стыке нескольких областей знания, развивавшихся достаточно давно. К ним относятся фотоника, квантовая физика, информатика, теория информации и криптография. Все задачи, относящиеся к этому направлению, можно разбить на две категории: задачи квантовой коммуникации и тесно взаимосвязанные с ними задачи квантовых вычислений. К квантовым коммуникациям относятся разработка систем квантовой криптографии, квантовой связи (например, на основе телепортации) и построение квантовых защищённых и вычислительных сетей. К квантовым вычислениям относят технологии обработки классической или квантовой информации и квантовыми методами: создание квантовых логических схем и вычислительных элементов, построение квантового компьютера (процессора и памяти) и разработка квантовых алгоритмов для него. Две области объединяет единая технологическая база: источники и приёмники одиночных фотонов, линейные и нелинейные элементы квантовых схем.

Квантовая криптография основывается на алгоритмах формирования квантовых ключей и их рассылки

Системы квантовой рассылки ключа (КРК) гарантируют отсутствие подслушивания в канале и используются для генерации случайных двоичных последовательностей, известных только отправителю и получателю (рис.3.5). Эти последовательности могут быть использованы для получения симметричных ключей, которые невозможно подобрать даже на квантовом компьютере. Таким

образом, в отличие от классических методов защиты данных, стойкость систем квантовой коммуникации не зависит от времени и вычислительной мощности нарушителя. Квантовая коммуникация может осуществляться по любому оптическому каналу: волокну или открытому пространству. Также квантовая криптография может совмещаться с существующей криптографией открытым ключом для повышения надёжности шифрования (рис.3.6).



Рис.3.5. Схема квантовой рассылки ключа



Рис.3.6. Схема формирования комбинированного ключа шифрования на основе протоколов: BB84 (квантовый протокол) и RSA2048 (несимметричный ключ)

Системы квантовой рассылки ключа (КРК), представляющие собой наиболее развивающийся класс устройств квантовой передачи информации, позволяют осуществлять распределение ключей, которые могут быть использованы в качестве симметричных ключей, между двумя (и более) пользователями (Алиса и

Боб). Генерация квантовых ключей происходит путём получения, передачи и обработки закодированных квантовых сигналов по определенному алгоритму (протоколу). На практике в системах КРК в основном используются следующие характеристики однофотонного излучения: **поляризация, фаза, пространственная и временная отстройки**. Системы КРК обеспечивают безусловную конфиденциальность передачи информации. В теории все возможные вмешательства в квантовый канал нелегитимного пользователя (Евы) и попытки получить доступ к информации о ключе ведут к увеличению квантовых ошибок по битам (QBER) в соответствии с законами квантовой физики, а именно: с принципиальной невозможностью измерения состояния фотона, с невозможностью его разделить, а также скопировать. Уровень ошибок, вызванный, в том числе, прослушиванием канала нелегитимным пользователем, может быть устранен, если значение в просеянной последовательности не превышает 11% (для протокола BB84). В противном случае канал связи считается заблокированным. Однако в квантовой теории информации принято считать, что все ошибки, вносимые в канал, вносятся как раз нелегитимным пользователем, что значительно усложняет работу по очистке ключа. Появление систем КРК заблаговременно предвосхитило реализацию квантового компьютера, который потенциально обладает более высокой вычислительной мощностью по сравнению с классическими аналогами. Системы КРК разрабатываются исходя из принципа технологической и вычислительной неограниченности возможностей нелегитимного пользователя, что учитывается при строгих математических доказательствах обеспечения секретности.

3.3. Протоколы квантового распределения ключей

Главная идея квантовой криптографии – передавать информацию таким образом, чтобы ее было нельзя перехватить. Причем это должно быть невозможно не потому, что алгоритмы шифрования слишком сложные, и не из-за того, что злоумышленник не располагает достаточно высокими вычислительными мощностями. Защищённая система передачи данных должна быть построена так, что ее взлом противоречил законам физики.

Квантовая криптография, квантовая связь и квантовые коммуникации решают задачу так, что перехватывать информацию ограниченного доступа запрещает сама природа. Сигналы передаются по линиям связи не в классическом виде, а с помощью потока одиночных фотонов. Фотон нельзя разделить или измерить, скопировать или незаметно отвести в сторону. Он из-за этого однозначно разрушается и не доходит до принимающей стороны.

Квантовая криптография обеспечивает абсолютно защищенное распределение ключа, поскольку, в отличие от классической криптографии, она основана на законах физики, а не на ограниченности вычислительных мощностей.

Ключевой вопрос в том, как сделать это эффективно, так как используется не идеальная система, а физические линии связи – оптическое волокно или открытое пространство. На пути к получателю на фотон может воздействовать много факторов, которые могут его разрушить.

В основе квантовой криптографии лежит тезис о том, что злоумышленник может пытаться делать что угодно, использовать любые инструментарий и оборудование – хотя бы технику прищельцев, но перехватить данные он не должен. А на базовый принцип (физическую основу) уже «накручиваются» технические решения, о которых далее будет сообщено.

Существует несколько схем реализации базового принципа, основанных на разных подходах, которые вносят свои возможности по увеличению скорости и дальности передачи сообщений. Системы квантовой криптографии давно производятся коммерческими компаниями с использованием поляризационного ортогонального и неортогонального кодирования.

Системы КРК обеспечивают безусловную конфиденциальность передачи информации. В теории все возможные вмешательства в квантовый канал нелегитимного пользователя (Е - Евы) и попытки получить доступ к информации о ключе ведут к увеличению квантовых ошибок по битам (QBER) в соответствии с законами квантовой физики, а именно: с принципиальной *невозможностью измерения состояния фотона*, с *невозможностью его разделить*, а также *скопировать*.

Специалисты Университета ИТМО предложили новый принцип, который иначе формулирует понятие квантового состояния, «способа приготовления» фотона как порции излучения, чтобы он был более устойчивым к внешним воздействиям, система связи не требовала дополнительных средств организации устойчивой передачи и не несла в себе явных ограничений на скорость модуляции сигнала со стороны отправителя и получателя. Предложено выносить квантовые сигналы, формируемые по какому-либо протоколу, на так называемые боковые частоты, это позволяет значительно расширить возможности по скорости и снять явные ограничения по дальности, присущие уже принятым схемам (рис.3.7).

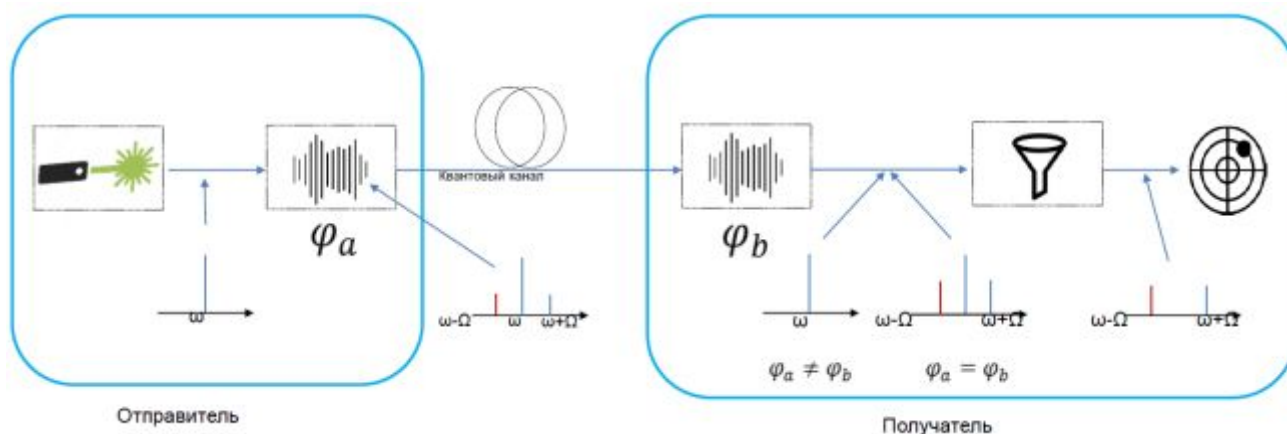


Рис.3.7. Формирование боковых частот для квантовых сигналов (по материалам компании СМАРТС КВАНТТЕЛЕКОМ)

Чтобы понять, в чем отличие предлагаемого метода, можно начать с принципов работы классических схем.

Обычно люди, когда строят системы квантовой связи, генерируют слабый импульс, эквивалентный или близкий к энергии одиночного фотона, и отправляют его по линии связи. Чтобы закодировать в импульсе квантовую информацию, проводят модуляцию сигнала – изменяют поляризацию или фазовое состояние. Если речь идёт про волоконно-оптические линии связи, для них более эффективно использовать фазовые состояния, потому что сохранять и передавать поляризацию в оптической линии на протяженные дистанции проблематично.

Вообще фаза фотона – это вульгаризм, который придумали экспериментаторы в области квантовой физики. Фотон – это частица, у нее нет фазы, но она является частью волны. А фаза волны – это характеристика, которая показывает некоторую отстройку состояния поля электромагнитной волны. Если представить волну как синусоиду на координатной плоскости, сдвиги ее положения относительно начала координат соответствуют некоторым состояниям фазы.

Говоря простыми словами, когда человек шагает, шаг – это процесс, который повторяется по кругу, у него тоже есть период, как у волны. Если два человека идут в ногу – фазы совпадают, если не в ногу – то фазовые состояния разные. Если же один начинает движение в середине шага другого, то их шаги находятся в противофазе.

Для того, чтобы закодировать в импульсе квантовую информацию, используют модулирующее устройство, которое сдвигает волну, а чтобы измерить сдвиг, мы складываем эту волну с такой же и смотрим, что получится. Если волны находятся в противофазе, то две величины накладываются и гасят друг друга, на выходе получается ноль. Если фазы совпали, то синусоиды складываются, поле увеличивается и итоговый сигнал получается высокий. Это называется конструктивной интерференцией излучения, ее можно проиллюстрировать теми же человеческими шагами.

Как работает предлагаемая схема? Лазер излучает оптический сигнал на волне ω , которая проходит через электрооптический модулятор (рис.3.8). На модулятор подается сигнал на другой частоте Ω , существенно более низкой, и в результате кодирование осуществляется не основной синусоидой, а параметрами вспомогательной синусоиды – ее частотой смены фазы, фазовым положением. Квантовая информация передается отстройкой дополнительных частот в спектре импульса относительно центральной частоты.

Наше решение

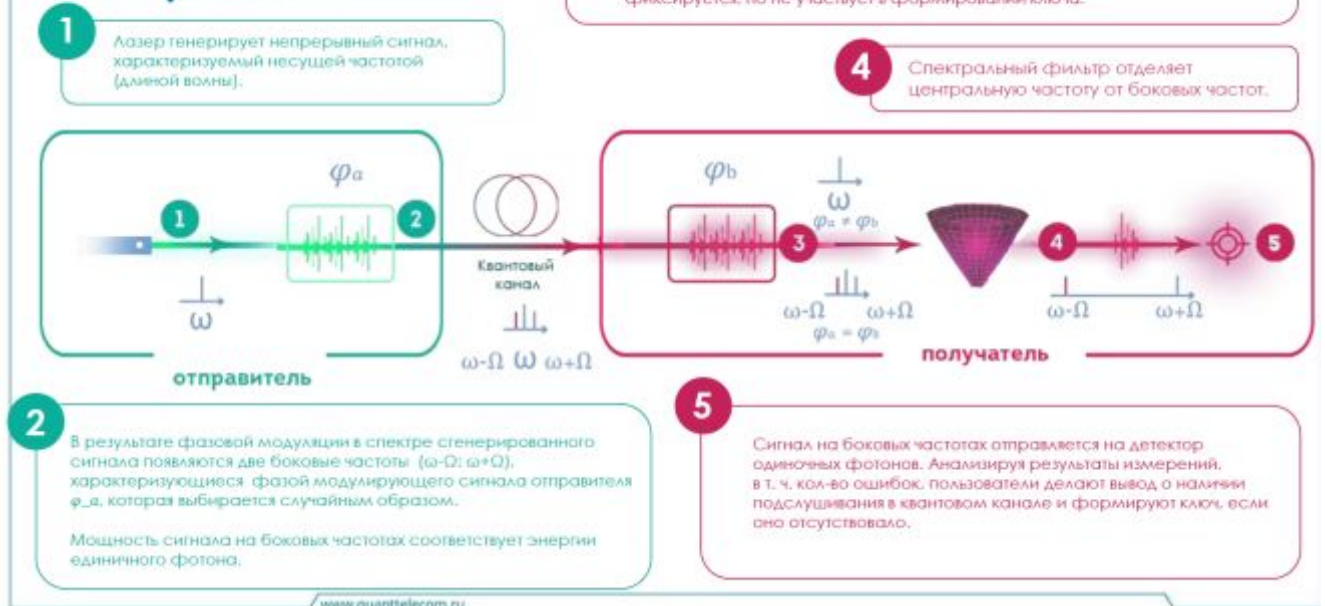


Рис.3.8. Процедуры передачи в квантовом канале

Такое шифрование становится куда более надежным, так как спектр передается по линиям связи одним импульсом, и если среда передачи вносит какие-то изменения, их претерпевает весь импульс целиком. Также можно добавить не одну дополнительную частоту, а несколько, и одним потоком единичных фотонов можно поддерживать, к примеру, пять каналов связи. В итоге не нужен интерферометр в явном виде – он «защит» внутри импульса, нет нужды в схемах компенсации дефектов в линии, нет ограничений на скорость и дальность передачи данных, а эффективность использования линий связи – не 4%, как в случае с классическими подходами, а до 40%.

Все эти квантовые решения нужны для формирования секретного ключа – случайной последовательности, которая перемешивается с данными, чтобы их в итоге было невозможно перехватить. По принципу действия системы для безопасной передачи эквивалентны VPN-роутеру, когда через внешний интернет прокладывается локальная сеть, чтобы в нее никто не ломился. Устанавливаются два устройства (например, QKD312), у каждого из которых есть порт, который подключается к компьютеру, и порт, который «смотрит» во внешний мир. Отправитель подает данные на вход, устройство их шифрует и безопасно передает через внешний мир, вторая сторона принимает сигнал, расшифровывает и передает получателю.

В настоящее время существует несколько протоколов квантового распределения ключа, основу которых составляют следующие принципы. Квантовое распределение ключа начинается с пересылки одиночных или перепутанных квантов от отправителя к пользователю по какой-либо физической среде (волоконные световоды или воздушная атмосфера). Предполагается, что

отправитель отправляет пользователю конфиденциальную информацию. Несанкционированный съём информации агентом (злоумышленником), с физической точки зрения, основан на серии экспериментов, выполняемых агентом на носителях информации, в данном случае на пересылаемых квантах. Согласно правилам квантовой механики, в общем случае любое измерение, выполняемое агентом, неизбежно меняет состояния передаваемых квантов. Отправитель и пользователь могут это обнаружить (выяснить) в последующей открытой связи.

Таким образом, основные составляющие квантового распределения ключа таковы: квантовый канал для обмена квантами и так называемый открытый канал, который используется, чтобы проверить искажено ли сообщение через квантовый канал.

Во время квантовой пересылки ключ либо закодирован с использованием заданного набора неортогональных квантовых состояний одной частицы, либо он получается из заданного набора измерений, выполняемых на перепутанных частицах после пересылки. В последнем случае во время пересылки ключ еще даже не существует.

Квантовые протоколы распределения ключа, основанные на передаче одиночных фотонов с неортогональными состояниями поляризации, наиболее привлекательны в свободном пространстве, где сохраняется их поляризация, но их труднее осуществить в оптических волноводах, из-за деполяризации и случайно флуктуирующего двулучепреломления. Деполяризация не является основной проблемой: ее действие можно подавить посредством достаточно когерентного источника. Временные флуктуации двулучепреломления при стационарных условиях являются довольно медленными (1 час). Электронная система компенсации, осуществляющая непрерывное отслеживание и исправление поляризации, возможна, но она требует процедуры согласования между отправителем и пользователем. Квантовая криптография, реализуемая в открытых линиях связи, лишена такого недостатка как изменение поляризации. Однако здесь возникает проблема прохождения света через турбулентную атмосферу и детектирование единичных фотонов при интенсивной фоновой засветке. В то же время, сочетание узкополосной частотной и пространственной фильтрации с наносекундной техникой позволяет осуществить генерацию ключа с приемлемыми величинами относительной ошибки.

Как происходит формирование квантового ключа шифрования? В устройствах стоит генератор случайных чисел (причем физический, не псевдо-ГСЧ), и каждое устройство задает квантовое состояние фотонов случайным образом. В квантовой коммуникации отправителя принято называть «Алиса», а получателя – «Боб» (А и Б). Допустим, Алиса и Боб выбрали квантовое состояние, соответствующее 0, фазы оптического излучения совпали, получился высокий уровень сигнала и детектор фотонов Боба сработал. Если Алиса выбрала 0, а Боб 1, фазы разные и детектор не срабатывает. Далее приемная сторона говорит, когда фазы совпали, допустим, на первой, пятой, пятнадцатой, сто пятьдесят пятой передачах, в остальных случаях либо были разные фазы, либо фотоны не дошли. Для ключа мы оставляем только то, что совпало. И Алиса, и Боб знают,

что у них совпали передачи 1, 5, 15 и 155, но что они при этом передавали – 0 или 1 – знают только они и никто больше.

В квантовой криптографии выделились **два основных направления** развития систем распределения ключей (рис.3.9).

Первое направление основано на кодировании квантового состояния одиночной частицы и базируется на принципе *невозможности различить абсолютно надёжно два неортогональных квантовых состояния*.

Защищенность первого направления основывается на *теореме о запрете клонирования неизвестного квантового состояния*. Благодаря унитарности и линейности квантовой механики, невозможно создать точную копию неизвестного квантового состояния без воздействия на исходное состояние.

Основным протоколом квантовой криптографии на одночастичных состояниях является протокол BB84.

Второе направление развития основано на эффекте *квантового перепутывания (запутывания)*. Две квантово-механические системы (в том числе и разделённые пространственно) могут находиться в состоянии корреляции, так что измерение выбранной величины, осуществляемое над одной из систем, определит результат измерения этой величины на другой. Ни одна из запутанных систем не находится в определённом состоянии. Поэтому запутанное состояние не может быть записано как прямое произведение состояний систем.

Базовым протоколом квантового распределения ключей на основе эффекта квантового запутывания является протокол EPR (Einstein-Podolsky-Rosen), второе его название E91.

Всего известно порядка полутора десятка протоколов квантового формирования и распределения ключей, разработанных за последние сорок лет.

BB84 (1984) - схема распределения квантовых ключей, которая позволяет двум сторонам безопасно передавать закрытый ключ для использования в одноразовом шифровании с использованием квантового свойства, заключающегося в том, что получение информации возможно только за счет искажения сигнала, если два состояния, которые вы пытаетесь различить, не являются ортогональными и аутентифицированным общедоступным классическим каналом.

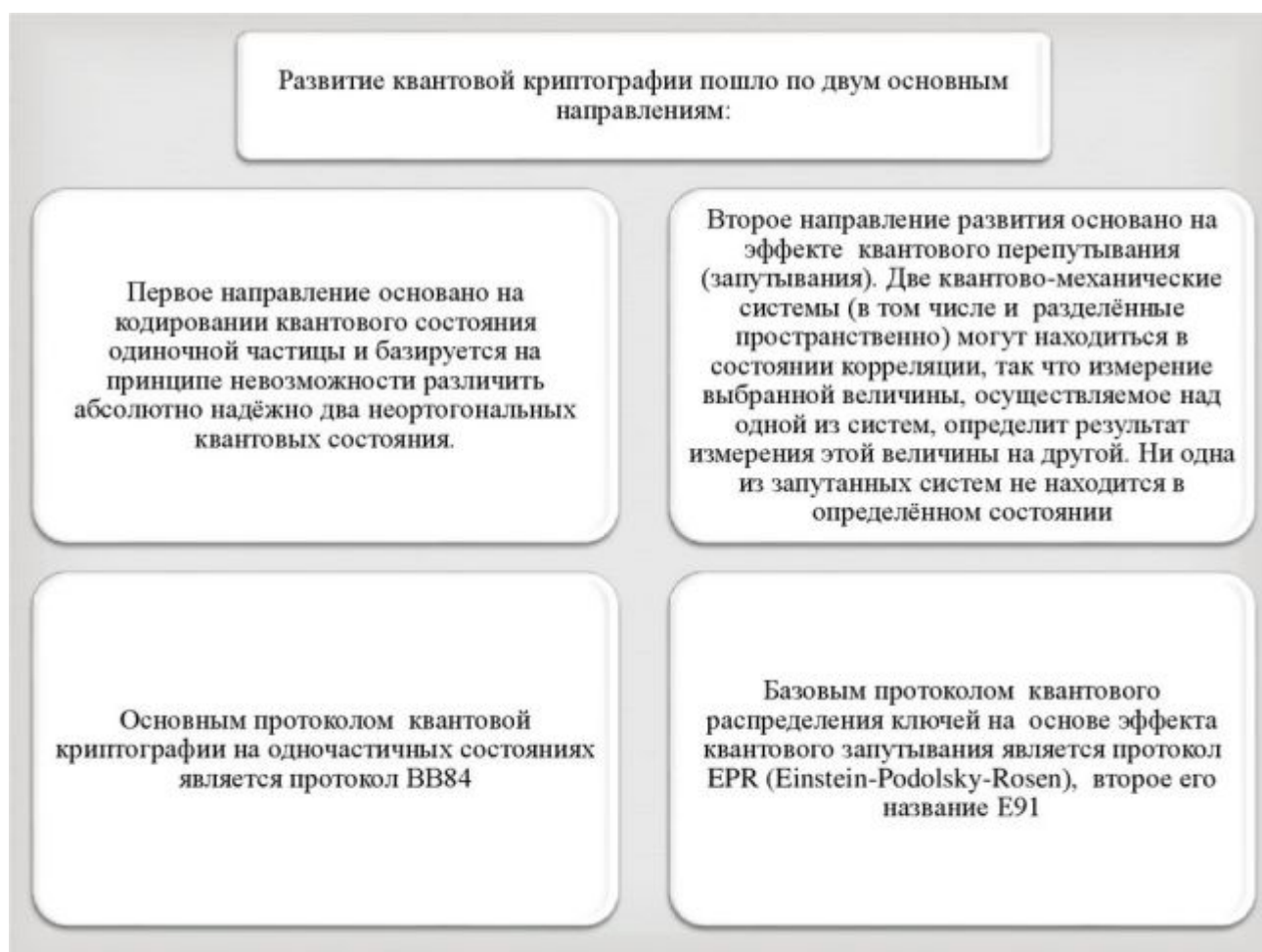


Рис. 3.9. Базовые направления развития квантовой криптографии, ставшие основой для ряда протоколов формирования и распределения ключей

Протокол E91 (1991) представляет собой метод квантовой криптографии, который использует запутанные пары фотонов для генерации ключей для безопасной связи, с возможностью обнаружения любых попыток подслушивания со стороны внешней стороны путем нарушения теоремы Белла и сохранения идеальной корреляции между измерениями двух сторон.

Протокол BBM92 (1992) - это метод распределения квантовых ключей, который использует поляризованные запутанные пары фотонов и состояния-приманки для безопасной передачи неортогональных квантовых сигналов.

Протокол B92 (1992) представляет собой метод распределения квантовых ключей, который использует протоколы перегонки запутанности для подготовки и передачи неортогональных квантовых состояний с безусловной безопасностью, даже по каналам с потерями и шумом, путем измерения состояния на основе Z и использования локальной фильтрации и измерений на основе Z для обеспечения безопасности передачи, определяемой количеством ошибок и количеством используемых пар фильтров.

Протокол MSZ96 (1996) использует четыре неортогональных квантовых состояния слабого оптического поля для кодирования бита криптографического ключа без использования поляризации фотонов или запутанных фотонов.

Протокол с шестью состояниями (1998) - это метод передачи защищенной информации с использованием квантовой криптографии, который более устойчив к шуму и в нем легче обнаруживать ошибки по сравнению с протоколом BB84, благодаря использованию схемы поляризации с шестью состояниями на трех ортогональных основаниях и его способности выдерживать более шумный канал.

Протокол DPS (2002) представляет собой простой и эффективный метод квантового распределения ключей (QKD), который не требует процесса выбора основы, как традиционный протокол BB84, имеет более простую конфигурацию приемника с меньшим количеством детекторов, использует эффективные последовательные импульсы во временной области для высокой скорости создания ключа и устойчив к атакам с расщеплением числа фотонов даже при слабом когерентном свете.

Протокол состояния-приманки (2003) - это метод, используемый в практических системах квантовой криптографии, который использует несколько уровней интенсивности в источнике передатчика и отслеживает частоту ошибок в битах для обнаружения и предотвращения атак с разделением числа фотонов, обеспечивая более высокие скорости безопасной передачи или большую максимальную длину канала.

SARG04 (2004) - протокол квантового распределения ключей, который был разработан как более надежная версия BB84, особенно для защиты от атак с разделением числа фотонов, для использования с ослабленными лазерными импульсами в ситуациях, когда информация поступает от пуассоновского источника, генерирующего слабые импульсы, и принимается несовершенным детектором.

Протокол COW (2005) обеспечивает безопасную связь между двумя сторонами путем передачи ключа с использованием слабых когерентных импульсов света и обладает преимуществами, заключающимися в том, что требуется только генератор случайных чисел на стороне клиента и возможность передавать ключевую информацию с высокой скоростью.

Трехэтапный протокол квантовой криптографии (2006) - это метод шифрования данных, который использует случайные повороты поляризации двумя аутентифицированными сторонами для непрерывного шифрования данных с использованием одиночных фотонов, а также может использоваться для обмена ключами с возможностью многофотонной квантовой криптографии и возможностью устранения атак типа "человек посередине" путем модификации.

Протокол KMB09 (2009) позволяет увеличить расстояния передачи между Алисой и Бобом за счет использования двух взаимно несмещенных базисов и введения минимальной частоты ошибок при передаче индекса и частоты ошибок в квантовых битах, что особенно эффективно для состояний фотонов более высокой размерности.

HDQKD - это технология, которая обеспечивает безопасную связь между двумя сторонами путем кодирования квантовой информации в больших измерениях, таких как режимы оптического углового момента, и передачи ее на большие расстояния по многоядерным волокнам или каналам связи свободного пространства.

Протокол T12 направлен на повышение практичности QKD путем устранения определенных идеализаций и включения функций, которые могут увеличить скорость передачи ключей системы.

Протокол BB84(4+2) является промежуточным между протоколами BB84 и B92. В протоколе используются 4 квантовых состояния для кодирования «0» и «1» в двух базисах. Состояния в каждом базисе выбираются неортогональными, состояния в разных базисах также попарно неортогональны.

3.4. Протокол распределения квантовых ключей BB84

В протоколе BB84 используются 4 квантовых состояния фотонов, например, направление вектора поляризации, одно из которых Алиса выбирает в зависимости от передаваемого бита: 90° или 135° для «1», 45° или 0° для «0» (рис.3.10). Одна пара квантовых состояний соответствует $0+$ и $1+$ и принадлежит базису «+». Другая пара квантовых состояний соответствует $0\times$ и $1\times$ и принадлежит базису « \times ». Внутри обоих базисов состояния ортогональны, но состояния из разных базисов являются попарно неортогональными (неортогональность необходима для детектирования попыток съёма информации).

BB84 работает следующим образом.

Изначально участники формирования ключа могут договариваются, как будут интерпретировать каждое из состояний фотонов (например (рис.3.10), 1 для вертикальной поляризации, 0 для горизонтальной в вертикально-горизонтальном базисе, аналогично для диагонального базиса, т.е. всего два базиса).

Один из собеседников (традиционно его называют Алисой) посылает другому (Бобу) фотоны, поляризованные в одном из двух, неортогональных друг другу, базисах: прямоугольном или диагональном. Боб получает их и измеряет поляризацию, выбирая базисы для измерения случайным образом, и записывает результаты измерений и базисы. Затем он и Алиса обмениваются информацией об использованных базисах (но не о результатах измерения) по открытому каналу, и данные, полученные при несовпавших базисах, сбрасываются. Остаются только значения, измеренные в совпадающих базисах (в технологии квантового распределения ключей это называется “просеиванием ключа”). Возможный “шпион”, который подслушивает передачу данных по этой линии связи (его обычно называют Ева) может перехватить одиночный фотон, измерить его поляризацию и попытаться переслать копию фотона Бобу. Но, в соответствии с теоремой о невозможности клонирования произвольного квантового состояния, это приведет к росту числа ошибок в распределяемом квантовом ключе. В результате и Алиса, и Боб поймут, что их канал прослушивает посторонний. Для определения уровня ошибок в ключе после процедуры квантового распределения Алиса и Боб по открытому каналу сравнивают небольшую часть ключа. Считается, что если уровень ошибок в ключе менее 11 процентов, то можно гарантировать безопасность линии связи. В противном случае квантовый канал считается заблокированным.

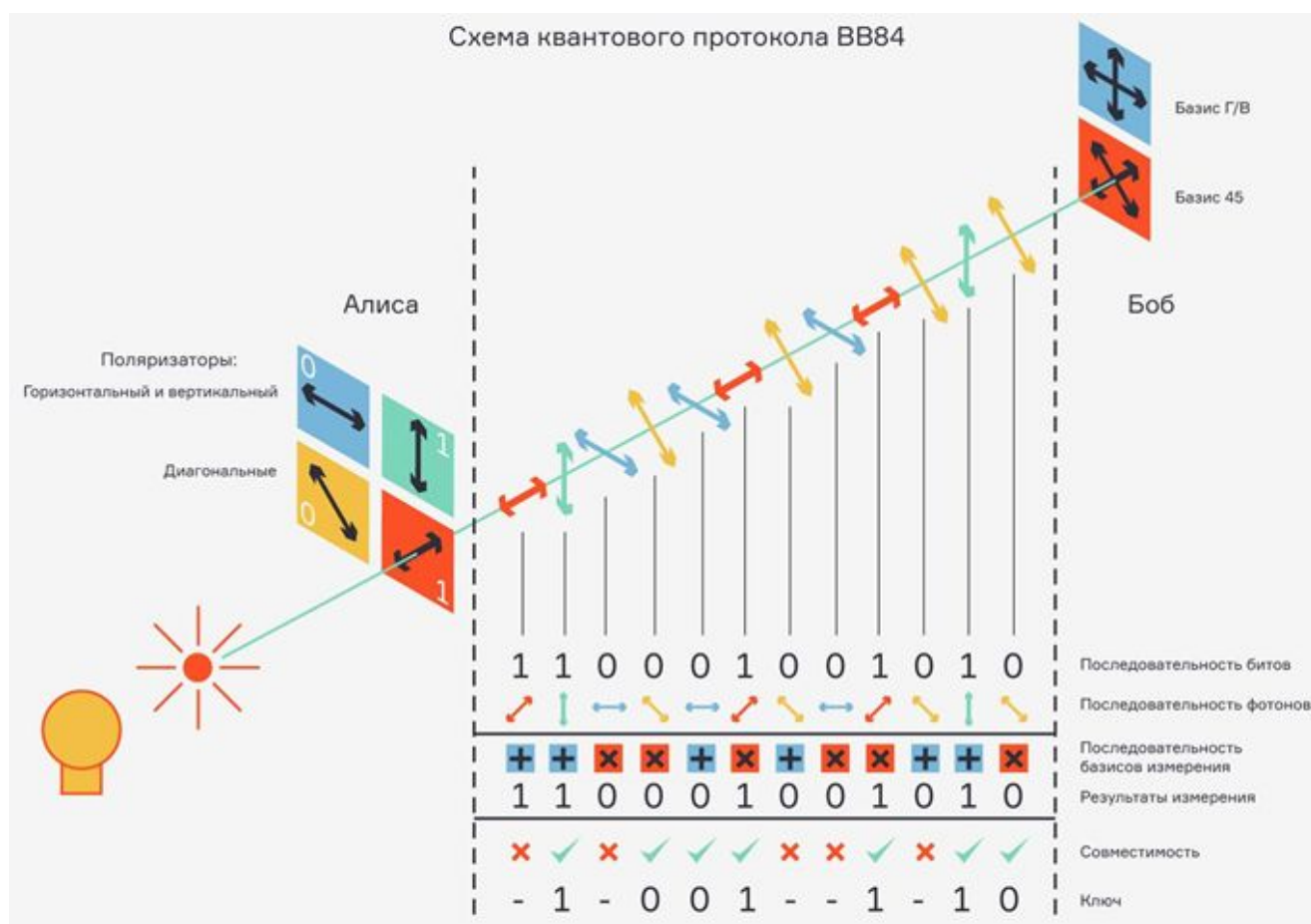


Рис.3.10. Схема квантового протокола BB84

Пример использования протокола BB84 на защищённой линии квантовой связи продемонстрирован в 2021 году в России, где запущена защищённая линия длиной 700 км. Линия соединила Москву и Санкт-Петербург. Протокол передачи разработал Санкт - Петербургский национальный исследовательский университет информационных технологий, механики и оптики (ИТМО) (<http://government.ru>). Также сообщается, что выполненный проект обеспечит к 2024 году создание до 7 тыс. км защищённых квантовых линий связи по всей стране, взломать которые едва ли возможно.

ПРИМЕР ОБОРУДОВАНИЯ QKD312, разработка российского квантового центра (РКЦ).

Оборудование использует метод передачи ключей шифрования, основанный на принципах квантовой физики. Установка передает секретный ключ на расстояние до 120 км в заданный период времени с исключением риска перехвата. Оборудование квантового распределения ключей устанавливается поверх существующей инфраструктуры и работает совместно с предустановленными средствами криптографической защиты информации.

На карте стратегических рисков информационной безопасности все чаще фигурирует атака, направленная на алгоритмы асимметричного шифрования, реализуемая с применением различных квантовых вычислителей, в частности, квантового компьютера. С учетом экспоненциального роста мощности квантовых

вычислителей можно ожидать достаточной для этого мощности на горизонте 3-5 лет.

Интеграция системы квантового распределения ключей (КРК) в современную инфраструктуру информационной безопасности позволит достичь максимального уровня криптостойкости по отношению к потенциальным атакам злоумышленников. При этом процесс распределения и управления ключевыми документами становится прозрачным, непрерывным и освобождается от влияния человеческого фактора.

Технические характеристики QKD312:

Протокол функционирования установки QKD312: **BB84 Decoy-State** (состояний ловушек)

Функциональный диапазон длины волны: $1\,550 \pm 10$ нм

Частота приготовления квантовых состояний: 312,5 МГц

Скорость генерации ключа на расстоянии до 30 км: 40 Кбит/сек

Бюджет канала: 24 дБ

Максимальное расстояние между доверенными узлами: 120 км

Поддерживаемые протоколы: ETSI, ПЛИВ, API

Требования к вспомогательному каналу обмена данными: L2/L3 от 10 Мбит/с

Габариты блока передачи и приёма: 450*600*177 мм, 4U, 19"

Пиковая потребляемая мощность: 800 Вт

3.5. Квантовая запутанность и протоколы распределения ключей

Квантовая запутанность – определение по ГОСТ ПНСТ 830—2023:

квантовая запутанность или *сцепленность*: квантовое явление, при котором квантовые состояния двух или более частиц являются взаимозависимыми, (примечание — квантовую запутанность описывают состоянием квантовой системы в целом, а не квантовым состоянием отдельных входящих в нее частиц).

Распределение квантовой запутанности: распределение квантовых состояний, находящихся в состоянии квантовой запутанности, между различными точками пространства.

Протокол на основе явления квантовой запутанности E91 был разработан Артуром Экертом в 1991 году. Так же он имеет название EPR (Einstein-Podolsky-Rosen) так как он основан на [парадоксе Эйнштейна-Подольского-Розена](#). В протоколе предлагается использовать, например, пары фотонов, рождающихся в антисимметричных поляризационных состояниях. Перехват одного из фотонов пары не приносит Еве никакой информации, но является для Алисы и Боба сигналом о том, что их разговор прослушивается.

Отправитель генерирует некоторое количество EPR фотонных пар. Один фотон из каждой пары он оставляет для себя, второй посылает своему партнеру. При этом, если эффективность регистрации близка к единице, при получении отправителем значения поляризации 1, его партнер регистрирует значение 0 и наоборот. Ясно, что таким образом партнеры всякий раз, когда требуется, могут получить идентичные псевдослучайные кодовые последовательности.
<https://www.pvsm.ru/>.

В протоколе Бенета В92, также основанном на явлении квантовой запутанности, используются фотоны, поляризованные в двух различных направлениях для представления нулей и единиц (рис.3.11). Фотоны, поляризованные вдоль направления $+45^\circ$, несут информацию о единичном бите, фотоны, поляризованные вдоль направления 0° – о нулевом бите 0.

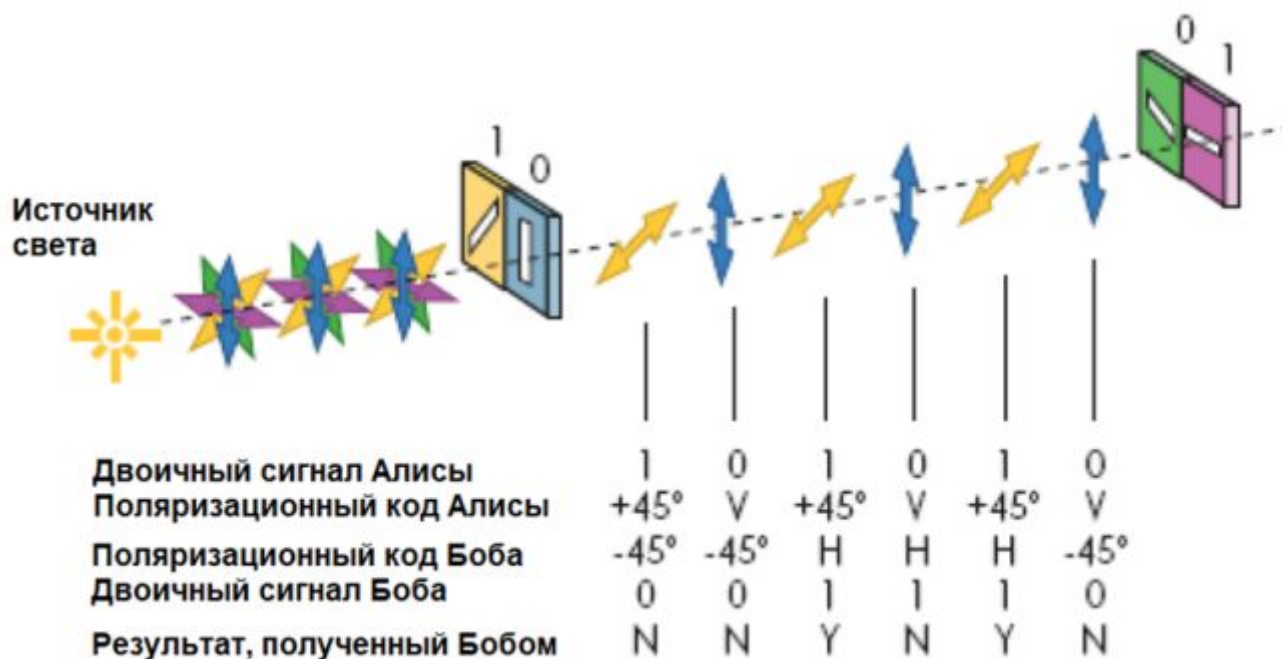


Рис.3.11. Схема квантового протокола В92

Принцип действия протокола состоит в следующей последовательности.

Станция Алиса посылает фотоны, поляризованные в направлениях 0° и $+45^\circ$, представляющие нули и единицы. Причем последовательность фотонов, посылаемая станцией Алиса, случайно ориентирована. Станция Боб принимает фотоны через фильтры ориентированные под углом 90° и 135° (-45°). При этом если фотон, переданный станцией Алиса, будет анализирован станцией Боб при помощи фильтра ориентированного под углом 90° по отношению к передаваемому фотону, то фотон не пройдет через фильтр. Если же этот угол составит 45° , то фотон пройдет через фильтр с вероятностью $0,5$.

Для определения поляризации станция Боб анализирует принимаемые ей фотоны, используя выбранный случайным образом один из двух неортогональных базисов «+» или «х». Если станция Боб анализирует посланный фотон фильтром с ортогональным направлением поляризации, то он не может точно определить, какое значение данный фотон представляет: 1 , соответствующее фотону, который не проходит, или 0 , соответствующее фотону, который не проходит с вероятностью $0,5$. Если же направления поляризации между посланным фотоном и фильтром, неортогональны, то станция Боб может определить, что принят фотон соответствующий 0 . Если фотон был принят удачно, то очередной бит ключа кодируется 0 (если фотон был принят фильтром, ориентированным под углом 135°), либо 1 (если фотон был принят фильтром, ориентированным по направлению горизонтально).

То есть в результате передачи такого ключа, около 25% фотонов будут правильно детектированы станцией Боб.

После этого по открытому каналу связи станция Боб может передать станции Алиса, какие 25 фотонов из каждой 100 были ей получены. Данная информация и будет служить ключом к новому сообщению. При этом чтобы злоумышленник не узнал информацию о ключе, по открытому каналу связи можно передать информацию только о том, какие по порядку фотоны были приняты, не называя состояния фильтров и полученные значения поляризации. После этого станция Алиса может передавать сообщения Бобу зашифрованные этим ключом.

Для обнаружения факта съема информации в данном протоколе используют контроль ошибок, аналогичный контролю ошибок в протоколе BB84.

Применение протокола B92 отмечено в системе VIP NET QSS от компании ИнфоТеКС, продемонстрировавшей в оборудовании квантовой сети МГУ им. М.В. Ломоносова в 2021 году с демонстрацией расстояния до 50 км с однофотонной передачи (www.tadviser.ru).



Рис.3.12. Защита инфраструктуры сети управления ОАО РЖД в перспективе

3.6. Оборудование квантовых коммуникаций для сетей связи

3.6.1. СКЗИ «Квазар-СКР» — модули шифрования с квантовой криптографической системой выработки и распределения ключей МШ-ТР-СКР

«Квазар-СКР». Особенностью модуля шифрования «Квазар-СКР» является сопряжение с квантовой криптографической системой выработки и распределения ключей (ККС ВРК). Необходимость «Квазар-СКР» обусловлена стремлением повысить удобство работы конечных пользователей за счёт отказа от

периодической доверенной доставки ключей симметричных криптоалгоритмов и, соответственно, увеличения автономности СКЗИ благодаря такому отказу.

Это усовершенствование потребовало проработки и реализации интерфейса взаимодействия модулей шифрования «Квазар» с ККС ВРК, а также механизмов использования полученных по интерфейсу квантовых величин для защиты передаваемой по OTN-каналу информации. Модуль шифрования обеспечивает криптоимитозащиту и преобразование клиентского потока информации по интерфейсам 10 Gbit Ethernet или 8 Gbit Fibre Channel. Планируемое получение сертификата ФСБ России о соответствии требованиям к СКЗИ по классу КСЗ в 2022 году.

Поддержка возможности сокращения общего количества оптоволоконных линий связи в системе за счет реализации в составе протокола взаимодействия СКЗИ – ККС ВРК функционала по передаче сообщений служебного канала, необходимого для успешной выработки квантовой величины. Конструкция модуля представлена на рис.3.13.



Рис.3.13. Конструкция модуля «Квазар-СКР»

Для защиты высокоскоростных оптических каналов со строгими требованиями к параметрам сети применяются **устройства класса L1 Services Encryption**.

«Квазар» — это единственное на сегодняшний день сертифицированное в системе ФСБ России криптосредство на российском рынке с поддержкой российских криптоалгоритмов для шифрования на **уровне L1 в оптических сетях**.

С помощью модулей «Квазар» можно построить защищённые каналы между филиалами компании, основными и резервными ЦОДами, обеспечить защиту различных мультисервисных сетей (потокное видео, ВКС, телефония, передача данных) (рис.3.14).

L1-шифраторы «Квазар» эффективны при построении оптических высокоскоростных каналов связи между площадками, когда предъявляются требования по защите передаваемой информации с применением сертифицированных СКЗИ, а также при наличии систем и сервисов с высокими показателями SLA.

Наличие сертификата соответствия требованиям ФСБ России к СКЗИ по классу КСЗ даёт возможность использовать модули шифрования «Квазар» в составе комплексов защиты систем, где применение сертифицированных продуктов обязательно (государственные информационные системы,

информационные системы персональных данных, финансовые (банковские) системы, подпадающие под требования ГОСТ Р 57580.1-2017).

Модули «Квазар» помимо функций криптозащиты также могут выполнять роль каналообразующего оборудования. Низкие показатели вносимой задержки у «Квазаров» наряду с отсутствием джиттера и потерь даже при стопроцентной загрузке канала позволяют интегрировать криптосредства в сеть без влияния на работу информационных систем и сервисов. Прозрачная работа «Квазаров» не требует их участия в маршрутизации или коммутации пакетов. Совместимость «Квазаров» с DWDM-системами даёт возможность работать на скорости линии и не вносить изменений в DWDM-систему существующей сети, обеспечивая защиту последней без ограничения её пропускной способности. Как таковых недостатков обнаружено не было, поскольку продукт является единственным в своём роде на рынке. Однако можно отметить некоторые нюансы, обусловленные спецификой L1 Services Encryption — учитывая то, что все заголовки L2 и выше шифруются, возможно только позвенное шифрование (в том числе в кольцевых сетях OTN). Вследствие этого необходимо использовать большое количество таких шифраторов.

Достоинства:

Отечественная разработка, L1-шифрование с применением алгоритма ГОСТ. Сертификат соответствия требованиям ФСБ России к СКЗИ по классу КСЗ. Минимальное влияние на ИТ-сервисы благодаря уникальным сетевым характеристикам, простая интеграция и внедрение без перерыва сервисов, включая интеграцию с системами мониторинга. Реальная производительность 10 и 100 Гбит/с без потерь, возможность масштабирования. При использовании дополнительного коммуникационного оборудования DWDM возможно мультиплексировать потоки нескольких СКЗИ в одно оптическое волокно, наращивая необходимую производительность по защите информации, при этом не увеличивая количество используемых оптических волокон. Защита мультисервисных сетей (потокоеое видео, ВКС, телефония, передача данных) обеспечивается без необходимости разделения потоков информации. Возможность подключения к магистральным каналам OTN, поддержка основных протоколов передачи данных (Ethernet: 1G, 10G, 100G; 8GFC; STM 1-4-16), совместимость с любым DWDM или работа по «тёмному» волокну. Маскирование типа трафика в каналах связи. Возможность использовать в роли каналообразующего оборудования. Низкая стоимость в пересчёте на гигабит защищённой информации.

Недостатки: Топология «точка — точка»: необходимо использовать большое количество модулей шифрования, т. к. возможно только позвенное (каскадированное) шифрование.

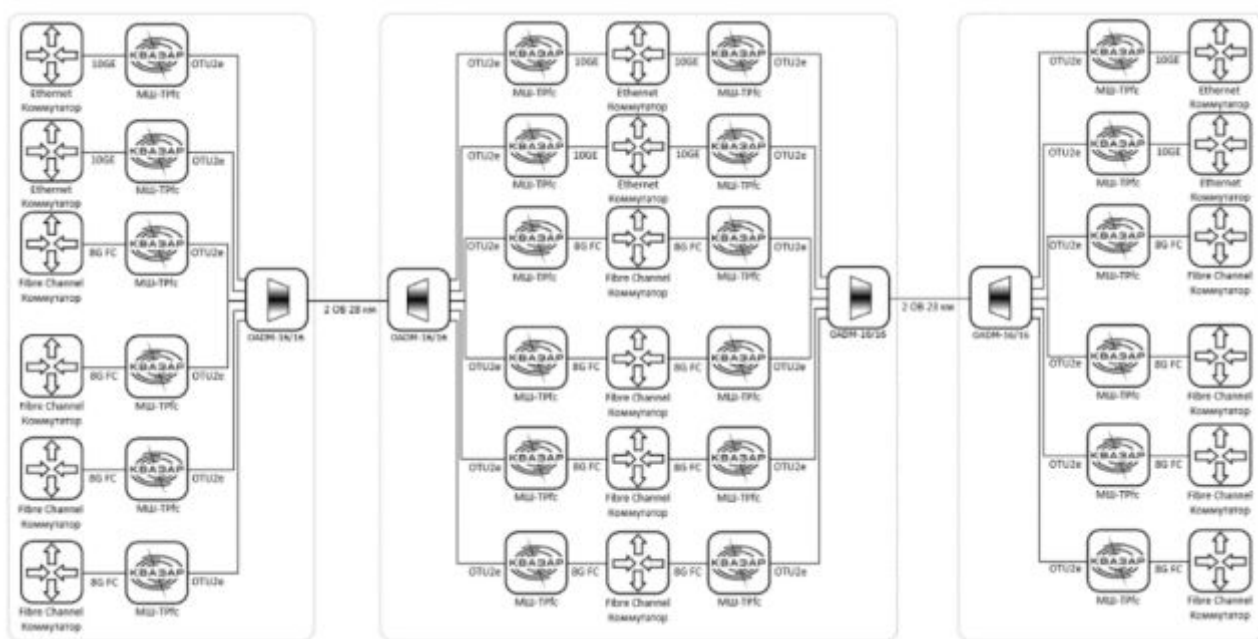


Рис.3.14. Схема применения СКЗИ «Квazar-СКР»

3.6.2. Оборудование ViPNet Quandor

Оборудование ViPNet Quandor 2 — инновационный продукт, первый в линейке квантовых продуктов ИнфоТеКС.

ViPNet Quandor 2 — это квантовая криптографическая система выработки и распределения ключей (ККС ВРК), снабжающая квантовозащищенными ключами шифрования каналные шифраторы ViPNet L2Q-10G.

Особенности

Функционирование ККС ВРК в топологии «точка-точка».

Максимальная длина квантового канала 100 км.

Скорость выработки квантовых ключей от 256 бит/мин.

Используется фундаментальный принцип квантовой физики о невозможности «подслушивания» квантовой информации без ее изменения (закон о запрете клонирования).

Оригинальный протокол квантового распределения ключей (КРК) с использованием геометрически однородных ортогональных квантовых состояний.

ViPNet Quandor состоит из двух устройств: сервер квантового распределения ключей; клиент квантового распределения ключей. Сервер и клиент имеют одинаковое конструктивное исполнение и являются парными узлами в сети квантового распределения ключей.

К серверу и клиенту квантового распределения ключей подключаются два сопряженных ViPNet L2Q-10G. Сопряженные ViPNet L2Q-10G обеспечивают безопасную передачу информации между доверенными сетями с помощью ключей шифрования, выработанных с помощью квантовых ключей.

Устройства ViPNet Quandor соединены квантовым каналом связи, по которому передаются квантовые состояния во время выработки квантовых ключей. Выработанные квантовые ключи сохраняются в защищенном хранилище

и передаются ViPNet L2Q-10G по запросу. Для функционирования ViPNet Quandor дополнительно необходимы: ViPNet Coordinator HW — для организации взаимодействия устройств ViPNet Quandor в сети ViPNet.

Для работы системы ViPNet Quandor требуется сеть ViPNet, управление которой осуществляется с помощью программного комплекса ViPNet Administrator. Сеть ViPNet представляет собой виртуальную защищенную сеть, которую можно развернуть поверх локальных или глобальных сетей произвольной топологии. Технология ViPNet обеспечивает защищенное взаимодействие между узлами сети ViPNet по схеме «клиент-клиент».

Волоконно-оптическая линия связи (далее — ВОЛС) образует квантовый канал связи. Для эксплуатации ViPNet Quandor ВОЛС должна иметь следующие параметры: ВОЛС должна использоваться для передачи квантовых состояний и синхроимпульсов и не должна использоваться для передачи иных сигналов. При этом квантовые состояния и синхроимпульсы при передаче используют разную длину волны. При создании ВОЛС должно использоваться одномодовое волокно. Тип коннекторов — FC/UPC. Запрещено использовать коммуникационное оборудование, преобразующее сигналы (усилители, регенераторы, ретрансляторы и т. д.). Длина квантового канала не должна превышать 100 км. Оптические потери на длине волны 1550 нм на единицу длины квантового канала связи должны быть не более 0,2 дБ/км.

Устройства ViPNet Quandor имеют следующие режимы работы:

Стартовый контроль. В этот режим устройство переходит после включения. Выполняется проверка работоспособности аппаратной платформы и выбор режима работы.

Режим инициализации. В этот режим устройство переходит после успешного прохождения стартового контроля, если отсутствует ключевая информация.

Режим конфигурации — режим ограниченной функциональности. В этот режим устройство переходит: о после завершения инициализации; о по команде администратора; о по истечения срока действия ключей ViPNet; о при возникновении некоторых ошибок во время штатного режима работы.

Штатная работа. В этом режиме вырабатываются и распределяются квантовые ключи. Во время штатной работы устройствами ViPNet Quandor вырабатываются квантовые ключи, которые сохраняются в ViPNet Quandor до их загрузки в ViPNet L2Q-10G.

Загрузка квантовых ключей в ViPNet L2Q-10G выполняется по запросу ViPNet L2Q-10G. Количество выработанных (сохраненных) квантовых ключей и необходимость выработки новых проверяется: о после успешной выработки квантового ключа, о после успешной загрузки квантовых ключей обоим ViPNet L2Q-10G, о при ошибке выработки квантового ключа; о после перезагрузки устройства; Если во время выработки квантового ключа возникла ошибка, то повторная выработка будет запущена через 1 минуту. Если ошибка является неустранимой, то выработка квантовых ключей будет прекращена и устройство перейдет в режим Жесткая блокировка.

Жесткая блокировка. В этом режиме устройство не может выполнять никаких операций — устройство неработоспособно. Для восстановления работоспособности обратитесь в ИнфоТеКС.

Оборудование ViPNet Quandor является частью линейки оборудования Инфотекс (рис.3.15).



Рис.3.15. Линейка оборудования VipNet Quantum Security System

Пример области реального применения оборудования VipNet Quantum Security System представлен на рис.3.16.



Рис.3.16. Участок применения оборудования VipNet Quantum Security System между ЦОД

В состав комплекса входит квантовая криптографическая система выработки и распределения ключей (ККС ВРК) сопряженная IP-телефонами ViPNet Quantum Security System, область использования которой представлена рис.3.17, 3.18.

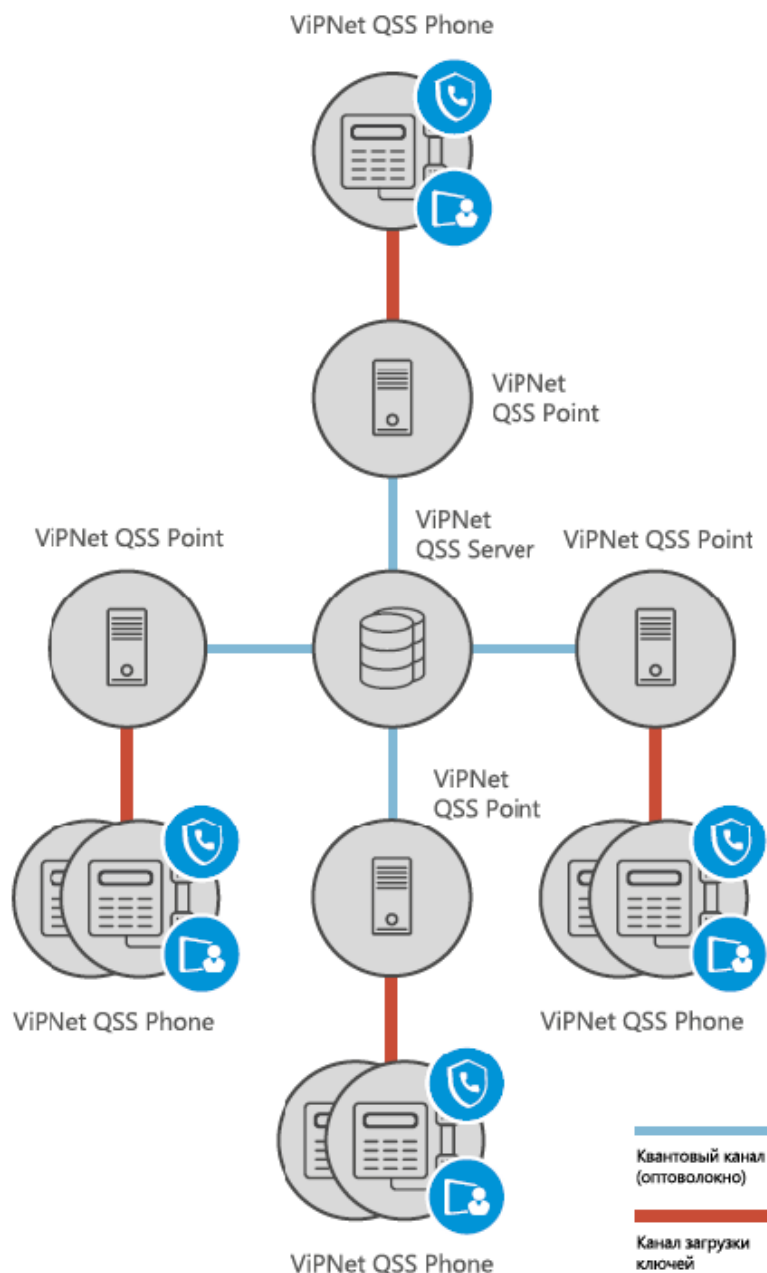


Рис.3.17. Оптическая сеть с квантовым шифрованием

К оборудованию защищаемой сети относятся соединения: Сервер и Клиент КРК – КС3; Абонент КРК (Android) –КС1; Абонент КРК (Windows) –КС3; Абонент КРК(Linux) –КВ.

Расстояние СКРК-ККРК до 44 км.

3 уровня оптической коммутации резервированием каналов.

До 860 Клиентов КРК.

1 Клиент – N Абонентов (в пределах КЗ).

Не содержит ни одного асимметричного криптографического механизма

Имеет 2 ключевые системы и обеспечивает защиту от компрометации ключей администраторами

Скомпрометировать систему можно только путем одновременного подкупа двух администраторов (ViPNet и КРК) в период развертывания системы (рис.3.19) !

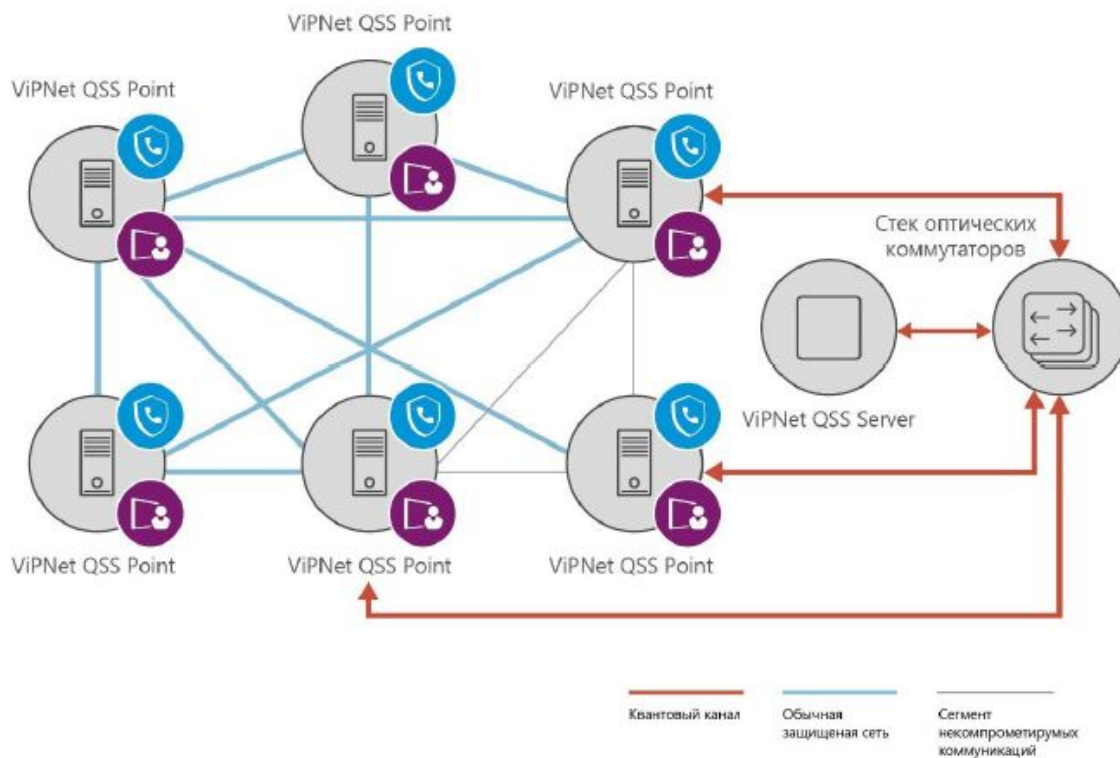


Рис.3.18.Квантовые каналы для защищаемой сети

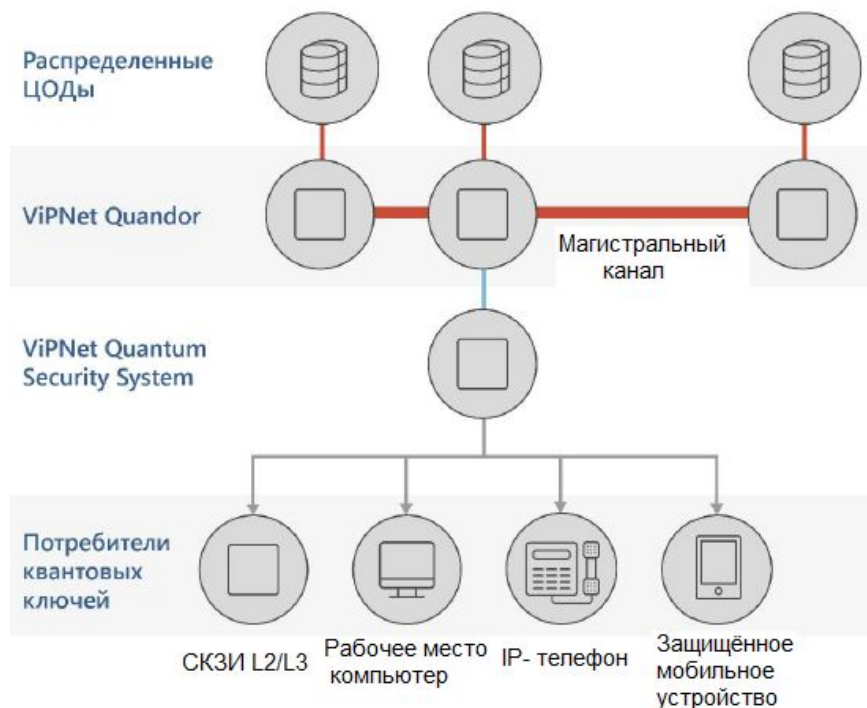


Рис.3.19. Потребители квантовых ключей



Рис.3.20. Пример использования ViPNetQuandor в магистральной транспортной сети

3.6.3. Оборудование ООО «СМАРТС - Кванттелеком» для квантовых коммуникаций

Оборудование построено для квантово-криптографической системы на боковых частотах (КРКБЧ). Преимущества систем на боковых частотах (КРКБЧ)

Генерируем абсолютно стойкие ключи (одноразовый блокнот) на основе законов физики. Для генерации используем кванты света — фотоны. Их физические свойства позволяют отправителю и получателю всегда знать, есть ли в системе «нарушитель», и понять, можно ли использовать ключ. Спектр сгенерированного фотона дополняем двумя боковыми частотами для устойчивости к внешним помехам и повышения скорости данных

Спектральная эффективность:

лучшие мировые системы КК: скорость 1-2 Мбит/с, 20 каналов DWDM = 40-80 Мбит/с, спектральная эффективность в канале с интерфейсом 1 Gbit Ethernet: 4-8%.

Системы ККБЧ позволят передавать до 10 независимых каналов на каждой паре боковых частот (разнос каналов ~ 4 ГГц) внутри одного окна DWDM (разнос каналов ~ 100 ГГц). Высокая устойчивость к внешним воздействиям на канал. Полная поляризационная независимость. Работают в стандартных оптических волокнах. Однонаправленная оптическая схема.

Гибкость реализуется на основе разных протоколов.

Технические параметры не ограничены архитектурой системы.

Скорость генерации квантового ключа: до 10 кбит/с.

Частота обновления ключа до 10 раз в секунду.

Скорость передачи данных 10 Гбит/с.

Поддержка протоколов OTN, TCP/IP, UDP.

Предельные потери в оптическом канале: 39 дБ (230 км).

Спектральный диапазон С (1530 .. 1565 нм).

Тип волокна: SMF-28е или аналогичное.

Интерфейс подключения: FC/APC.

Частота импульсов: 100 МГц.

Шифратор на основе системы КВАЗАР.

Основные параметры и характеристики КРК:

Энергопотребление: не более 450 Вт

Расстояние: до 80 км (между КМ КРК-А и КРК-Б)

Режимы выработки ключей: "точка-точка"

Возможность шифрования ключей и передачи их по каналам общего пользования (для клиентов, не имеющих квантовой аппаратуры).

Криптоалгоритм: ГОСТ Р 34.12-2015

Режим шифрования: ГОСТ Р 34.13-2015 (режим гаммирования)

Реализация шифрования: аппаратная (ПЛИС)

Алгоритм исправления ошибок в квантовом канале: LDPC; исправляемый QBER: 6%

Локальное управление/мониторинг: да (ПК, разъем подключения 1Гбит/сек, RJ45)

Габариты: 19" 2U 600x175x436 (без учета ручек на фронтальной панели) (рис.3.21).



Рис.3.21. Оборудование МШ-ТР КРК

Основные параметры и характеристики МШ-ТР-КРК

Клиентские интерфейсы (Клиент): 10 Gbit Ethernet или 8 Gbit FC, модуль SFP+

Линейные интерфейсы (Канал): 2xOTU2e, модуль SFP+

Линейные интерфейсы КРК: КК-1 Gbit Ethernet, тип FC, СК-1 Gbit Ethernet, модуль SFP+

Производительность при передаче: 10 Gbit/s Ethernet или 6, 8 Gbit/s FC

Скорость генерации КК не менее 1 кбит/с (для линии связи с потерями 10 дБ (эквивалент 50 км))

Латенсия (Latency), мс 0,044

Резервирование Автоматическое переключение между линиями за время не более 50 мс

Коррекция ошибок (FEC): ITU-T G.709/ITU-T G.975.1

Пример сетевого решения «Точка-Точка» для МШ-ТР КРК представлено рис.3.22.

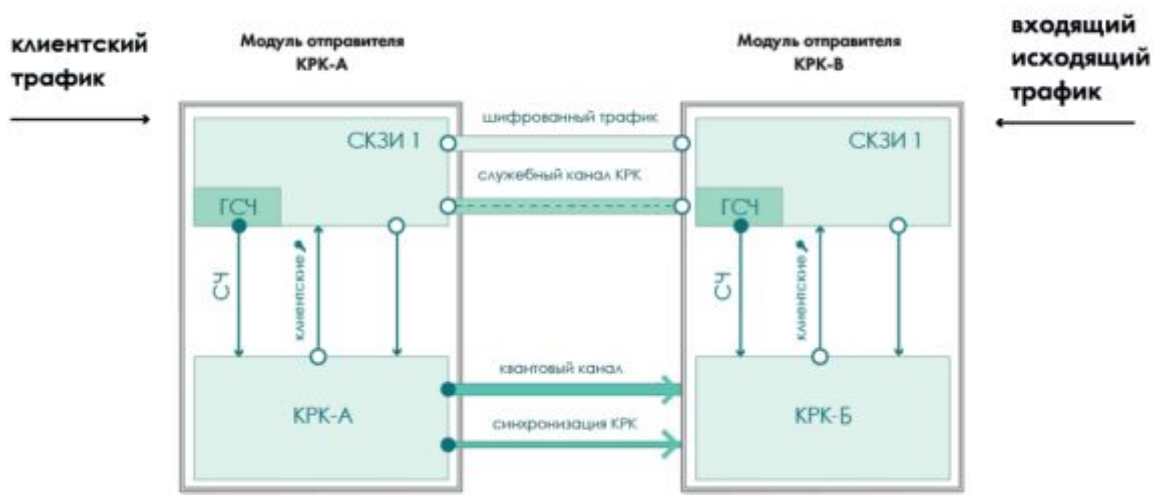
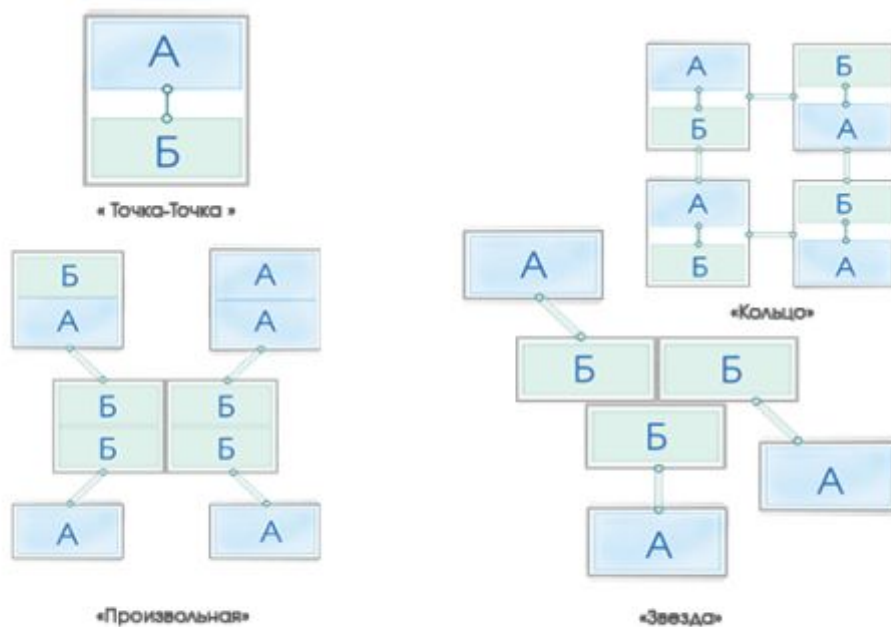


Рис.3.22. Сетевое решение «Точка-Точка» для МШ-ТР-КРК

Другие возможные сетевые решения представлены на рис.3.23.



Образец ККС ВРК изготовлен на собственной производственной базе.
Оборудование доступно для заказа, по всем вопросам обращайтесь по телефону или
заполните форму обратного звонка на сайте.

Рис.3.23. Возможные сетевые решения с применением МШ-ТР-КРК

Более сложные топологии чем «Точка-точка» предполагают использование доверенного узла (рис.3.24).

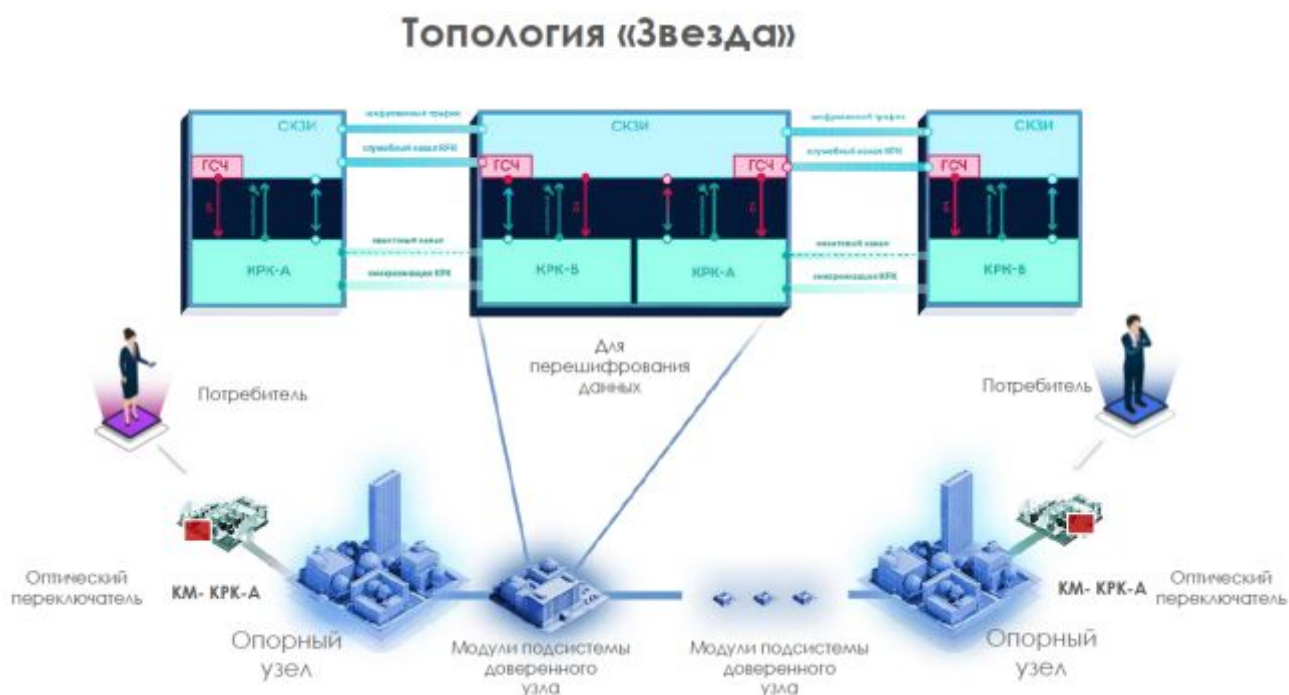


Рис.3.24. Сетевое решение с модулем доверенного узла

3.6.4. Примеры зарубежного оборудования ККЗ

На рынке систем квантовой коммуникации сегодня доминируют три компании: китайские **Qasky** и **QuantumCTek**, а также швейцарская **ID Quantique** (рис.3.25).

Clavis² та Cerberis (ID Quantique, Швейцария)



Криптосистема Clavis²

- Автокомпенсирующая оптическая платформа обеспечивает стабильность и низкий уровень квантовых ошибок;
- Защищенное распределение ключей шифрования между двумя абонентами на расстояние до 100 км;
- Рыночная стоимость системы около € 90 тыс.



Криптосистема Cerberis

- Сервер с автоматическим созданием и секретным обменом ключами по оптоволоконному каналу до 50 км;
- 12 параллельных криптовычислений;
- Шифрование протоколом AES (256 бит), а для КРК - протоколы BB84 и SARG;
- Ориентировочная стоимость такой системы на рынке € 70 тыс.

Рис.3.25. Зарубежные виды оборудования квантовых коммуникаций

Объем рынка квантовой криптографии в 2018 году оценивался в 101 миллион долларов, в 2023 году он вырос до 506 миллионов долларов.

Компания ID Quantique является лидером этого рынка и предлагает два типа систем квантовой криптографии: на основе двунаправленной схемы (**plug and play**) и когерентной однопроходной на базе протокола **COW** (его безопасность пока не доказана).

Эти устройства рассчитаны на работу на городских волоконно-оптических сетях и дают возможность генерации квантовых ключей на расстояниях до 70 километров.

Компания Qasky занимается разработкой решений для государственных и силовых структур, поэтому ее продукции нет на открытом рынке.

Компания QuantumSTek в 2018 году представила линейку устройств для городских сетей: системы генерации ключей, совместимые коммутаторы, устройства для телефонии.

Главными клиентами производителей систем квантовой криптографии являются в основном банки и финансовый сектор, государственные и силовые структуры, центры обработки данных.

Особенно быстро квантовые сети развиваются в Китае. Квантовое оборудование установлено в крупнейших банках Китая и других финансовых компаниях, сервисных компаниях в области безопасности.

На основе оборудования компании QuantumSTek в Китае создана квантовая сеть суммарной протяженностью 6000 километров. А продукция компании ID Quantique эксплуатируется пятеркой крупнейших банков Швейцарии.

Совместно с компанией Battelle швейцарская компания также участвует в строительстве магистральных сетей в США. Информация об объемах ее продаж публично не представлена. Капитализация компании в настоящий момент составляет около 150 миллионов долларов.

3.7. Построение квантово-защищённых оптических сетей

Волоконно-оптические сети и защита соединений с ключами QKD для всех соединений (магистральных, региональных – городских, доступа и клиентских терминалов) предусматривается в перспективе развития квантовых коммуникаций (рис.3.26).

Для полноценной реализации квантово-защищённых сетей необходимо создание сетей провайдеров квантовых ключей (рис.3.27.).

Поскольку сеть с распределением квантовых ключей QKD построена с узлами трансляции, коммутации, разветвления ключей и доверенными узлами формирования ключей, то необходимо единое централизованное управление! Т.е. обязателен уровень управления (рис.3.28).

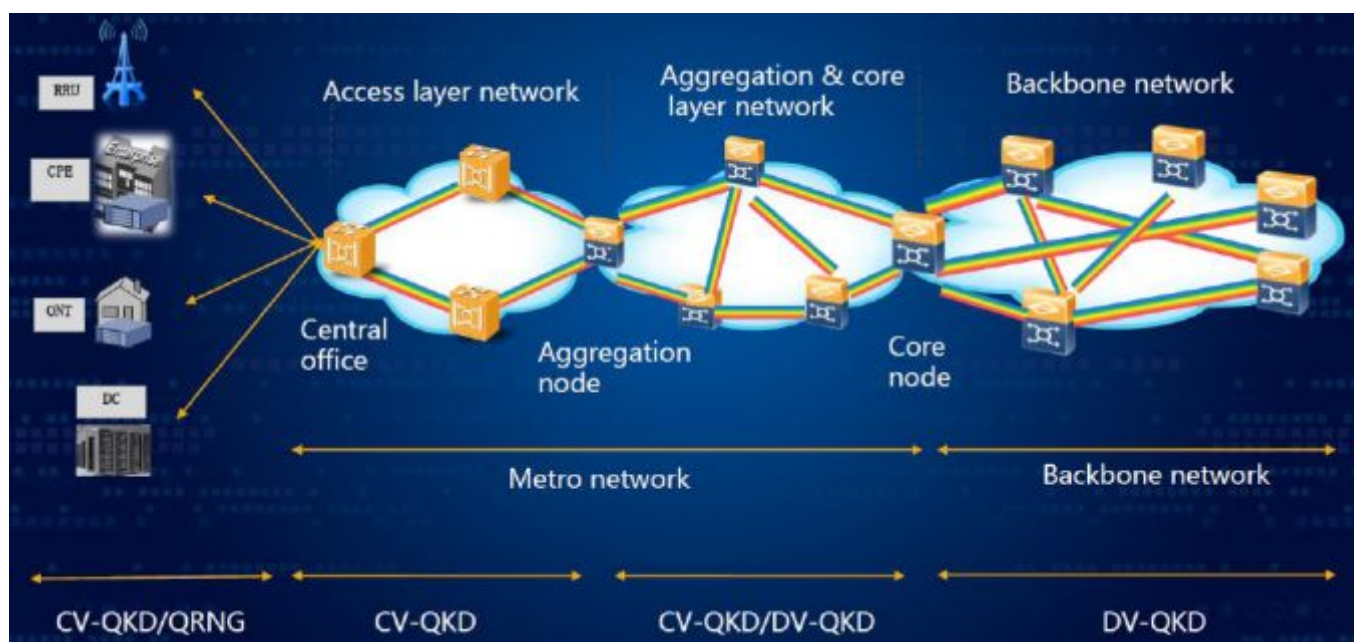


Рис.3.26. Сети с квантовыми ключами CV-QKD, Continuous-Variable QKD; DV-QKD, Discrete-Variable QKD; QRNG, Quantum Random Number Generator

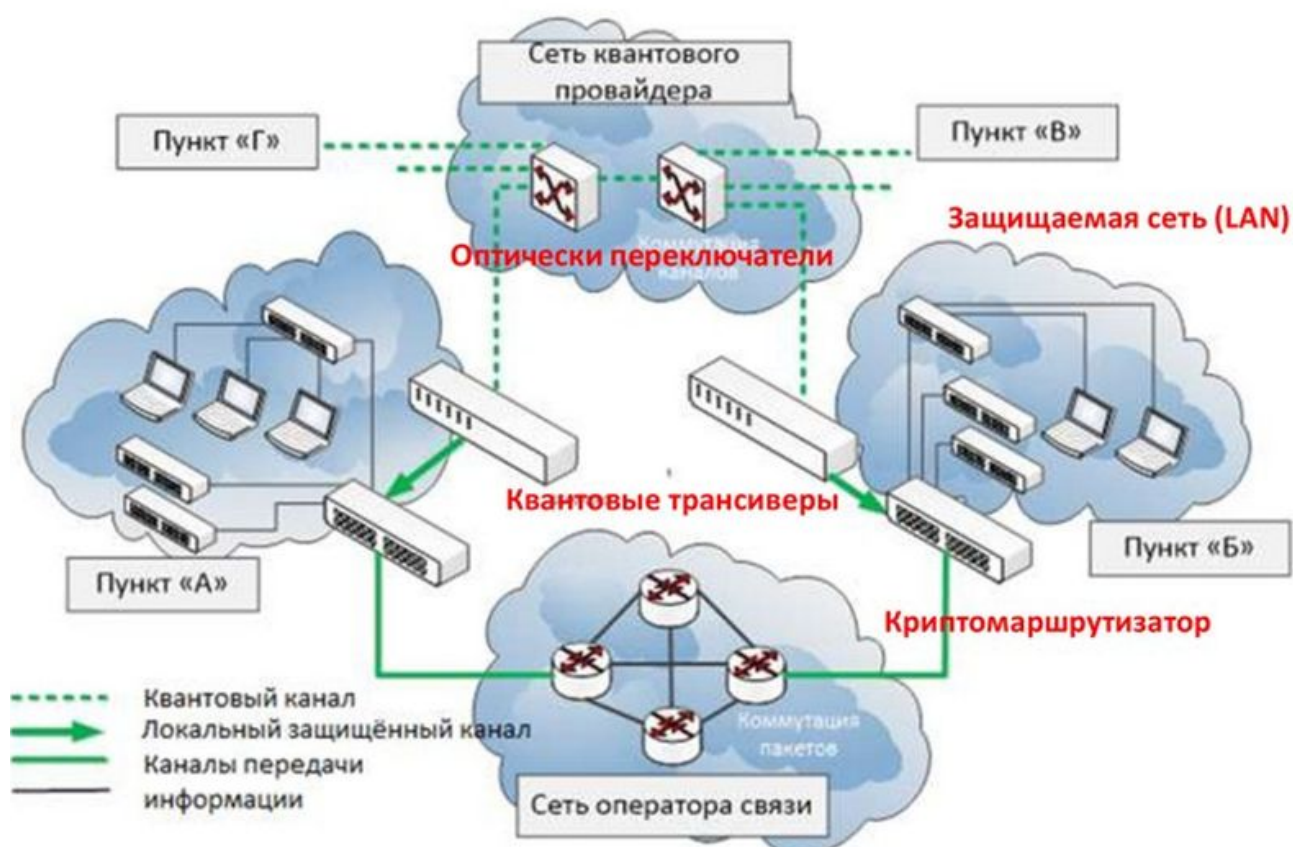


Рис.3.27. Необходимость создания сети квантового провайдера

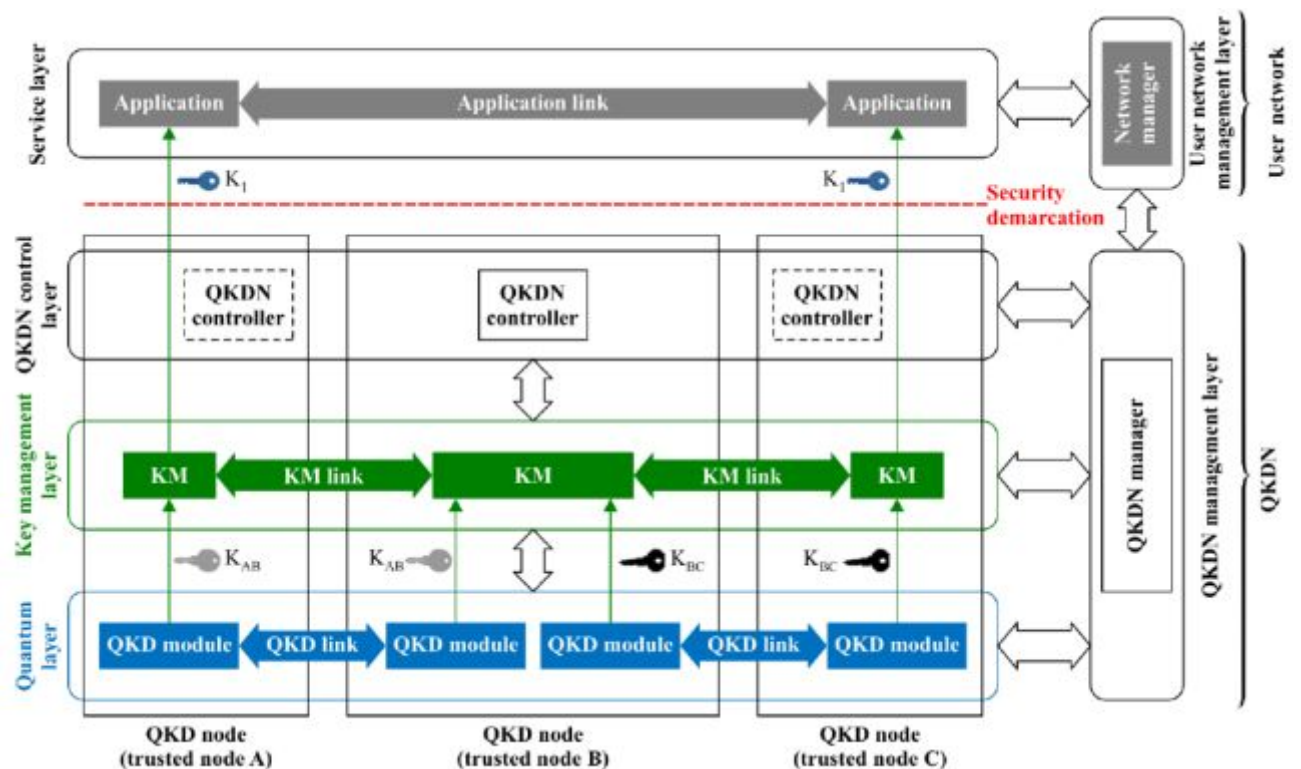


Рис.3.28. Структура модели оптической сети с функциями QKD и уровнем сетевого управления, предложенная в ITU-T

3.8. Проблемы шифрования и квантовых коммуникаций

Проблемы начинаются с не обеспечения безусловной секретности ключей.

Дорогостоящие организационно-технические меры.

Всегда есть «человеческий фактор».

Создание квантового компьютера приведет к компрометации всех асимметричных криптографических алгоритмов и протоколов на их основе (DH, RSA, ECDSA TLS/SSL, HTTPS, IPsec, X.509).

Зачем нужна быстрая смена ключей?

Для конкретного алгоритма шифрования в конкретном режиме работы для конкретного варианта реализации СКЗИ имеется предельное количество данных, которые допустимо зашифровать на одном ключе – **нагрузка на ключ**

Пример:

Алгоритм блочного шифрования по ГОСТ 28147-89

Размер блока $n = 64$ бит

Предельная теоретическая нагрузка $2^{64}/2 = 2^{63}$ блоков шифротекста, или 256 Гбит данных

Шифратор на скорости 10 Гбит/с израсходует ключ за 25 секунд

Для квантовых коммуникаций прежде всего, **существуют физические ограничения**, обусловленные затуханием луча лазера в оптическом канале. Поэтому как минимум через 400 км нужно устанавливать повторитель, причем он должен находиться в доверенной среде. Над устройствами для работы в

недоверенной среде ученые ломают головы, но пока прорывов нет. Но все же благодаря государственной поддержке инфраструктура строится.

Сложнее ситуация с предоставлением квантовых услуг. **Оборудование дорогое**, а большинство компаний исповедует принцип «пока гром не грянет, мужик не перекрестится». Квантового компьютера, способного взломать используемые средства криптографии (своего рода «черного лебедя»), пока нет, и не очевидно, что в ближайшие годы он появится. Теория взлома сообщений, зашифрованных с помощью алгоритма RSA, известна давно – достаточно применить квантовый алгоритм Шора и иметь компьютер с сотней тысяч кубитов. Но создание такого компьютера – задача крайне сложная. Сегодня самая мощная квантовая система обладает мощностью 433 кубита.

Однако работы продолжаются, и повод для беспокойства есть. В декабре прошлого года группа китайских исследователей опубликовала **методику взлома** ключа RSA-48. Китайцы взяли за основу методику Клауса-Питера Шнорра и так оптимизировали алгоритм, что для дешифровки ключа RSA длиной 48 бит хватило 10-кубитного компьютера. Ученые утверждают, что при использовании их методики для взлома 2048-битного ключа понадобится всего 372 кубита. А такие квантовые компьютеры уже есть.

Другие проблемы связаны с оборудованием (рис.3.29), которое после введения санкций стало невозможно купить. Нужны аппаратные шифраторы и дешифраторы, лазеры, испускающие последовательности фотонов, и приемники, способные их принять и проанализировать. И это не говоря уже об используемых в устройствах процессорах «Байкал», которые оказались недоступны после того, как Тайвань присоединился к санкциям. Появилось понимание, что в дальнейшем придется полагаться только на свои силы.

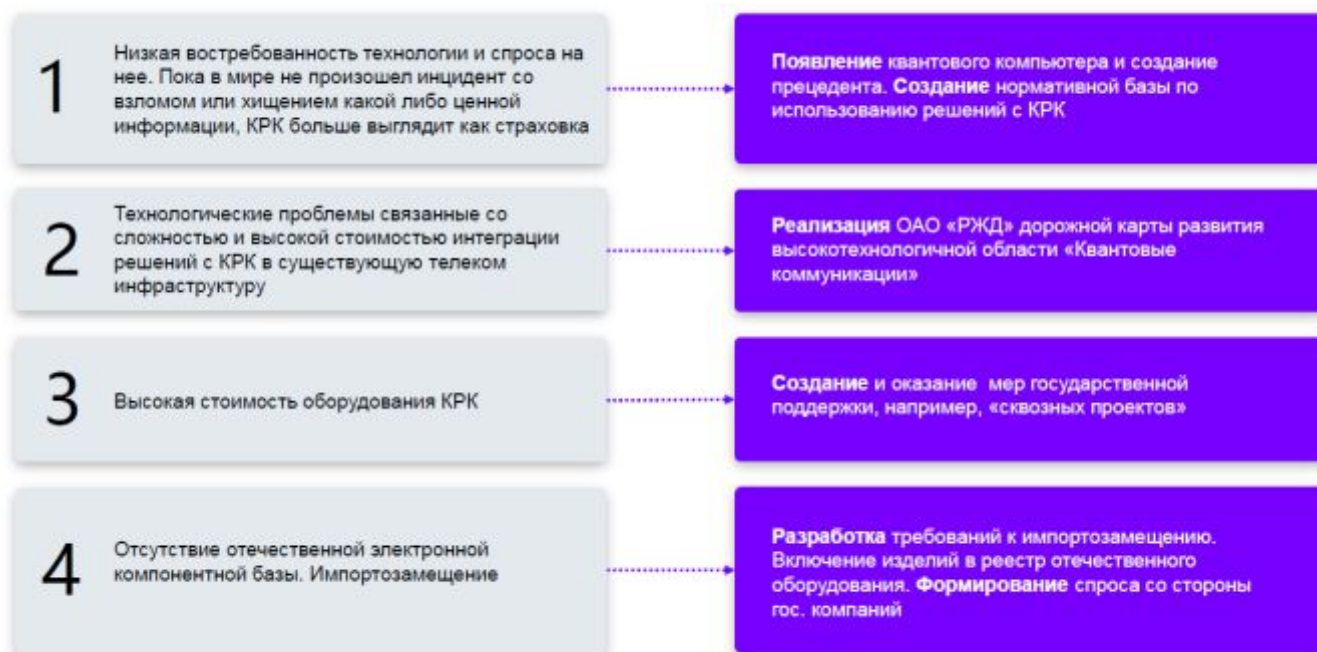


Рис.3.29. Проблемы квантовых коммуникаций и возможные решения

3.9. Постквантовая криптография

Постквантовая криптография — это новое поколение криптографических алгоритмов, которые оказываются устойчивыми как к атакам с применением традиционных вычислительных архитектур, так и к атакам с применением квантовых компьютеров.

По сравнению с традиционными алгоритмами, постквантовые используют другие математические принципы. Квантовая и постквантовая криптографии дополняют друг друга, как аппаратные и программные решения в классической криптографии. Если посмотреть, как это применяется на практике, мы увидим, что квантовая криптография подходит для защиты высоконагруженных каналов связи и каналов, по которым передается стратегически ценная информация. Например, между банковскими офисами, дата-центрами или видеоконференции топ-менеджмента. В это же время постквантовая криптография может решить задачи по безопасности ненагруженных каналов.

Постквантовая криптография — новые криптографические алгоритмы, устойчивые к кибератакам с применением квантовых компьютеров.

В настоящее время международное криптографическое сообщество выбирает наиболее оптимальные постквантовые алгоритмы, но это не мешает реализации и пилотированию решений с использованием уже проверенных квантово-устойчивых алгоритмов.

Разрабатываемые и используемые сегодня квантово-устойчивые решения информационной безопасности на основе постквантовых алгоритмов не заменяют традиционные методы шифрования, а усиливают их.

Постквантовые криптографические алгоритмы основаны на специальном классе математических преобразований, инвертирование которых представляет большую сложность, как для классических, так и для квантовых компьютеров. Использование постквантовых алгоритмов для передачи и хранения данных позволит повысить безопасность информации, жизненный цикл которой превышает 5 лет. В горизонте нескольких лет полностью небезопасными становятся многие традиционные алгоритмы криптографии: распределение ключей (ECDH, DH); асимметричное шифрование (RSA); электронная подпись (ECDSA, DSA, ГОСТ Р 34.10-2012).

Контрольные вопросы

1. Что следует понимать под квантовыми коммуникациями?
2. Для чего нужна сеть КРК?
3. Что обозначает QKD?
4. Какие уровни характеризуют сеть QKD с доверенными промежуточными узлами?
5. В чём состоит главная идея квантовой криптографии?
6. Какие квантово-механические принципы положены в основу квантовой криптографии?
7. Какие каналы необходимы для реализации квантовой криптографии?

8. Какие процедуры предусмотрены для формирования квантового ключа?
9. По каким направлениям развиваются алгоритмы квантовой криптографии?
10. Чем отличаются направления развития алгоритмов квантовой криптографии?
11. Какие протоколы формирования и распределения квантовых ключей являются базовыми по двум направлениям?
12. Какие этапы формирования квантового ключа предусмотрены в алгоритме BB84?
13. Чем отличается «сырой» квантовый ключ от «просеянного» ключа?
14. В результате каких операций формируется квантовый ключ?
15. Что следует понимать под «запутанным» состоянием фотонов?
16. В чём состоит метод протокола E91?
17. Сколько состояний поляризации используют фотоны в протоколе B92?
18. Для чего необходим провайдер квантовой сети?
19. Что входит в уровень управления QKDN?
20. В каких транспортных сетях применим QKD?
21. В чём состоят проблемы квантовых коммуникаций?
22. Как можно попытаться решить проблемы квантовых коммуникаций?
23. Что предусмотрено планами РЖД по развитию квантовых коммуникаций?
24. В чём необходимость применения постквантовой криптографии?
25. Какая особенность отмечается у модуля Квазар СКР?
26. Какой уровень оптической транспортной сети поддерживают модули Квазар СКР?
27. Какие возможности реализуют модули Квазар СКР кроме криптозащиты?
28. В чём состоят недостатки модулей Квазар СКР?
29. Какие скорости для клиентских интерфейсов поддерживают модули Квазар СКР?
30. Для чего предназначена система ViPNet Quandor?
31. Какая компания разработала систему ViPNet Quandor?
32. Что обозначает ViPNet L2Q-10G?
33. Что такое ККС ВРК?
34. С какой скоростью вырабатываются ключи в системе ViPNet Quandor?
35. Что относится к оборудованию ViPNet Quandor?
36. Что необходимо для удалённого взаимодействия устройств ViPNet Quandor?
37. Сколько соединений требуется для применения ViPNet Quandor?
38. Какие режимы работы предусмотрены для ViPNet Quandor?
39. Как происходит загрузка квантовых ключей шифрования в ViPNet Quandor?
40. Как часто запускается выработка квантового ключа?
41. Что относится к линейке оборудования ИнфоТекс?
42. Что относится к техническим характеристикам ViPNet Quandor?
43. Как можно скомпроментировать систему шифрования ViPNet Quandor?
44. Где размещаются доверенные промежуточные узлы сети КРК?

45. Что представляет собой разработка «Смартс-Кванттелеком» для КР КБЧ?
46. В чём преимущество разработки КР КБЧ?
47. Какой протокол используется для генерации квантовых ключей в системе «Смартс-Кванттелеком»?
48. Какие процедуры формирования ключа шифрования выполняются при реализации КР КБЧ?
49. С какой скоростью генерируется квантовый ключ КБЧ?
50. Какие клиентские интерфейсы поддерживает оборудование МШ-ТР-КРК?
51. Какие функции поддерживает ККС ВРК?
52. Какие сетевые решения возможны в реализации ККС ВРК?
53. Какое шифрование применено в криптосистеме Cerberis?
54. Что меняется на рынке оборудования квантовых коммуникаций?
55. Для чего нужен провайдер квантовых ключей?

Задача 3.

Используя квантовый ключ шифрования (табл.1) составьте зашифрованное в двоичном коде слово для передачи в оптическом канале в формате линейного кодирования NRZ. Квантовый ключ шифрования представлен шестнадцатеричным числом, которое необходимо перевести в двоичный восьмиразрядный код и побитно сложить по модулю два с буквами слова в двоичном формате, взятого по варианту из табл.2. Кодирование букв по формату UTF-8 приведено в табл.3.

Табл.1. Номер варианта соответствует предпоследней цифре студенческого билета или номера пароля

Вариант	0	1	2	3	4	5	6	7	8	9
Квантовый ключ шифрования	25	29	33	37	3D	65	6B	72	79	7D

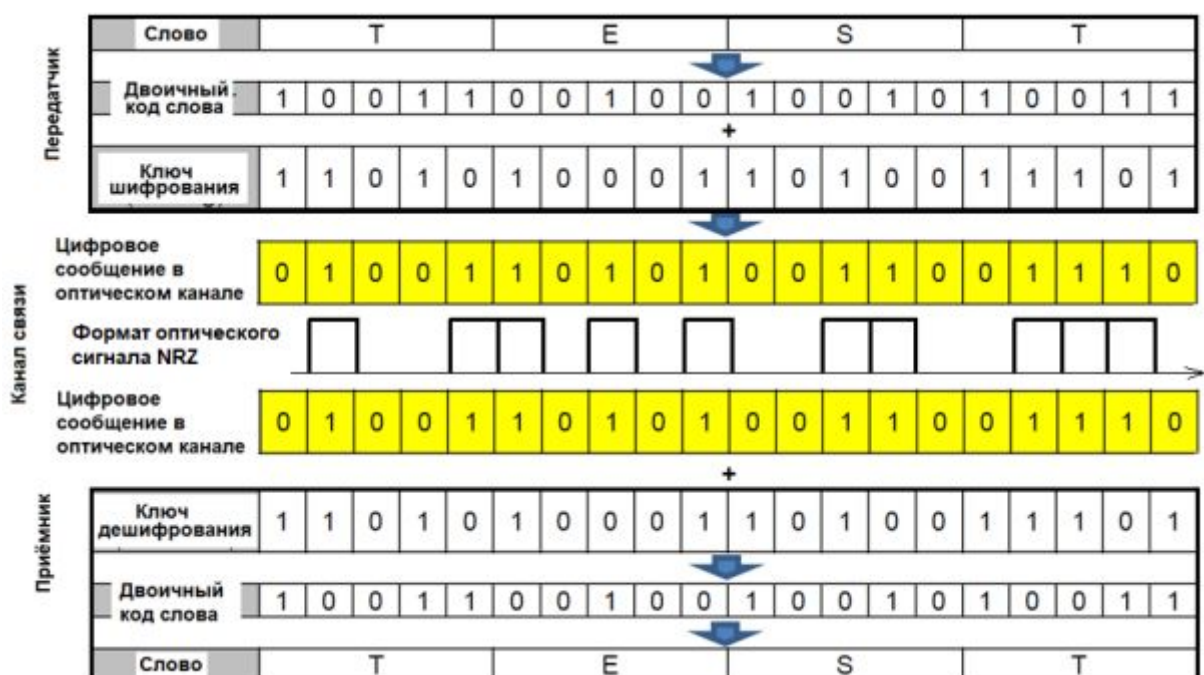
Табл.2. Номер варианта соответствует последней цифре студенческого билета или номера пароля

Вариант	0	1	2	3	4	5	6	7	8	9
Шифруе мое слово	LAUN CH	POW ER	CHANN EL	NONLINEA RITI	MODULAT ION	DISPERSI ON	DESIGN ET	MANA GE	PHA SE	LIMIT ED

Табл.3. Unicode Transformation Format, 8-bit (UTF-8)

Двоичный код	Десятичный код	Шестнадцатеричный код	Буквенный знак
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z

Пример графического решения задачи 3 с упрощенным представлением



4. Инженерная инфраструктура центров обработки данных, кабельная инфраструктура и способы защиты соединений

Сегодня практический интерес к вопросам построения ЦОД проявляют разные структуры от небольших компаний до гигантских транснациональных корпораций и операторов связи. Значимость хранимой и обрабатываемой в ЦОД информации выдвигает самые серьезные требования ко всем его подсистемам.

В мае 2023 года Минцифры РФ совместно с крупнейшими операторами связи представили стратегию развития отрасли до 2035 года. Среди прочего в документе говорится о перспективах развития в России небольших центров обработки данных. Речь идет о небольших дата-центрах, которые в отличие от корпоративных и коммерческих ЦОДов на десятки тысяч серверов могут устанавливаться вместе с базовыми станциями вблизи жилых домов или промышленных предприятий, а также в районах массового скопления людей. К концу этого отрезка времени на мини-ЦОДы будет приходиться 30% вычислений в России.

Этапы развития

Первая волна массового строительства центров обработки данных (ЦОД) пришлась на конец 90х годов прошлого века времена хорошо известного Интернет бума. Последующий затем кризис в телекоммуникационной отрасли несколько приостановил "победоносное шествие" ЦОД по планете, однако в настоящее время интерес к ним снова очень велик. Рост объемов и ценности информации, быстрое развитие различных форм электронных коммуникаций (электронная и голосовая почта, IP телефония, чаты, мгновенный обмен сообщениями и пр.), разнообразие видео сервисов эти и многие другие факторы способствуют росту числа и размеров ЦОД.

Их строят как крупные предприятия и другие корпоративные структуры, так и сервис провайдеры. В корпоративных ЦОД располагаются системы хранения и обработки собственной информации компаний, а также сетевое и телекоммуникационное оборудование, необходимое для функционирования корпоративных локальных (ЛВС) и территориально распределенных (WAN) сетей. В ЦОД сервис провайдеров и операторов связи располагаются средства связи и другое оборудование, необходимое для предоставления ими услуг своим абонентам. Кроме того, часть ресурсов таких ЦОД может выделяться для размещения оборудования и программных систем заказчиков на принципах аутсорсинга.

Что такое ЦОД?

ЦОД представляет собой технологическое помещение, в котором размещаются системы хранения данных, их обработки (серверы), а также сетевое и телекоммуникационное оборудование. Он может занимать одну или несколько комнат, а также целиком все здание. Кроме того может размещаться в контейнере

для любых климатических условий. Для работы современной электронной аппаратуры требуется довольно жесткий температурно-влажностный режим, поэтому обязательной в современном ЦОД является система обеспечения такого режима (кондиционирование и вентиляция). Требовательна аппаратура и к качеству электропитания, что достигается установкой источников бесперебойного питания (ИБП) необходимой мощности и альтернативных источников электричества (аккумуляторные батареи, дизель генераторные установки и пр.). Размещают серверы, системы хранения и сетевые устройства в специальных монтажных стойках и шкафах, которые должны быть достаточно надежными и удобными для обслуживания аппаратуры. Не менее важными для нормального функционирования ЦОД являются система обеспечения безопасности (контроль доступа, видеонаблюдение и т. д.), а также система контроля и управления инженерными средствами. Все это обязательно должно быть предусмотрено еще на этапе проектирования таких объектов.

Конечно, нельзя забывать и о кабельной системе. Именно она служит своеобразной кровеносной системой, которая связывает воедино все, начиная от основного оборудования и заканчивая датчиками и контроллерами инженерных средств, и превращает ЦОД в единый "организм". А, как известно, любые проблемы в работе кровеносной системы чреваты летальным исходом, т. е. в нашем случае остановкой работы ЦОД. Поэтому к вопросам проектирования, инсталляции и обслуживания кабельной системы надо подходить максимально внимательно, учитывая ряд специфических требований ЦОД, что делает их кабельные системы несколько отличными от офисных СКС.

ЦОД и стандарты

В последнее время одним из наиболее часто цитируемых является стандарт на ЦОД TIA942, принятый в США. Однако существуют также европейский стандарт EN 501735 и основанный на нем международный стандарт ISO/IEC 24764. Американский стандарт TIA942 охватывает широкий круг вопросов, связанных с организацией ЦОД, включая: характеристики помещения (размеры, высота потолка, двери, освещение, нагрузка на пол...); принципы построения системы кондиционирования и электропитания; требования по резервированию различных элементов; принципы построения кабельной системы; Европейский стандарт EN501735 рассматривает только вопросы, связанные с построением кабельной системы. Хотя положения стандартов TIA942 и EN 501735 в части кабельной системы ЦОД схожи, имеются и некоторые отличия.

Стандарты России для ЦОД:

ГОСТ Р 70627–2023 Центры обработки данных. Инженерная инфраструктура. Документация. Техническая концепция. Требования к составу и содержанию;

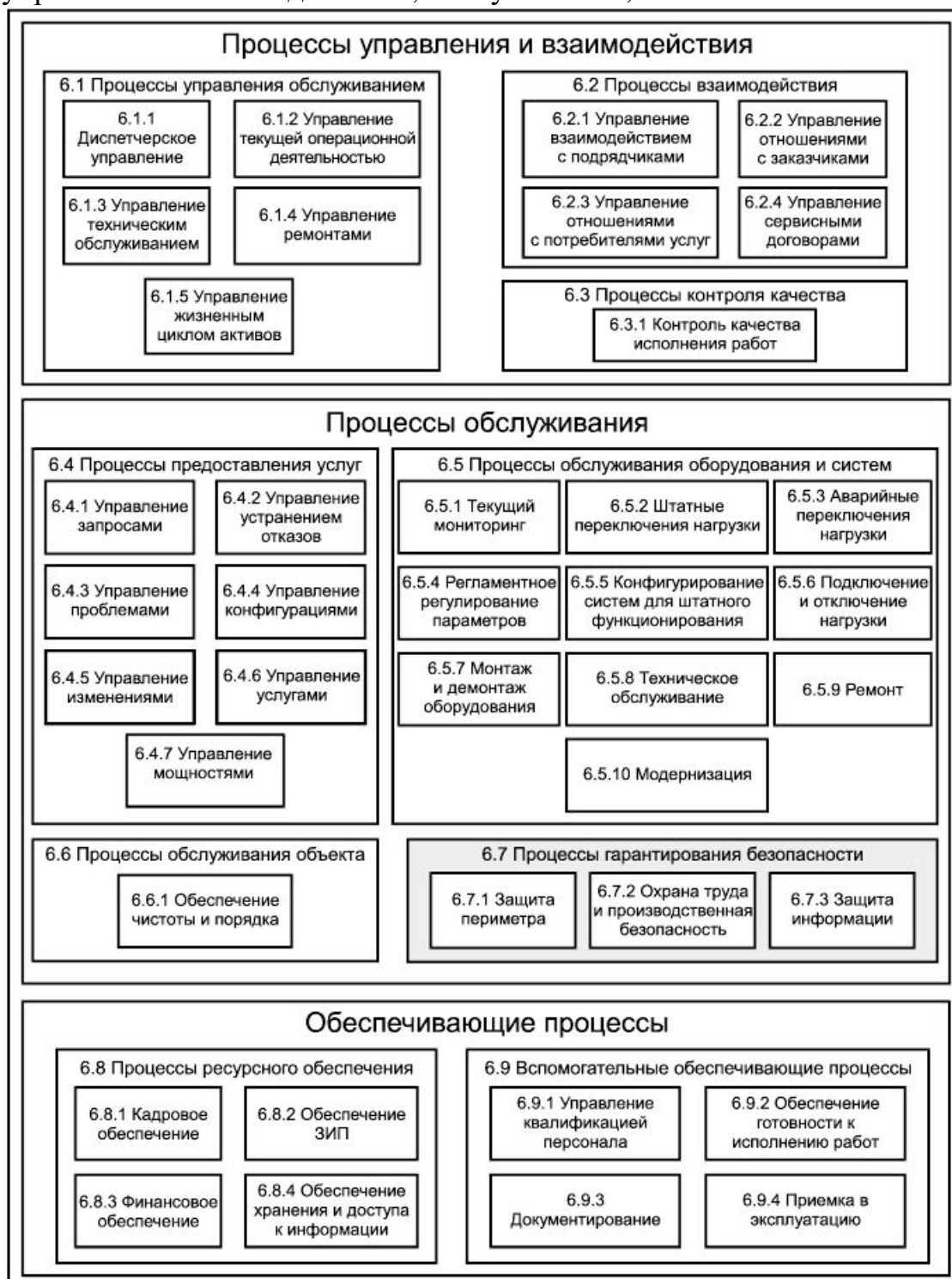
ГОСТ Р 70139—2022 Центры обработки данных . Инженерная инфраструктура. Классификация;

ГОСТ Р 58812-2020 Центры обработки данных. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация;

ГОСТ Р 58811-2020 Центры обработки данных. Инженерная инфраструктура. Стадии создания.

Защита корпоративной информации стоит на первом месте для многих компаний. И здесь нельзя идти на компромиссы: потеря важной информации или ее попадание в руки злоумышленников чреваты громадными убытками, а, возможно, и разорением компании.

Операционная модель ЦОД по стандарту отражает три группы процессов: управления и взаимодействия; обслуживания; обеспечения.



Термины и определения

центр обработки данных: Специализированный объект, представляющий собой связанную систему ИТ-инфраструктуры и инженерной инфраструктуры, оборудование и части которых размещены в здании или помещении, подключенном к внешним сетям, как инженерным, так и телекоммуникационным.

Примечание: При необходимости здание ЦОД может иметь прилегающую территорию.

инженерная инфраструктура центра обработки данных: Комплекс систем и их оборудования, обеспечивающих бесперебойное функционирование систем и оборудования ИТ-инфраструктуры ЦОД.

служба эксплуатации центра обработки данных: Организация или ее подразделение, в обязанности которым вменяется проведение работ по эксплуатации систем и оборудования центра обработки данных.

подразделение эксплуатации инженерной инфраструктуры центра обработки данных: Структурное подразделение службы эксплуатации ЦОД, в обязанность которому вменяется проведение работ по эксплуатации систем и оборудования инженерной инфраструктуры ЦОД.

модернизация инженерной инфраструктуры ЦОД: Замена оборудования, относящегося к инженерной инфраструктуре ЦОД, или отдельных его комплектующих с целью изменения совокупных характеристик оборудования, систем и объекта в целом для обеспечения его соответствия установленным целевым значениям.

запрос: Обращение заказчиков, потребителей услуг, смежных эксплуатирующих структур, прочих внутренних или внешних контрагентов в службу эксплуатации ЦОД.

диспетчерское управление: Централизованная форма оперативного управления на основе применения технических средств связи, сбора информации, ее обработки, осуществления оперативного контроля и регулирования производства.

мониторинг: Методика и система наблюдений за состоянием определенного объекта или процесса, дающие возможность наблюдать их в развитии, оценивать, оперативно выявлять результаты воздействия различных внешних факторов.

операционная модель эксплуатации инженерной инфраструктуры ЦОД:

Описание набора необходимых элементов, применяемых способов и порядка реализации повседневной деятельности по эксплуатации инженерной инфраструктуры ЦОД.

Примечание - Она объясняет, каким образом эксплуатирующая структура организует и использует имеющиеся у нее ресурсы для того, чтобы изо дня в день исполнять текущие операции по эксплуатации ИИ ЦОД.

штатное функционирование системы: Состояние работы системы, в котором значения ее эксплуатационных параметров находятся в допустимых в соответствии с инструкцией по эксплуатации пределах.

мастер-план машинного зала: Схема (чертеж), отражающая основные объекты машинного зала, в том числе размещение оборудования инженерной инфраструктуры ЦОД в машинном зале, территории (площади), выделенные под различные цели, размещение ИТ-оборудования в машинном зале, аварийные и пожарные выходы, технологические коридоры и др.

Основные типы ЦОД

Модульные (шкафные).

Собирается из блоков, в которые входят в том числе инженерные системы. Дешевле, чем контейнерные, но дороже, чем классические ЦОД. Можно быстро развернуть и сравнительно просто масштабировать.

Контейнерные (рис.4.1).

По сути это тот же модульный Дата-центр, но в защищенном контейнере. Чаще всего применяется для организации ИТ-инфраструктуры в «поле» — на приисках, рудниках, раскопках. Разворачивается за считанные часы, часто комплектуется собственным источником питания и оборудованием для спутниковой связи.

Классические.

Подойдет для тех, кому важна максимальная безопасность данных или провайдером облачных услуг. Этот тип Дата-центра выгодно использовать, если вы уверены, что потребности компании в ИТ-ресурсах не вырастут в ближайшие несколько лет.

Облачные.

В этом случае арендуются аппаратные мощности провайдера. Фактически вы пользуетесь сервером поставщика услуг единолично или совместно с другими арендаторами. Легко масштабируется, выгоднее по сравнению с остальными вариантами. Не нужно тратить время на развертывание и запуск.

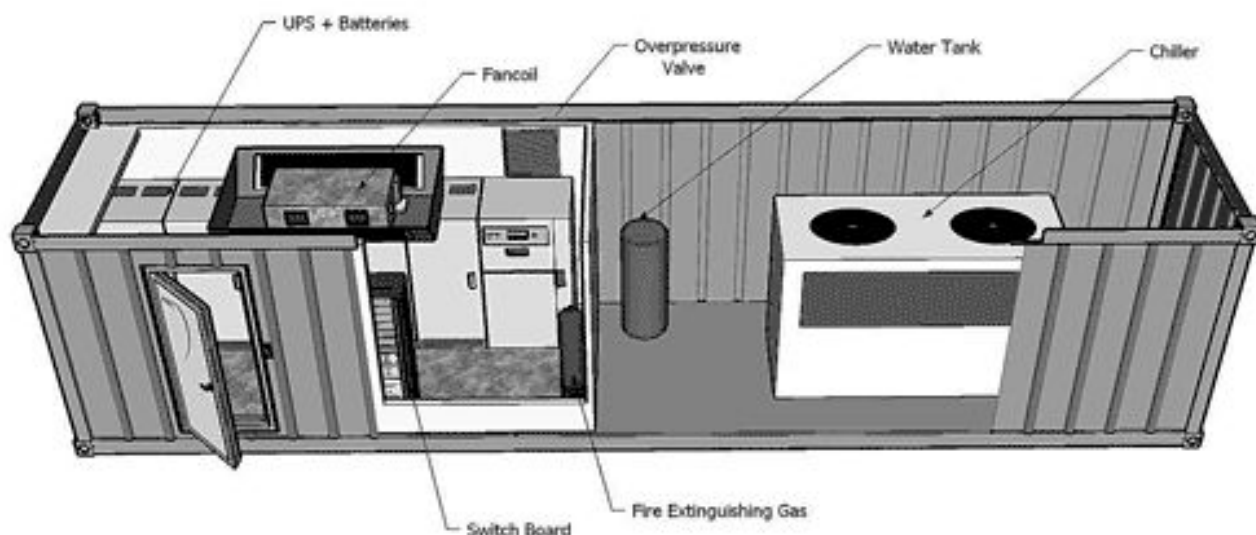


Рис. 4.1. Конструкция контейнерного ЦОД

4.1. Инженерная инфраструктура ЦОД. Основные компоненты

Инженерной инфраструктурой ЦОД называется совокупность технических компонентов, обеспечивающих основную поддержку работы и соблюдение комплекса условий эксплуатации оборудования вычислительного центра.

К основным условиям технической эксплуатации вычислительного оборудования относится обеспечение:

- общего электроснабжения;
- гарантированного электроснабжения;
- бесперебойного электроснабжения;
- поддержания климатических параметров в помещении;
- информационного взаимодействия вычислительного оборудования.
- Выполнение условий технической эксплуатации обеспечивается при

помощи построения соответствующих инженерных систем:

- системы общего электроснабжения;
- системы гарантированного электроснабжения;
- системы бесперебойного электроснабжения;
- системы вентиляции и кондиционирования ЦОД;
- структурированной кабельной системы и телекоммуникационного

оборудования.

В составе инженерной инфраструктуры ЦОД также выделяются системы, обеспечивающие удобство обслуживания, защиту устанавливаемого оборудования от несанкционированного доступа, защиту от повреждения вследствие пожара, затопления и т.д. Данные инженерные системы также являются очень важными, однако они выполняют вспомогательные (не основные) функции инженерной инфраструктуры ЦОД (рис.4.2):

система пожарной сигнализации и пожаротушения, предназначенная для своевременного обнаружения, локализации и тушения очага возгорания внутри ЦОД;

система охранной сигнализации, видеонаблюдения и контроля доступа, предназначенная для обеспечения регламентированного доступа к оборудованию ЦОД и визуального наблюдения за происходящим внутри ЦОД;

система закладных и кабельных каналов, предназначенная для защиты и упорядоченной прокладки слаботочных и силовых кабелей внутри ЦОД, а также трасс системы кондиционирования;

система электрического освещения, предназначенная для обеспечения основного и резервного освещения помещений ЦОД;

система мониторинга климатических параметров, предназначенная для сбора, обработки, хранения информации о состоянии климатических параметров внутри помещения ЦОД и т.д.



Рис.4.2. Круг инженерной инфраструктуры ЦОД

Пример инженерной инфраструктуры представлен на рис.4.3.

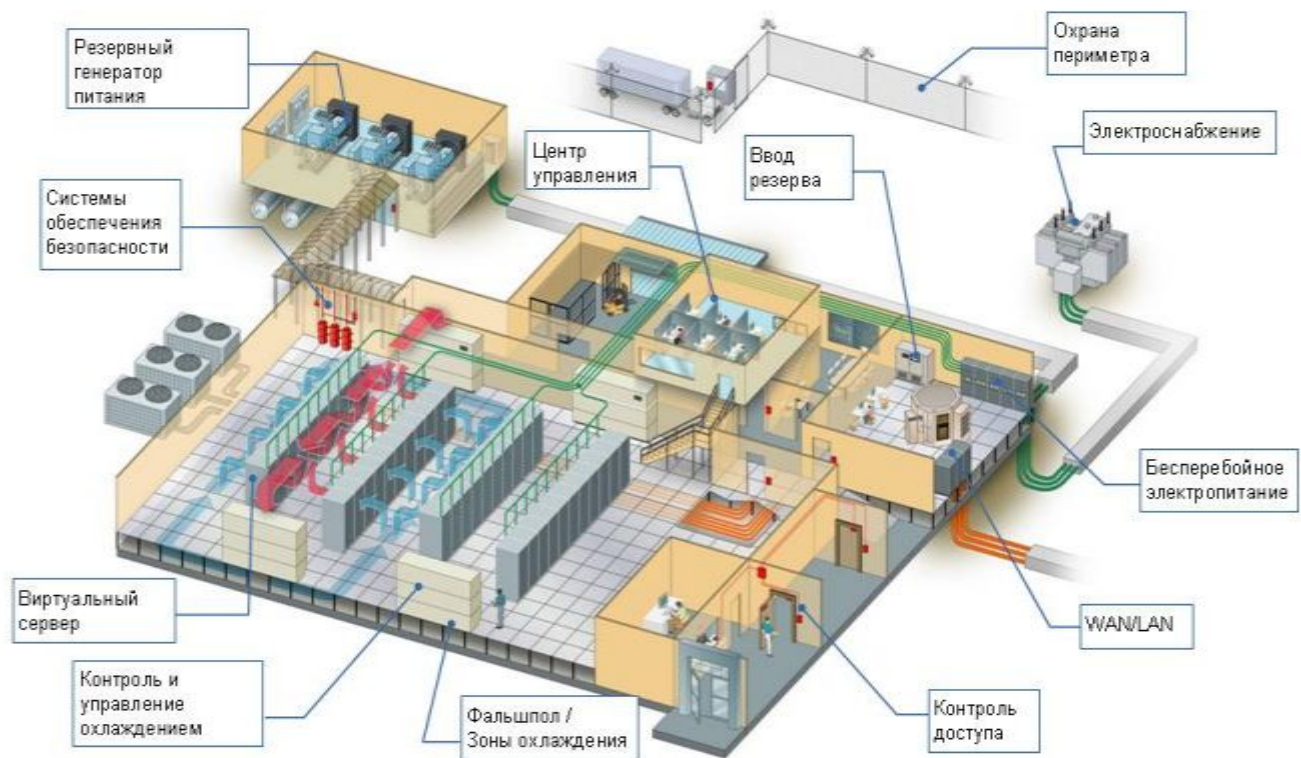


Рис.4.3. Пример инженерной инфраструктуры ЦОД

Структура ЦОД содержит в себе функциональные элементы, предназначенные для выполнения определенных задач работы центра обработки данных. Стандартом ANSI/TIA/EIA-942 определены следующие структурные элементы ЦОД:

- машинный зал;
- телекоммуникационные узлы, телекоммуникационная инфраструктура;
- узлы ввода кабельной инфраструктуры;
- коммутационные узлы;
- телекоммуникационная кабельная инфраструктура;
- электрическое и механическое оборудование технической поддержки ЦОД;
- помещения операторов;
- складские помещения ЦОД.

4.2. Структурированная кабельная система и телекоммуникационное оборудование ЦОД

Структурированная кабельная система предназначена для формирования единой среды передачи информации внутри ЦОД.

Поскольку передача и обработка данных является основной функцией устанавливаемого вычислительного оборудования ЦОД, то построение структурированной кабельной системы является одной из наиболее важных задач при его построении.

Ввиду важности данной системы и сложности ее топологии рассмотрение структурированной кабельной системы и используемого телекоммуникационного оборудования является предметом изучения, проектирования, инсталляции и обслуживания.

Подсистемы СКС имеют иерархическую структуру. В нее входят соединительные кабели («витая пара» или волоконно-оптические), коммутационные панели (с врезными контактами или модульными гнездами), коммутационные шнуры, разъемы, розетки, адаптеры. Монтажные шкафы и стойки, кабельные каналы в СКС не включаются, но могут поставляться с нею как готовое решение. Активное сетевое оборудование также не входит в состав СКС.

4.3. Обязательная разрабатываемая документация для ЦОД

1. Основные инженерно-технические системы: - электроснабжения; - холодоснабжения.

2. Вспомогательные инженерно-технические системы:

- - отопления, вентиляции и комфортного кондиционирования воздуха;
- - водоснабжения;
- - водоотведения;
- - *система кабеленесущих конструкций;*
- - *структурированная кабельная система;*
- - *охранно-тревожная сигнализация;*
- - *система контроля доступа;*
- - *видеонаблюдения;*
- - *видеоконференц-связи;*
- - *телефонной связи;*
- - регистрации переговоров;
- - голосового оповещения;
- - *радиосвязи;*
- - *электрочасофикации;*
- - *сбора и отображения информации;*
- - *автоматизированная система диспетчеризации и управления;*
- - газового пожаротушения;
- - пожарной сигнализации;
- - раннего обнаружения пожара.

4.4. Топологии ЦОД

Стандартом ANSI/TIA/EIA-942 приводятся три основных возможных варианта топологии ЦОД :

- редуцированная топология ЦОД;
- базовая топология ЦОД;
- распределенная топология ЦОД.

Редуцированная (сокращенная) топология – используется для построения небольших и средних ЦОД. Основными ее особенностями являются:
наличие одного (главного) коммутационного узла ЦОД;
совмещенные (конструктивно) главные коммутационные узлы здания и ЦОД.

На рис.4.4 приведен пример редуцированной топологии ЦОД.

Главные коммутационные узлы на схеме расположены в *главной распределительной зоне*.



Рис.4.4. Упрощенная топология ЦОД

Недостатками данной топологии является отсутствие разграничения доступа к коммутационным узлам ЦОД и здания, а также оборудованию провайдера услуг. Использование единого *коммутационного узла* приводит к появлению большого количества кабелей структурированной кабельной системы (СКС), сходящихся в *главной распределительной зоне*. При достижении определенного количества портов, требуемых для подключения оборудования, сильно усложняется эксплуатация ЦОД, в частности, переключение (коммутация) портов в *главных коммутационных узлах*. Поэтому при достаточно большом количестве требуемых портов СКС следует рассматривать *базовую топологию* ЦОД. ЦОД с редуцированной топологией часто используются в качестве резервных.

Базовая топология ЦОД (рис.4.5) – это помещение с определенной структурой. Оно может состоять из таких элементов, как:

Машинный зал, в котором размещается оборудование, связанное кабельной системой;

Комната ввода, которая подключается к одному или нескольким интернет-провайдерам;

Главная распределительная зона, в которой располагаются коммутаторы и маршрутизаторы;

Горизонтальная распределительная зона, связывающая элементы ЦОД с помощью кабелей;

Аппаратные зоны (например, серверные стойки и распределительные шкафы);

Кабельная система.

Подробнее: <https://www.cableman.ru/article/postroenie-sovremennogo-tsoda-s-nulya-chast-ii>



Рис.4.5. Базовая топология ЦОД

Распределенная топология – используется для построения отказоустойчивых ЦОД больших размеров. Ее особенностями являются:

дублирование структурных элементов (помещений ввода операторов услуг, главных коммутационных узлов, машинных залов и т.д.);

высокая отказоустойчивость и надежность ЦОД;

размещение в большом количестве помещений.

На рис.4.6 приведен пример распределенной топологии ЦОД.

Использование *распределенной топологии* позволяет повысить общую надежность ЦОД. Для подобной топологии характерно использование большого количества помещений, используемых под размещение структурных элементов ЦОД, а также избыточность структурных элементов. Данный вид ЦОД является наиболее устойчивым к различным аварийным ситуациям, в том числе и к пожарам.

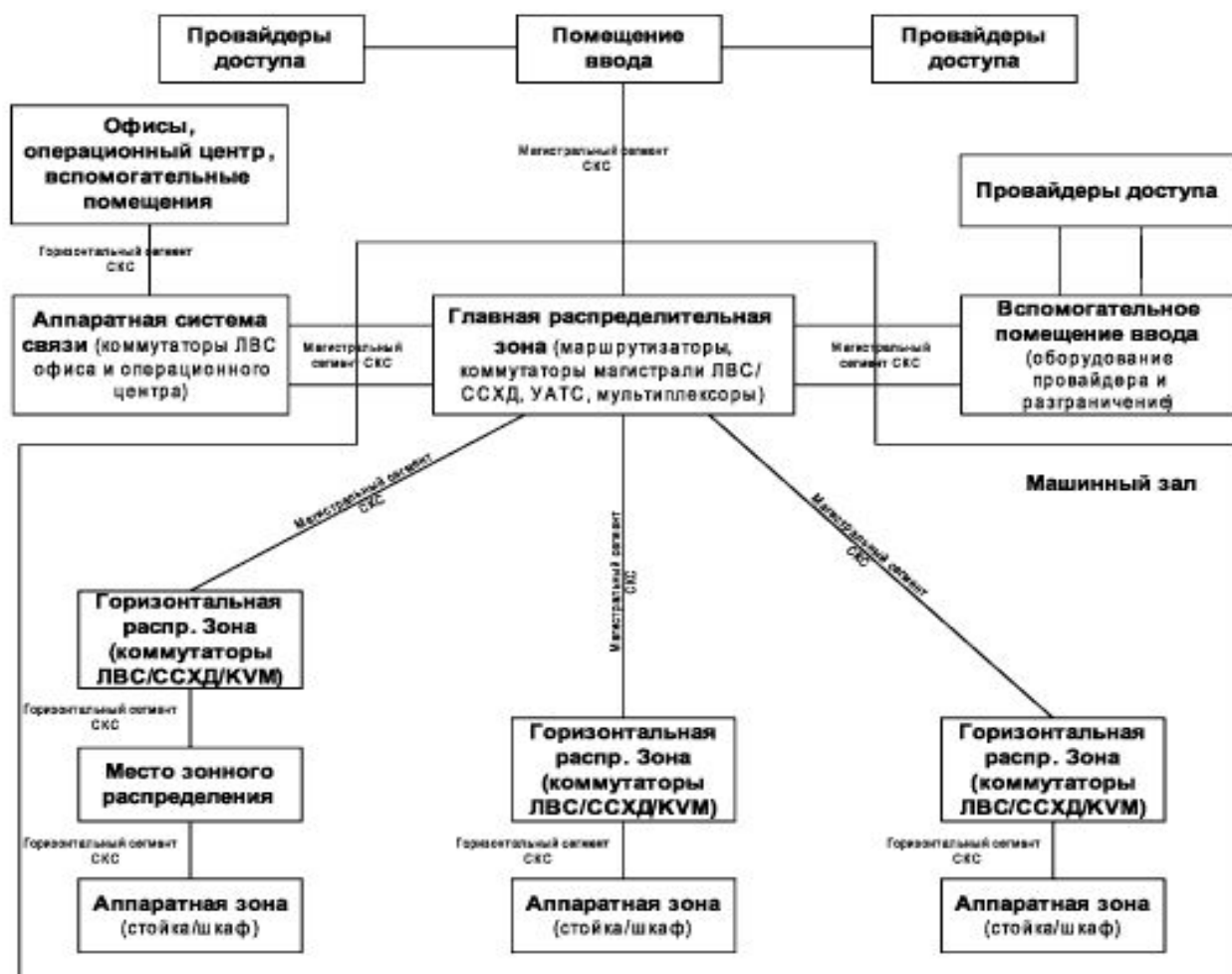
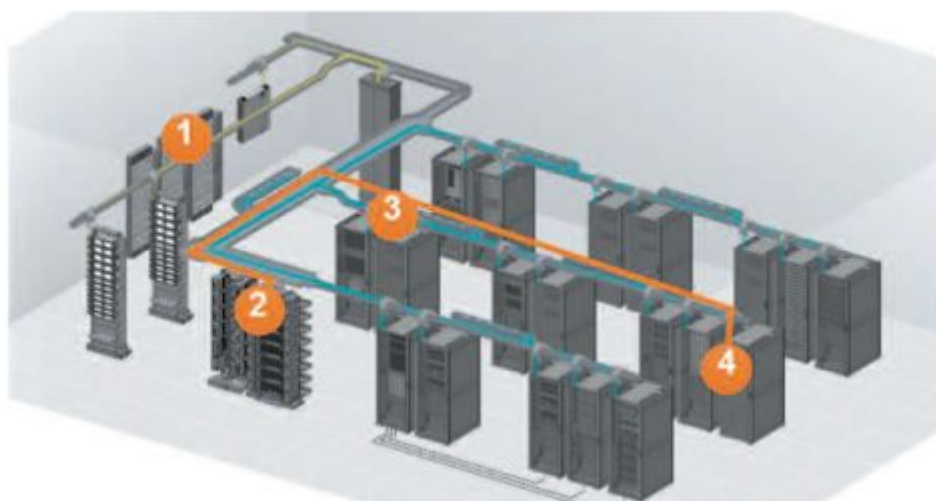


Рис.4.6. Распределённая топология ЦОД

4.5. Кабельная инфраструктура ЦОД

Телекоммуникационная кабельная инфраструктура ЦОД состоит из нескольких подсистем (1, 2, 3, 4). Пример приведён на рис.4.7. кабельные подсистемы делятся на внешние для взаимодействия с операторами телекоммуникационных сетей и между ЦОД соединений и внутренние для соединений оборудования электрическими и оптическими линиями.



Подсистема	Описание	Базовый состав
1 Entrance Facility	Городской ввод от операторов связи, одномодовые линии связи, кампусные магистрали в крупных ЦОДах	Оптический кросс операторского класса, одномодов., LC-APC, сварка
2 Main Distribution Area (Main Cross-Connect)	Главная распределительная область, главный оптический кросс	Многомодовые и одномодовые линии, наивысшие требования к пропускной способности
3 Main Distribution Area (Networking Core)	Главная распределительная область, ядро LAN, фабрика SAN	Многомодовые и одномодовые линии, наивысшие требования к пропускной способности
4 Horizontal and Equipment Distribution Areas	Горизонтальная и аппаратная распределительные области	Коммутационное оборудование для подключения серверов и СХД

Рис.4.7. Кабельные подсистемы ЦОД с четырьмя разновидностями

4.6. Функциональные узлы ЦОД

Машинный зал – помещение (помещения) предназначенные для размещения вычислительного оборудования ЦОД. Это основное помещение (помещения) ЦОД, определяющее его функциональное предназначение. Все остальные структурные элементы (размещаемые в машинном зале или в отдельных помещениях) обеспечивают работу вычислительного оборудования и соблюдение комплекса условий его функционирования.

Телекоммуникационные узлы, телекоммуникационная инфраструктура – структурные элементы, обеспечивающие передачу информации между вычислительным оборудованием. В их состав входят: **узлы ввода кабельной инфраструктуры, коммутационные узлы, телекоммуникационная кабельная инфраструктура.**

Узлы ввода кабельной инфраструктуры предназначены для обеспечения информационного взаимодействия и доступа к вычислительному оборудованию извне, посредством информационных каналов провайдеров.

Коммутационные узлы предназначены для осуществления коммутации (соединения/переключения) информационных каналов между вычислительным оборудованием. В их состав входит активное сетевое оборудование,

обеспечивающее переключение информационных каналов, и пассивное коммутационное оборудование в составе патч-панелей (или информационных розеток) и информационных кабелей. Подключение портов вычислительного (серверного) оборудования к активному сетевому оборудованию, расположенному в коммутационных узлах, осуществляется посредством *Телекоммуникационной кабельной инфраструктуры (Горизонтальной кабельной системы) и коммутационных панелей (или информационных розеток)*. Информационное взаимодействие между *коммутационными узлами* осуществляется посредством *Телекоммуникационной кабельной инфраструктуры (Магистральной кабельной системы) и коммутационных панелей*.

Электрическое и механическое оборудование технической поддержки ЦОД – включает в себя оборудование, обеспечивающее электроснабжение оборудования ЦОД (вычислительного и оборудования технической поддержки), соответствие климатических параметров помещений требованиям производителей оборудования, контроль и ограничение доступа и т.д.

4.7. СКС в ЦОД

Структурированная кабельная система (СКС) — основа информационной инфраструктуры предприятия, позволяющая свести в единую систему множество информационных сервисов разного назначения: локальные вычислительные и телефонные сети, системы безопасности, видеонаблюдения и т.д.

Кабельная система — это система, элементами которой являются кабели и компоненты, которые связаны с кабелем. К кабельным компонентам относится все пассивное коммутационное оборудование, служащее для соединения или физического окончания (терминирования) кабеля — телекоммуникационные розетки на рабочих местах, кроссовые и коммутационные панели (жаргон патч-панели) в телекоммуникационных помещениях, муфты и сплайсы.

СКС представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы.

Она состоит из набора медных и оптических кабелей, кросс-панелей, соединительных шнуров, кабельных разъемов, модульных гнезд, информационных розеток и вспомогательного оборудования. Все перечисленные элементы интегрируются в единую систему и эксплуатируются согласно определенным правилам.

Структура СКС современной структуры центра обработки данных (ЦОД):

Главная подсистема, выполняющая роль распределительной - MDA / Main Distribution Area. Она обеспечивает интерфейс доступа в центр, а также делит трафик, поступающий по главной магистрали, между внутренними магистралями. В MDA входят маршрутизаторы, оборудование операторов связи, магистральные коммутаторы и т. д.

Горизонтальная подсистема, распределяющая трафик из внутренней магистрали по локальным линиям, длина которых может быть не более 100 метров (HDA / Horizontal Distribution Area). Данные локальные линии выходят в аппаратные зоны. В данной подсистеме используется пассивное оборудование, а также коммутаторы KBM, коммутаторы ЛВС и другие элементы;

Подсистема разводки трафика по оборудованию (EDA / Equipment Distribution Area). Она отвечает за доставку трафика в рабочие области дисковых массивов, серверов и другого оборудования. Если в области требуется частая переконфигурация, то могут быть использованы ZDA - зонные сегменты с узлами консолидации.

Таким образом, структурированная кабельная система для центра обработки данных представляет собой часть комплексного сложного инженерно-информационного решения.

Особенности подсистем СКС ЦОД

Внутри главной подсистемы (Main Distribution Area) и для её соединения с горизонтальной (HDA) для магистралей необходим кабель с максимальными параметрами широкополосности. Это может быть волоконно-оптический кабель OM3, OM4, OM5 или кабель с витыми парами и защитным экраном 6-й, 7-й и 8-й категории с поддержкой 10/40/100/400Gigabit-приложений.

Кабель между HDA и EDA зависит от рабочих приложений и подвержен достаточно частым изменениям. К нему вместе с высокой плотностью предъявляются высокие требования по гибкости и простоте монтажа. Поэтому наиболее оптимальным вариантом будут системы, которые устанавливаются максимально оперативно, без последующего тестирования, как, например, система MPO и витая пара MRJ-2.

Отличия СКС для ЦОД:

В ЦОД используется другая топология сети с новыми иерархическими уровнями, такими, как помещение ввода внешних сервисов и места зонного распределения, которые используются для удобства эксплуатации кабельной системы.

В ЦОД выше минимальные требования к СКС, такие, как использование категории 6 и выше для медной подсистемы и оборудования класса OM3 и выше для оптической подсистемы.

СКС для ЦОД должна быть более отказоустойчивой за счет резервирования кабельных подсистем разного уровня иерархии.

Всё чаще в кабельных системах ЦОД применяется оборудование категории 6A, описанное в новом стандарте на СКС TIA-568C. В этом же американском стандарте прописано тестирование таких кабельных систем.

Стандарты об СКС применительно к ЦОД

В настоящее время действуют 6 основных стандарта в области СКС:

EIA/TIA-568B Commercial Building Telecommunications Wiring Standard (американский стандарт);

ISO/IEC IS 11801 Information Technology. Generic cabling for customer premises (международный стандарт);

CENELEC EN 50173 Information Technology. Generic cabling systems (европейский стандарт).

TIA-942 «Телекоммуникационная инфраструктура Центров Обработки Данных»;

EN 50173-5 «Информационные технологии. Структурированные кабельные системы»;

ISO 24764 «Информационные технологии. Общие кабельные системы для дата-центров» (ожидается принятие).

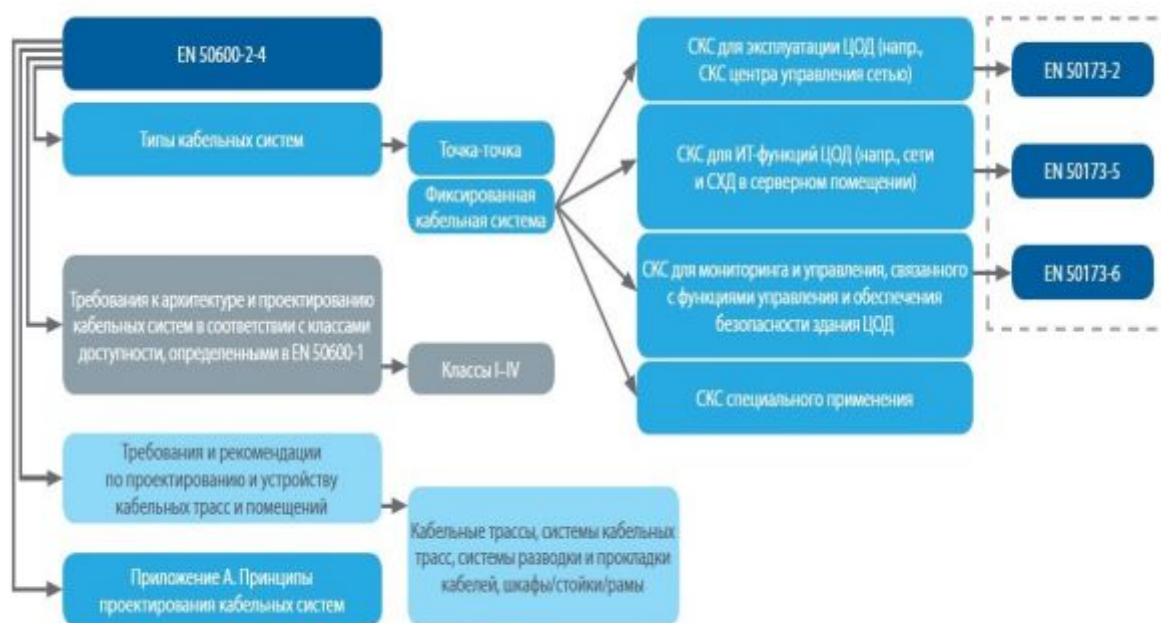


Рис.4.8. Пример структуры СКС стандарта EN 50600-2-4

Стандартизация ЦОД по Tier Standard

Классифицируется на стандарт **Tier Standard: Topology** и стандарт **Tier Standard: Operational Sustainability**, которые подразделяются на 4 уровня. Каждый из уровней включает в себя требования всех предыдущих уровней.

Tier I — базовая инфраструктура без резервирования;

Tier II — инфраструктура с резервными мощностями;

Tier III — инфраструктура, поддерживающая параллельный ремонт;

Tier IV — отказоустойчивая инфраструктура.

Топология — это инфраструктура центра обработки данных. Допускает множество решений, гарантирующих гибкость системы, что позволяет достичь желаемой производительности и соответствовать местным нормам, кодексам и правилам.

Особенности стандарта:

Определяет требования и преимущества классификаций Tier инфраструктуры ЦОД. Каждый уровень (Tier) соотносится с определенной коммерческой функцией и устанавливает соответствующие требования к электропитанию, охлаждению, техническому обслуживанию и безотказности работы.

Стандарты Tier I и Tier II являются тактическими решениями, для которых на первом месте стоит стоимость приобретения и срок вывода продукта на рынок, а не стоимость объекта с учетом срока службы и требования к производительности (безотказности).

Стандарты Tier III и Tier IV предъявляют жесткие требования к гарантии постоянной работоспособности. Решения должны иметь срок службы, превышающий текущие ИТ-потребности, и иметь возможность модернизации.

Операционная устойчивость — это управление центром обработки данных. Объединяет управление объектом и функциональность инфраструктуры объекта, подтвержденной Tier. Эксплуатационная устойчивость определяется как поведение и риски за пределами топологии инженерных систем, которые влияют на достижение целей ЦОДа или решение бизнес-задач в долгосрочной перспективе.

Особенности стандарта:

Опирается на выстраивание процессов работы службы эксплуатации во всех возможных ситуациях и их документирование.

Описывает необходимость проведения обслуживания и регулярного отслеживания состояния инженерных систем согласно рекомендациям производителей.

Описывает необходимость развития и повышения квалификации персонала служб эксплуатации

Учитывает необходимость мониторинга систем и возможности быстрой идентификации оборудования, их инструкций и месторасположения.

Учитывает условия местонахождения ЦОД и особенности его конструкции.

4.8. Оптические кабели ЦОД. Многомодовые OM1-OM5 (MMF)

Многомодовые соединительные кабели с разъёмными концами (патч-корды) описываются по их сердечнику и диаметрам оболочки. Обычно диаметр многомодового патч-корда составляет 50/125 мкм или 62.5/125 мкм.

В настоящее время имеются пять типов многомодовых патч-кордов: OM1, OM2, OM3, OM4 и OM5. Буквы «ОМ» означают оптический многомодовый. Каждый тип патч-кордов имеет свои разные характеристики. Каждые «ОМ» имеют требование на минимальную модовую широкополосность (MBW). OM1, OM2 и OM3 определяются стандартом ISO 11801, который основан на модовой широкополосности многомодового патч-корда. В августе 2009 года, TIA/EIA утвердила и выпустила 492AAAD, который определяет критерий эффективности для OM4. Хотя они разработали оригинальные обозначения «ОМ», IEC выпустил утвержденный эквивалентный стандарт, который в конце концов будет документирован как тип патч-корда A1a. 3 в IEC 60793-2-10.

Ассоциация телекоммуникационной промышленности (TIA) инициировала рабочую группу в октябре 2014 года для разработки руководства по стандарту широкополосного многомодового волокна (WBMMF) 50/125 мкм для поддержки передачи с мультиплексированием с короткой длиной волны (SWDM). Стандарт TIA-492AAAE был опубликован в июне 2016 года. Кабель OM5 предназначен для поддержки как минимум четырех длин волн в диапазоне 850-950 нм, что позволяет оптимально поддерживать короткие волны с мультиплексированием с коротковолновым разделением волн (SWDM), которые уменьшают количество параллельных волокон, по меньшей мере, в четыре раза, чтобы обеспечить постоянное использование всего двух волокон (а не восьми) для передачи 40 Гбит/с и 100 Гбит/с и уменьшение количества волокон для более высоких скоростей (рис.4.9).



Рис.4.9. Достижения для оптических многомодовых волокон ЦОД

Характеристики для кабелей ЦОД приведены ниже.

Кабель OM1 типично имеет оранжевую оболочку и его размер сердечника составляет 62.5 микрон (μm). Он может поддерживать 10 Gigabit Ethernet на расстоянии макс. до 33 метра. Он наиболее широко используется для приложений 100 Mbit Ethernet.

Кабель OM2 также имеет оранжевую оболочку. Его размер сердечника составляет 50 μm , а не 62.5 μm . Он поддерживает 10 Gigabit Ethernet на расстоянии макс. до 82 метра, но наиболее широко используется для приложений 1 Gigabit Ethernet.

Кабель OM3 имеет предлагаемую оболочку зелено-голубого цвета. Как OM2, его размер сердечника составляет 50 μm . OM3 поддерживает 10 Gigabit Ethernet на расстоянии до 300 метров. Кроме этого, OM3 может поддерживать 40 Gigabit и 100 Gigabit Ethernet до 100 метров. Наиболее широко используется для 10 Gigabit Eth.

Кабель OM4 также имеет предлагаемую оболочку зелено-голубого цвета. Он имеет дальнейшее улучшение по сравнению с OM3. Он также использует 50 μm сердечник, но поддерживает 10 Gigabit Ethernet на расстоянии до 550 метров и 100 Gigabit Ethernet на расстоянии до 150 метров.

Полоса пропускания: при 850 нм минимальная модовая широкополосность OM1 составляет 200 МГц*км, OM2 – 500 МГц*км, OM3 – 2000 МГц*км, OM4 – 4700 МГц*км. OM3&OM4 Превосходят OM1&OM2.

Волокна OM5 имеют ограниченную пропускную способность (4700 МГц · км на 850 нм и 2470 МГц · км на 953 нм) и пока неясно сможет ли оно конкурировать с одномодовым волокном. Тем не менее, развитие технологии SWDM продолжается. Разработчики планируют увеличить количество используемых волн до 8, для поддержания скоростей 200 Гбит/с и 400 Гбит/с.

Примеры конструкций соединительного кабеля ЦОД с волокном OM4 и OM5 представлены на рис.4.10, 4.11.



Рис.4.10. Оптический патч-корд LC-LC Cabeus FOP-50-OM4-LC-LC-25m 50/125 (OM4) 25 метров



Рис.4.11. Шнур оптический (патч-корд) duplex SC-SC 50/125 mm OM5 (длина 150 метров)

4.9. Оптические кабели ЦОД. Одномодовые решения SMF

Все стандарты IEEE в Ethernet 100/200 / 400/800G нового поколения будут работать либо с SMF, либо с MMF, но в большинстве ситуаций эти скорости следующего поколения потребуют одномодового волокна, поскольку IEEE всегда стремится разработать будущие стандарты, которые работают с основной установленной базой кабельной инфраструктуры, поэтому клиенты могут легко перейти на новые скорости. Кроме того, ни один из этих действующих действующих стандартов IEEE, ориентированных на скорости следующего поколения, не будет использовать технологию SWDM.

В центре обработки данных (ЦОД) используется 40GBase-SR4, чтобы увеличить плотность портов, вырвав 40G на 10G с помощью модуля прорыва MTP или кабеля пробоя MTP. Это также является преимуществом новых модулей 100GBaes-SR4, которые используют кабели OM4. Однако, если диспетчер центра обработки данных решит использовать 100G SWDM4-модули с кабелями OM5, они не смогут пробиваться в каналы 25 Гбит/с, что станет реальной проблемой по мере того, как экосистема 25 Гбит/с будет полностью развита, и мы начнем видеть больше 25G на сервере.

Хотя цена одномодового волокна (SMF) снижается в последнее время из-за применения новых технологий, стоимость подключаемой оптики по-прежнему ограничивает реализацию SMF в центрах обработки данных. По сравнению с этим OM5 может мультиплексировать четыре длины волн, расположенных в диапазоне от 850 нм до 953 нм, увеличивая емкость данных в четыре раза, а также уменьшая стоимость волокна.

Кроме того, MMF имеет больше преимуществ при установке, устранении неполадок, очистке и общем обслуживании, что делает его лучшим решением при построении центров обработки данных. Однако проблема MMF - это расстояние. Максимальное расстояние будет уменьшаться по мере увеличения скорости передачи данных. Поэтому многомодовое волокно имеет более высокую ценность для владельцев сетей на расстояние до 500 м, а OM5 позволяет переносить до 400 Гбит / с на расстояние до 150 м.

Для расстояний более 500 м следует выбрать одномодовое волокно!

Одномодовое волокно можно разделить на категории OS1 и OS2, которые являются его различными спецификациями. Одномодовое волокно OS1 соответствует стандартам ITU-T G.652A или ITU-T G.652B. Кроме того, волокно с низким водяным пиком, определенное стандартами ITU-T G.652C и G.652D, также относится к категории OS1.

Таким образом, OS1 соответствует спецификациям стандарта ITU-T G.652. Там временем категория одномодового волокна OS2 соответствует только стандартам ITU-T G.652C или ITU-T G.652D, что означает возможность его применения только для производства кабелей с низким водяным пиком. Такое волокно часто используется для приложений CWDM (неплотное спектральное уплотнение каналов).

Кроме стандартов, главным отличием категорий OS1 и OS2 является конструкция самого кабеля. Волокно OS1 используется для производства плотно

упакованного кабеля (tight buffered), который используется внутри зданий (например, кампусов или дата-центров) на максимальной дистанции 10 км.

Волокно OS2 - это кабель со свободной укладкой волокна (loose tube), созданный специально для наружных применений (например, вдоль улиц, под землей или в трубах), где максимальная дистанция достигает 200 км.

Внутренний кабель OS1 характеризуется большими потерями сигнала за километр, чем наружный кабель OS2. Как правило, максимальное значение затухания для волокна OS1 - 1,0 дБ/км, а для волокна OS2 - 0,4 дБ/км.

По кабелям обеих категорий OS1 и OS2 возможна передача гигабитной и 10-гигабитной сети Ethernet. Категория OS2 также поддерживает 40 Гбит и 100 Гбит Ethernet.

OS1 намного дешевле OS2. Ниже следует таблица 1, которая объясняет основные различия между OS1 и OS2.

Таблица 4.1. Классификация одномодовых кабелей

Категория	OS1	OS2
Соответствие стандартам	ITU-T G.652A/B/C/D	ITU-T G.652C/D
Конструкция кабеля	Плотно упакованный	Со свободной укладкой волокна
Применение	Внутреннее	Наружное
Максимальное затухание	1.0дБ/км	0.4дБ/км
Дистанция	10 км	200 км
Цена	Низкая	Высокая

Изучив различия между категориями одномодового волокна OS1 и OS2 применительно к ЦОД, можно приступить к выбору кабеля.

Во-первых, если планируется использовать его внутри здания, наилучшим выбором является OS1. Для наружного применения больше подойдет OS2.

Во-вторых, при дистанции до 2 км не ощутима разница между категориями и преимуществ OS2. Категория OS2 лучше проявляет себя на дистанциях свыше 2 км. К тому же волокно OS1 гораздо дешевле, чем OS2.

Если сэкономить и OS1 достаточно для достижения целей, то нет никакой необходимости выбирать OS2. Компании продают одномодовые кабели обеих категорий OS1 и OS2, а также все типы многомодовых кабелей. Это оптимальный выбор поставщика.

На основе многомодовой оптики успешно развиваются не только локальные сети Ethernet, но и другая неотъемлемая часть сетевых инфраструктур многих ЦОДов — сети хранения данных SAN на базе Fibre Channel. Причем все большее распространение получает технология параллельной передачи трафика по

нескольким волокнам, реализуемая с использованием претерминированных систем, оснащенных *многоволоконными (групповыми) соединителями МРО*.

Так, например, 24-волоконный тракт МРО вполне подойдет для формирования 12 дуплексных линий 10GbE. Затем на его базе (путем простой замены недорогих оконечных компонентов) можно реализовать переход на три линии 40GbE и далее, при необходимости, — на 100-гигабитный канал. Таким образом обеспечивается простая миграция на все более высокоскоростные приложения с максимальным сохранением сделанных инвестиций.

При всех преимуществах многоволоконных систем на базе МРО у них есть один серьезный недостаток — большое число необходимых волокон. В ЦОДах увеличение числа волокон зачастую нежелательно, поскольку это требует дополнительных расходов, в том числе на выделение дорогостоящего пространства под кабельные лотки, организаторы и пр.

Скорость передачи трафика можно повысить и другим способом: путем организации нескольких каналов на основе одного волокна. Это хорошо известная на телекоммуникационном рынке **технология спектрального уплотнения (WDM)**.

Мультиволоконные разъемы МРО высокой плотности для соединений в ЦОД

Использование 24-волоконных магистральных кабелей может поддерживать приложения 10G, 40G и 100G (рис.4.12). Для приложений 10G каждое из 24 волокон может использоваться для передачи 10G, всего 12 каналов. Для приложений 40G, для которых требуется 8 волокон (4 передающих и 4 принимающих), 24-волоконный магистральный кабель обеспечивает в общей сложности три канала 40G. Для 100G, для которого требуется 20 волокон (10 для передачи и 10 для приема), 24-волоконный магистральный кабель обеспечивает одну линию 100G.

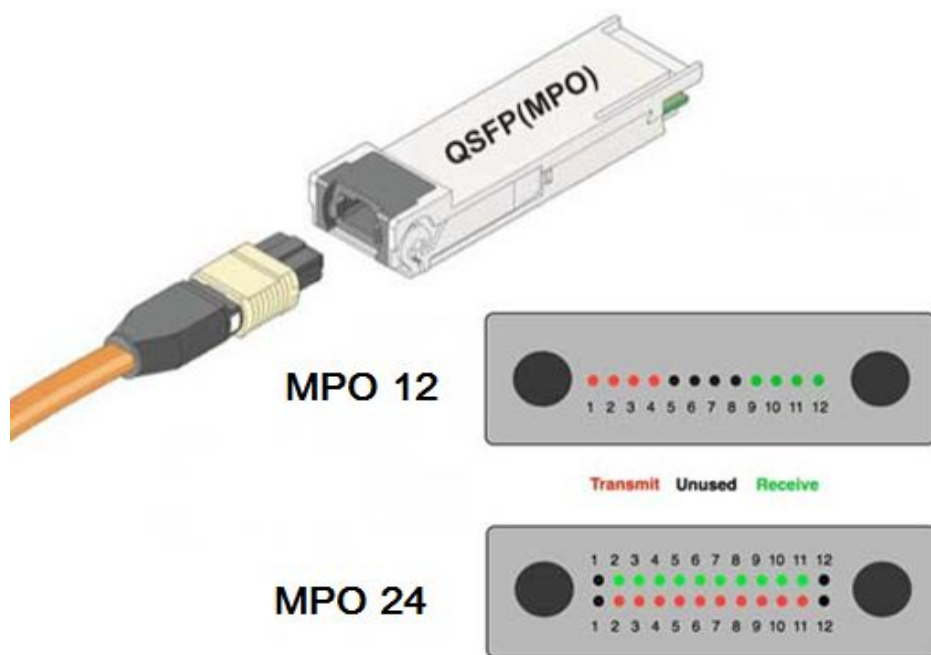


Рис.4.12.Мультиволоконные разъёмы

Конверсионный кабель 1 x MPO-32, 32 волокон разъем MPO на 2 x MPO-16, 16 волокон разъем MPO кабель ответвления 1 x MPO-32, 32 волокон разъем MPO на 2 x MPO-16, 16 волокон разъем MPO кабель ответвления.

Tarluz предлагает 16 волокон оптоволоконные сборки MTP/MPO 400G MPO/MTP для удовлетворения будущих требований к пропускной способности сети. Сборки предлагаются в однорядных конфигурациях с 16 волокнами и 32 волокнами (2 линии x 16 волокон) для достижения наибольшей плотности физического контакта для многоволоконных соединителей на рынке.

Этот магистральный кабель высокой плотности может напрямую подключаться к активным устройствам 16x25G, которые соответствуют стандартам Telcordia GR-326 Core, TIA 604-18 (FOCIS 18) и IEC (61754-7-3).

<http://www.tarluz.com/ru/product-details/конверсионный-кабель-мпо-32-на-2-х-мпо-16/>

Сверхвысокая по современным меркам производительность оптического канала связи не позволяет передавать информационный поток в одном волновом канале (в одном волокне) простой технологией. Иначе говоря, разработчики вынуждены прибегнуть к параллельной передаче линейного сигнала со скоростью не менее 25 Гбит/с в одном субканале, на одной оптической поднесущей частоте, причем для формирования отдельно взятого субканала могут быть использованы разнообразные технические средства (табл.). В рамках реализации подобной стратегии применяются как традиционные, так и новые решения (рис.4.13, 4.14).

500 м	2 км	10 км
4 волокна x 2 λ x 50G NRZ	1 волокно x 8 λ x 50G NRZ	1 волокно x 8 λ x 50G NRZ
4 волокна x 2 λ x 50G PAM4	1 волокно x 8 λ x 50G PAM4	1 волокно x 8 λ x 50G PAM4
4 волокна x 1 λ x 100G NRZ	1 волокно x 4 λ x 100G PAM4	1 волокно x 4 λ x 100G DMT
4 волокна x 1 λ x 100G DMT	1 волокно x 4 λ x 100G DMT	

Рис.4.13. Варианты повышения пропускной способности волокон с применением спектрального мультиплексирования для различных дистанций

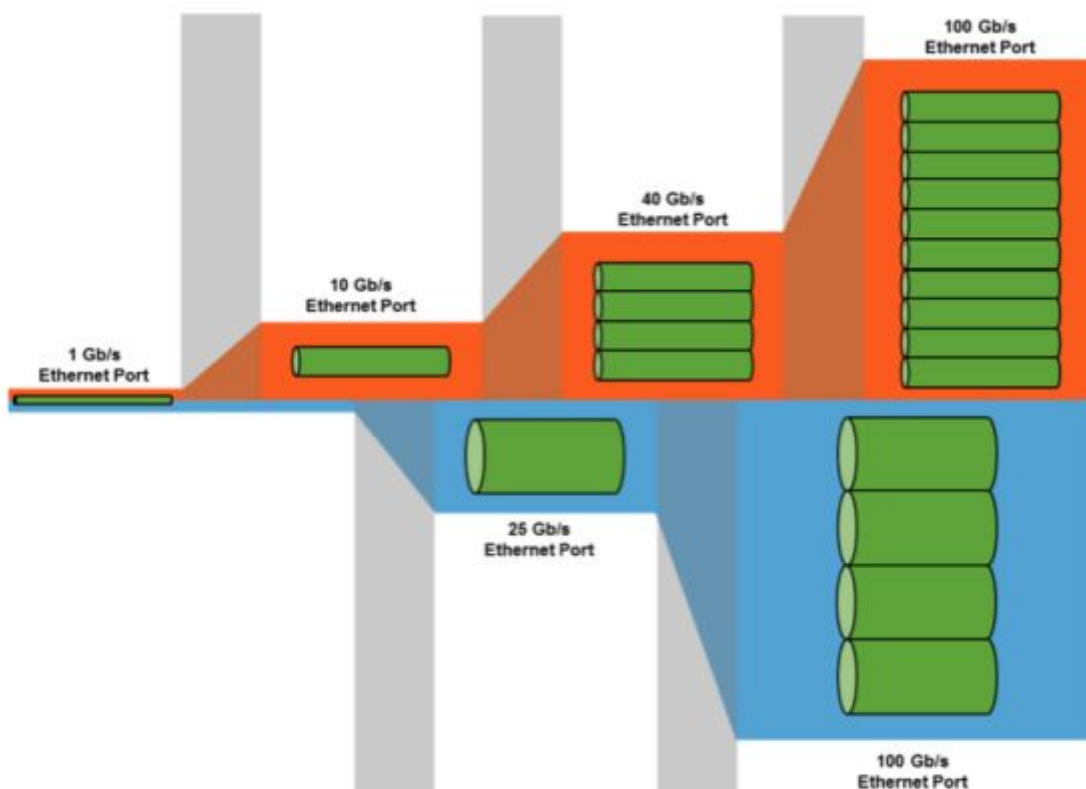


Рис.4.14 Варианты наращивания скорости передачи Ethernet в ЦОД

Развитие стандартизации Ethernet представлено рис.4.15.

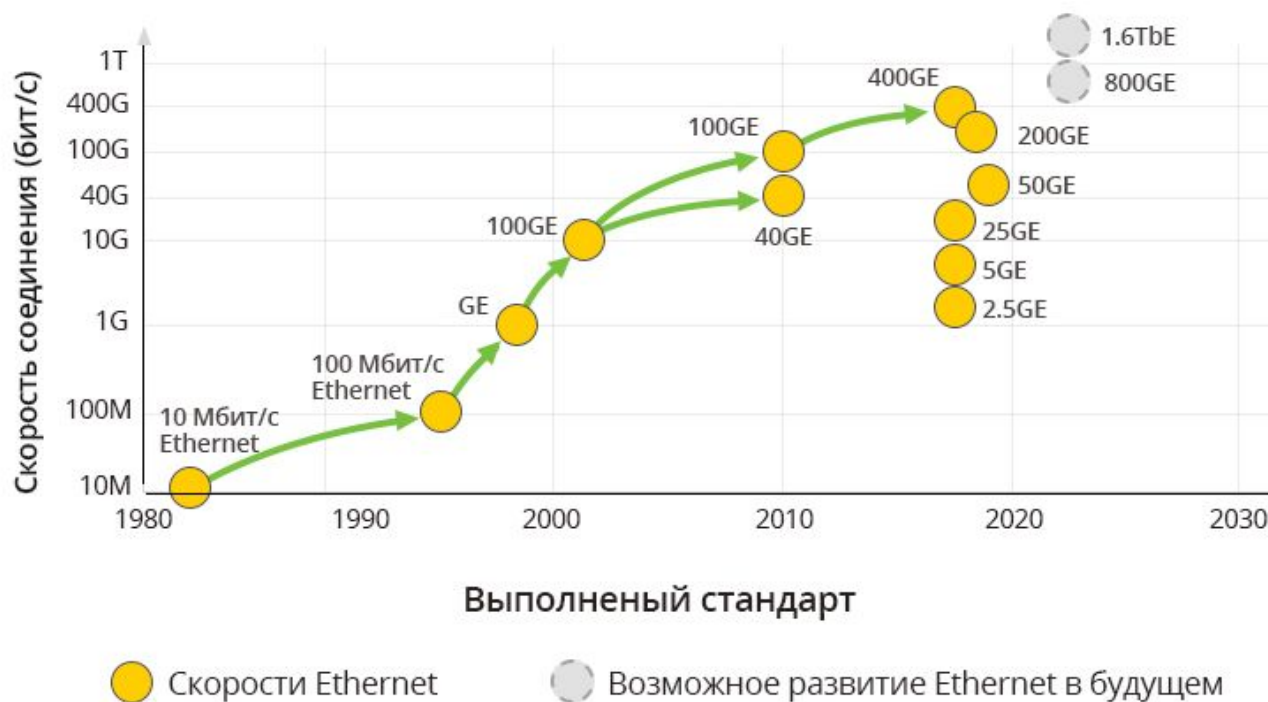


Рис.4.15 Развитие стандартизации Ethernet

Спецификация интерфейсов Ethernet

Спецификация	Расстояние, м	Тип волокна*	Примечание
400GBASE-SR16	100	MM	По 16 волокон на прием и передачу
400GBASE-DR4	500	SM	Четыре параллельных волокна в обоих направлениях, 100 Gb на одно волокно
400GBASE-FR8	2000	SM	WDM (два волокна, одно на прием, другое на передачу)
400GBASE-LR8	10000	SM	То же
200GBASE-DR4	500	SM	Четыре параллельных волокна в обоих направлениях
200GBASE-FR4	2000	SM	WDM (два волокна, одно на прием, другое на передачу)
200GBASE-LR4	10000	SM	То же

4.10. Электрические кабели ЦОД. Международный стандарт ISO / IEC 11801 "Информационные технологии — универсальные кабели для помещений заказчика"

Класс D: соединение / канал до 100 МГц с использованием кабеля / разъемов [категории 5e](#).

Класс E: соединение / канал до 250 МГц с использованием кабеля / разъемов [категории 6](#)

Класс E_A: соединение / канал до 500 МГц с использованием кабеля / разъемов [категории 6_A](#) (Поправки 1 и 2 к ISO / IEC 11801, 2-е изд.)

Класс F: соединение / канал до 600 МГц с использованием кабеля / разъемов [категории 7](#).

Класс F_A: соединение / канал до 1000 МГц с использованием кабеля / разъемов [категории 7_A](#) (Поправки 1 и 2 к ISO / IEC 11801, 2-е изд.)

Класс ВСТ-В: соединение / канал до 1000 МГц с использованием коаксиальных кабелей для приложений ВСТ. (ISO/IEC 11801-1, редакция 1.0 2017-11)

Класс I: соединение / канал до 2000 МГц с использованием кабеля / разъемов [категории 8.1](#) (ISO / IEC 11801-1, редакция 1.0 2017-11)

Класс II: соединение / канал до 2000 МГц с использованием кабелей / разъемов категории 8.2 (ISO / IEC 11801-1, редакция 1.0 2017-11)

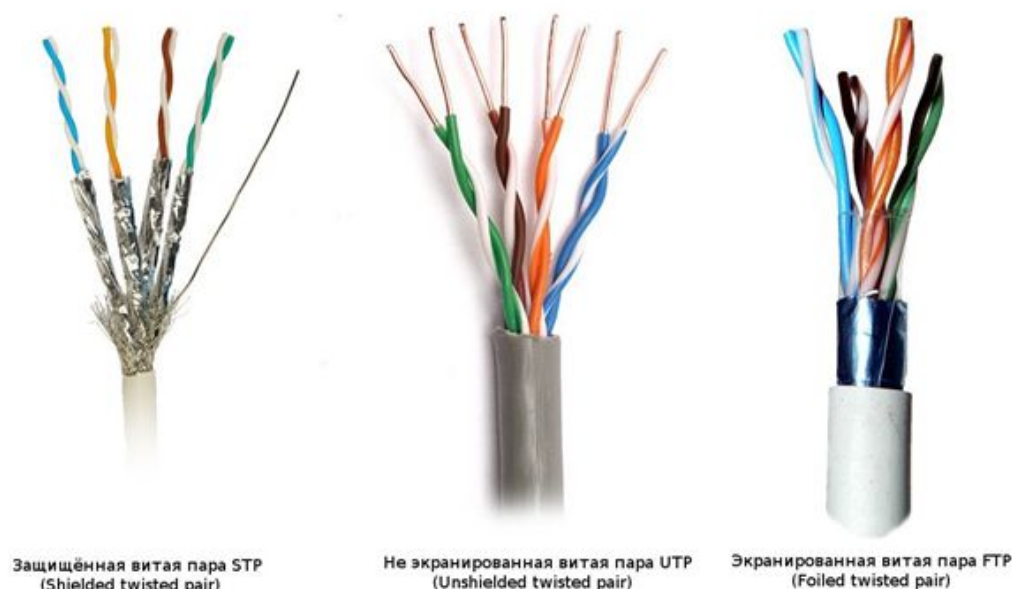


Рис.4.16. Примеры конструкций электрических кабелей ЦОД

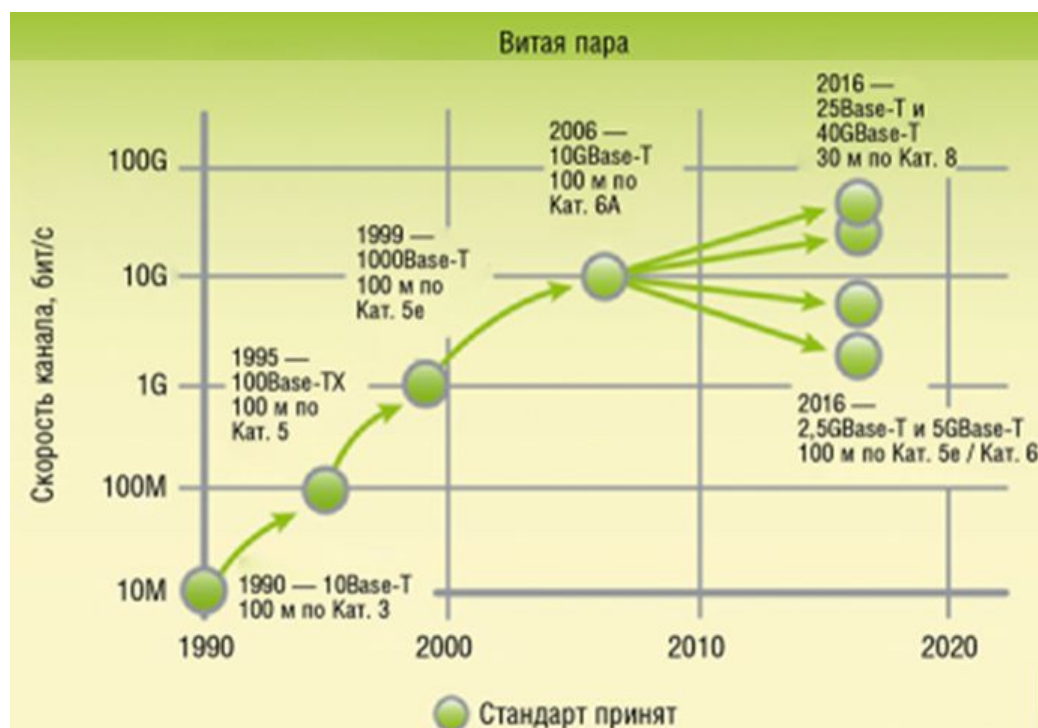


Рис.4.17. Электрические кабели ЦОД. Витая пара и скоростные режимы

Основные электрические кабели ЦОД.

Cat7 кабели иначе называют кабелем Ethernet категории 7. Он поддерживает высокоскоростную связь Ethernet до 10 Гбит / с. Кабель Cat7 обратно совместим с категориями кабелей Cat6, Cat5 и Cat5e. Он предлагает 100-метровый 4-контактный канал с использованием экранированных кабелей и предназначен для передачи сигналов с частотой 600 МГц.

Кабели категории 7 требуют, чтобы витые провода были полностью экранированными, известными как экранированная витая пара (SSTP) или экранированная витая пара из фольгированной витой пары (SFTP), что полностью устраняет перекрестные помехи, при этом значительно улучшая помехоустойчивость. Таким образом, он позволяет пользователю получать более высокие скорости даже при использовании более длинных кабелей.

Cat 8 кабель, или кабель категории 8, представляет собой Ethernet кабель, который сильно отличается от предыдущих кабелей тем, что он поддерживает частоту до 2GHz(2000MHz), и ограничен 30-метровым каналом 2-разъёма. Cat8 кабель также требует экранированного кабеля. Ethernet кабели Cat8 могут поддерживать скорость 25Gbps или даже 40Gbps. Внешний вид кабеля Cat8 аналогичен с кабелем нижней категории и он терминирован разъёмом RJ45 или другим разъёмом. Cat8 кабель также обратно совместим со своими предыдущими версиями. Так что можно использовать его со стандартным разъемом Cat7.

При сравнении Cat7 и Cat8, частота передачи и длина кабеля также имеют важное значение. Cat7 кабель обеспечивает производительность до 600MHz, а Cat8 кабель до 2000MHz. Максимальная длина кабеля Cat7 составляет 100m с 10Gbps, а Cat8 - 30m с 25Gbps или 40 Gbps.

Кабели категории 8 дешевле, чем оптические, обеспечивают обратную совместимость с кабелями категории 6 (разные порты одного коммутатора могут поддерживать разные скорости), так что при их использовании заказчик получает универсальную инфраструктуру, способную работать на скоростях от 1 до 40 Гбит/с.

Cat8 – идеальный вариант для малых и средних ЦОДов, в машинных залах которых в одном ряду размещается не более 30 стоек. В крупных ЦОДах, где стоек в рядах более 30 и требуются скорости выше 40 Гбит/с, следует применять оптоволокно.

Принятый официально 14 июля 2016 г. кабельный стандарт ANSI/TIA-568-C.2-1 на категорию 8 (Cat8) содержит требования к каналу на основе витой пары длиной до 30 м – традиционный 4-парный кабель оконцован 8-позиционными модульными гнездами RJ-45. Конфигурация отличается от общепринятого 100-метрового канала, описанного стандартом TIA 568-C.2, уменьшенной длиной и меньшим количеством точек соединения – их максимум две, а не четыре. В таких каналах для подключения активного оборудования могут использоваться только межсоединения, на концах задействовано только по одной единице коммутационного оборудования: порт патч-панели или розетки на одном конце и порт патч-панели или розетки на другом. ***Эта конфигурация отлично подходит для центров обработки данных***, как с топологией «*top of rack*» (в каждом шкафу устанавливается сетевой коммутатор), так и с топологией

«end of row» (крайний шкаф в каждом ряду играет роль распределителя и содержит патч-панели, горизонтальные кабели от которых ведут к панелям, установленным во всех остальных шкафах ряда). Ограничение по количеству точек соединения не имеет для ЦОД практического значения, поскольку в них нет нужды ни в кросс-соединениях (для чего потребовалась бы вторая патч-панель на конце), ни в использовании консолидационной точки (что повлекло бы за собой установку еще одной патч-панели в середине сегмента). На самом деле, для всех конфигураций с тремя или четырьмя коннекторами в канале характерна одна и та же монтажная проблема: участки горизонтальных кабелей с полнотелыми жилами (solid) приходится оконцовывать модульными вилками, что всегда нежелательно.



Пример конфигурации канала категории 8



Кабели и шнуры

Аппаратные шнуры A, C

Горизонтальный кабель B

Коммутационное оборудование

Модульные гнезда C1, C2

Максимальная длина

A + C см. таблицу

B 24 м

Калибр проводников в шнурах, AWG	Максимальная длина A + C, м
22-23	8
24	6
26	4

Рис.4.18. Конструкция кабеля категории 8 и пример его использования

Изменение требований к конфигурации канала в категории 8 в сравнении с предшествующими категориями вызвано тем, что частотный диапазон расширился вчетверо относительно категории 6A – потолок частот составляет не 500 МГц, а 2000 МГц.

Чтобы оборудование могло воспользоваться таким широким диапазоном, к каналу передачи предъявляются гораздо более строгие требования по вносимым потерям, перекрестным наводкам и возвратным потерям. Максимальная толщина проводников для систем на основе витой пары, допускаемая стандартом, соответствует калибру 22 AWG, и это ограничивает возможности улучшить значение вносимых потерь в горизонтальном сегменте. На самом деле, даже калибр 22 AWG создает определенные сложности, поскольку кабель получается довольно жесткий, а его внешний диаметр достигает 9 мм. В таких условиях единственный реальный способ обеспечить хорошие характеристики передачи в канале – уменьшить его длину.

Кроме вносимых потерь необходимо учитывать и наводки (помехи) между парами кабеля и между кабелями – это тоже значимый фактор, особенно для высоких частот (рис.4.19.). Исследования показали, что (межкабельные) наводки в неэкранированной витой паре UTP слишком высоки, чтобы можно было реализовать передачу данных по протоколу 40GBase-T. Чтобы добиться приемлемых значений межпарных наводок, необходимо прибегать к экранированию. Это может быть как общий экран, охватывающий 4 пары (кабель F/UTP), так и индивидуальное экранирование каждой пары плюс общий экран в виде фольги или оплетки (кабели F/FTP и S/FTP соответственно).

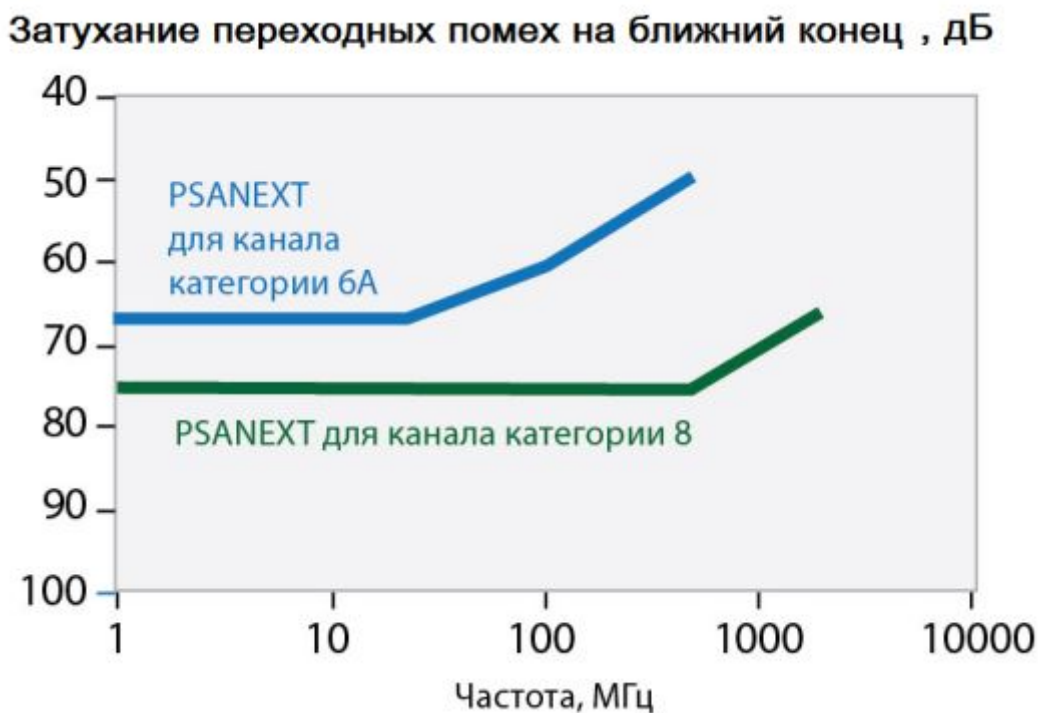


Рис.4.19. Межпарные наведённые помехи для категорий 6 и 8

Для ЦОД существуют рекомендации по использованию различных типов кабельной структуры. Ниже приведены примерные предпочтения использования металлического и оптического кабелей.

Малые корпоративные ЦОДы (площадь ИТ-зон менее 100 м²)

- Преимущественное использование витопарных кабелей.
- Одномодовые линии применяются для связи с городским вводом операторов связи.

Средние корпоративные ЦОДы (площадь ИТ-зон 100–300 м²)

- Ограниченное использование оптических кабелей, но большой потенциал для роста. Популярна архитектура Top of Rack (ToR).

Большие корпоративные ЦОДы (300–1000 м²), а также типичные коммерческие ЦОДы (500–5000 м²)

- 60–90% линий — многомодовая оптика, все чаще используются претерминированные МРО-кабели.
- Разнообразие архитектур (ToR, EoR/ MoR, Centralized Switching), но чаще предпочтение отдается ToR.
- «Медь» Категории 8 рассматривается как альтернатива межаппаратным кабелям.

Коммерческие мегаЦОДы, облачные и гипермасштабируемые (Hyperscale) комплексы (3000–50000 м² и более)

- Доминируют одномодовые линии (их доля может достигать 100%).
- Скорости 40G и 100G, перспективы внедрения технологии 400G на одномодовых линиях.
- Претерминированные МРО-кабели для высокоскоростных приложений.
- Соотношение долей медножильных и оптических линий в кабельной инфраструктуре ЦОДа во многом определяется его площадью. Так, в малых корпоративных ЦОДах, где площадь ИТ-зон не превышает 100 м², доминируют витопарные кабели — для небольших расстояний вполне хватает «дальнобойности» медножильной проводки. В крупных же корпоративных центрах обработки данных (более 300 м²), а также в коммерческих ЦОДах на многомодовую оптику приходится уже 60–90% всех линий, при этом постоянно увеличивается доля линий с волокном OM4. Кроме того, на таких объектах все чаще используются кабели с претерминированными многоволоконными МРО-соединителями; эти технические решения позволяют оперативно и с минимальными затратами по мере необходимости перейти на более высокие скорости: например, с 10GbE на 40GbE и далее на 100GbE.
- Отдельно следует упомянуть так называемые мегаЦОДы — в частности, огромные гипермасштабируемые (Hyperscale) комплексы, на базе которых многие интернет-гиганты предоставляют облачные сервисы. На таких объектах доминируют одномодовые линии, причем их доля может достигать 100%. Преимущественное использование одномодовой техники обусловлено рядом причин, в том числе большими расстояниями между ИТ-модулями и залами, а также высокими требованиями к пропускной способности сетей — владельцы мегаЦОДов одними из первых начали применять технологии 40GbE и

100GbE. Нельзя не упомянуть и о том, что некоторые из них разрабатывают собственные принципы организации СКС, которые получили дальнейшее развитие в рамках инициированного Facebook проекта Open Compute Project (OCP).

Ещё раз повторим, что СКС ЦОД состоит из следующих подсистем:

Главный распределительный пункт (MDA / Main Distribution Area).

Данная система обеспечивает интерфейс доступа в центр, а также осуществляет деление трафика, который поступает по главной магистрали, между внутренними магистралями. Включает в себя маршрутизаторы, магистральные коммутаторы, оборудование операторов связи.

Горизонтальная распределительная система (HDA /Horizontal Distribution Area), которая осуществляет распределение трафика от внутренней магистрали по локальным линиям, которые подходят к аппаратным зонам. Длина локальных линий не должна превышать 100 метров.

Аппаратная зона, где размещаются сервера, коммутаторы, коммутационные панели.

Система распределения трафика по оборудованию (EDA /Equipment Distribution Area). Данная система осуществляет распределение трафика между серверами и другим оборудованием.

4.11. Основные варианты кабельной инфраструктуры СКС и размещения коммутаторов в ЦОД

Варианты **Middle of row (MoR)**, **End of row (EoR)**, **Top of rack (ToR)** представлены рис.4.20.

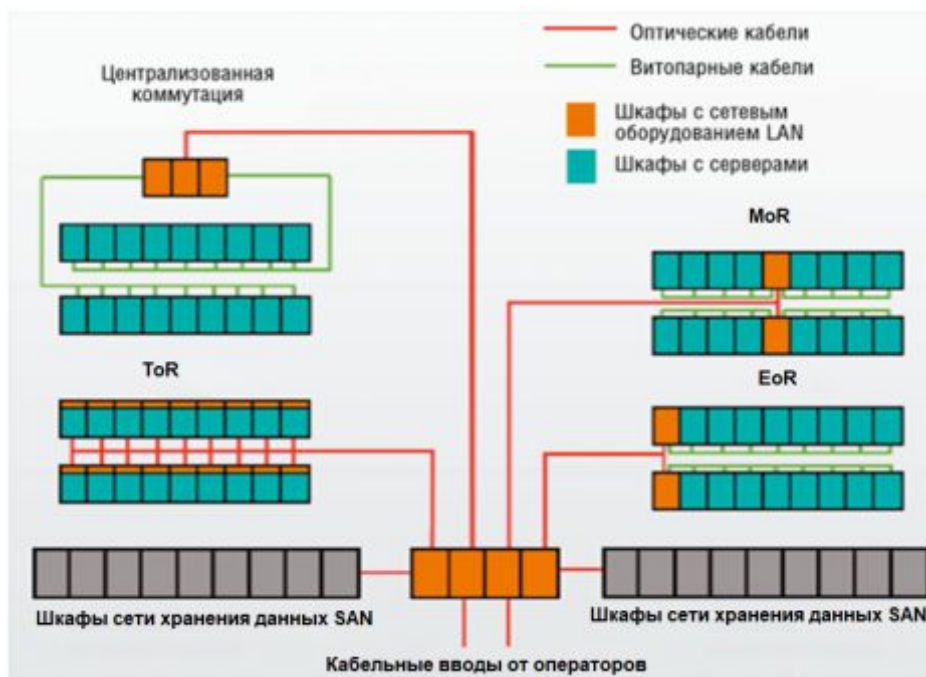


Рис.4.20. Варианты кабельной инфраструктуры СКС ЦОД

Архитектурные решения СКС в ЦОД в зонах подключения конечных устройств ЦОДа определяется расположением активного оборудования (коммутаторов). На практике получили распространение три основных варианта такого расположения. Первый, и наиболее популярный, — установка коммутатора в каждой стойке с ИТ-оборудованием (ToR). Второй — концентрация коммутаторов, обслуживающих оборудование данного ряда, в одной стойке. Стойка с коммутаторами может находиться в конце ряда (EoR) или в его середине (MoR). Наконец, третий вариант — централизованное размещение активного оборудования, обслуживающего серверный зал (Centralized Switching) (рис.4.21). В этом случае коммутаторы устанавливаются в главном кроссе, а в стойках находится только пассивное оборудование СКС.

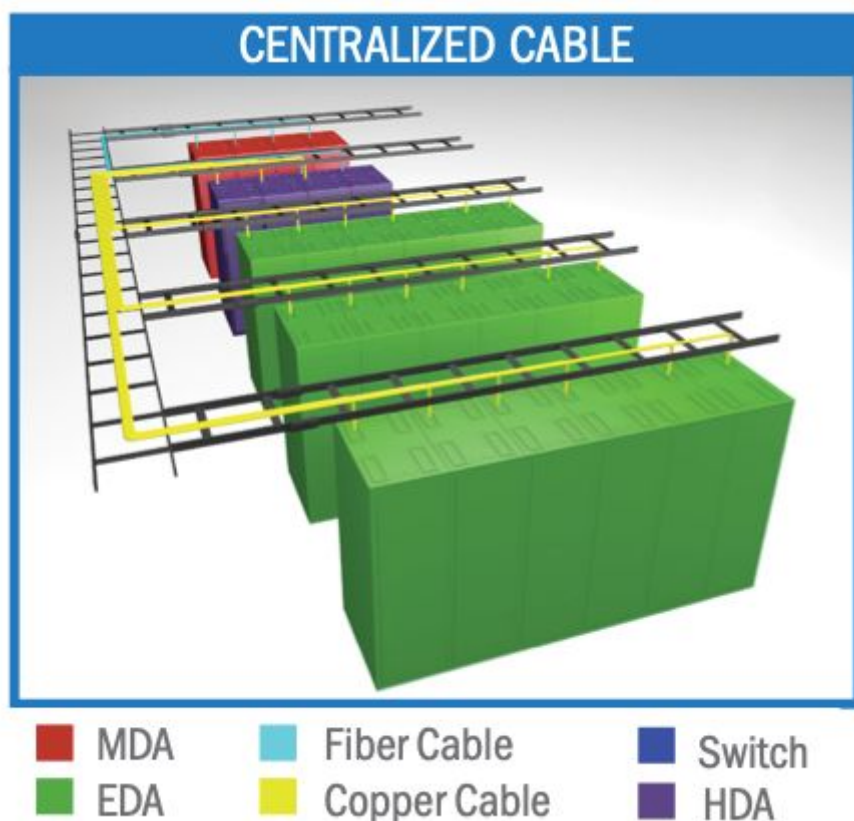


Рис.4.21. Архитектурное решение в ЦОД с централизованной коммутацией и построением кабельной инфраструктуры

Сокращения на рис.4.21: **MDA (Main Distribution Area)** – Space where core layer equipment such as routers, LAN/SAN switches, PBXs, and Muxes are located.

HAD (Horizontal Distribution Area) – Space where aggregation layer equipment such as LAN/SAN/KVM switches are located.

EDA (Equipment Distribution Area) – Space where access layer equipment such as LAN/SAN/KVM switches and servers are located.

ZDA (Zone Distribution Area) – Space where a consolidation point or other intermediate connection point is located.

Архитектурное решение ToR для ЦОД.

Top of rack (ToR) — это модель коммутации, когда в каждой стойке стоит коммутатор, который обрабатывает трафик с серверов в этой стойке, и соединен с коммутатором ядра или с агрегирующим слоем (в зависимости от количества уровней) (рис.4.22). Согласно результатам опроса, проведенного в 2015 году, ToR была наиболее популярной системой, как в центрах обработки данных, так и в корпоративных центрах обработки данных. Исходя из нынешней тенденции, он будет широко распространен как в настоящем, так и в будущем.

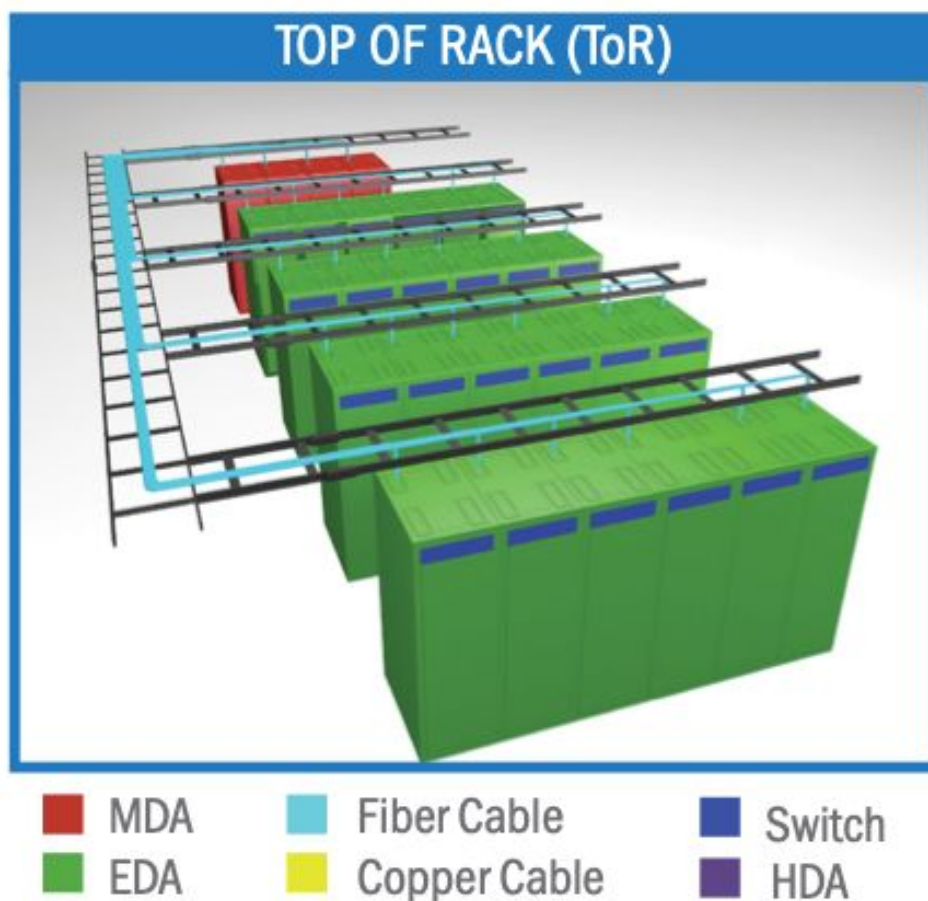


Рис.4.22. Архитектурное решение ToR для ЦОД

Сокращения на рис.4.22: **MDA (Main Distribution Area)** – Space where core layer equipment such as routers, LAN/SAN switches, PBXs, and Muxes are located. **HAD (Horizontal Distribution Area)** – Space where aggregation layer equipment such as LAN/SAN/KVM switches are located. **EDA (Equipment Distribution Area)** – Space where access layer equipment such as LAN/SAN/KVM switches and servers are located. **ZDA (Zone Distribution Area)** – Space where a consolidation point or other intermediate connection point is located.

Архитектура Top of Rack (в некоторых англоязычных публикациях используется ее сокращенное наименование в виде ToR) основана на установке в верхней части каждого серверного шкафа одного или нескольких пограничных коммутаторов. Верхняя установка этих устройств не является обязательной и

практикуется исключительно из соображений простоты работы с ними в тех немногочисленных случаях, когда требуется выполнение ручной коммутации.

Обращение к архитектуре рассматриваемой разновидности влечет за собой существенное упрощение горизонтальной подсистемы СКС из-за того, что сервер непосредственно подключается к портам коммутатора обычными коммутационными шнурами. В результате из ряда серверных шкафов выходят исключительно соединительные линии от up-link-портов пограничных коммутаторов. Кроме того, подключение новых серверов в структуру ограничивается фактически только наличием свободных портов у шкафного коммутатора.

Поскольку ToR является наиболее популярным проектом системы центра обработки данных, коммутаторы ToR становятся популярными. Вот некоторые производственные ToR switch с различной скоростью передачи данных от сервера к серверу, в диапазоне от 1G до 100G. Все коммутаторы ToR поддерживают функции L2/L3, IPv4/IPv6, мосты центров обработки данных (рис.4.23) . Коммутаторы ToR должны быть многопортовыми и с малой задержкой сигнала, поскольку им приходится иметь дело с трафиками разных уровней.

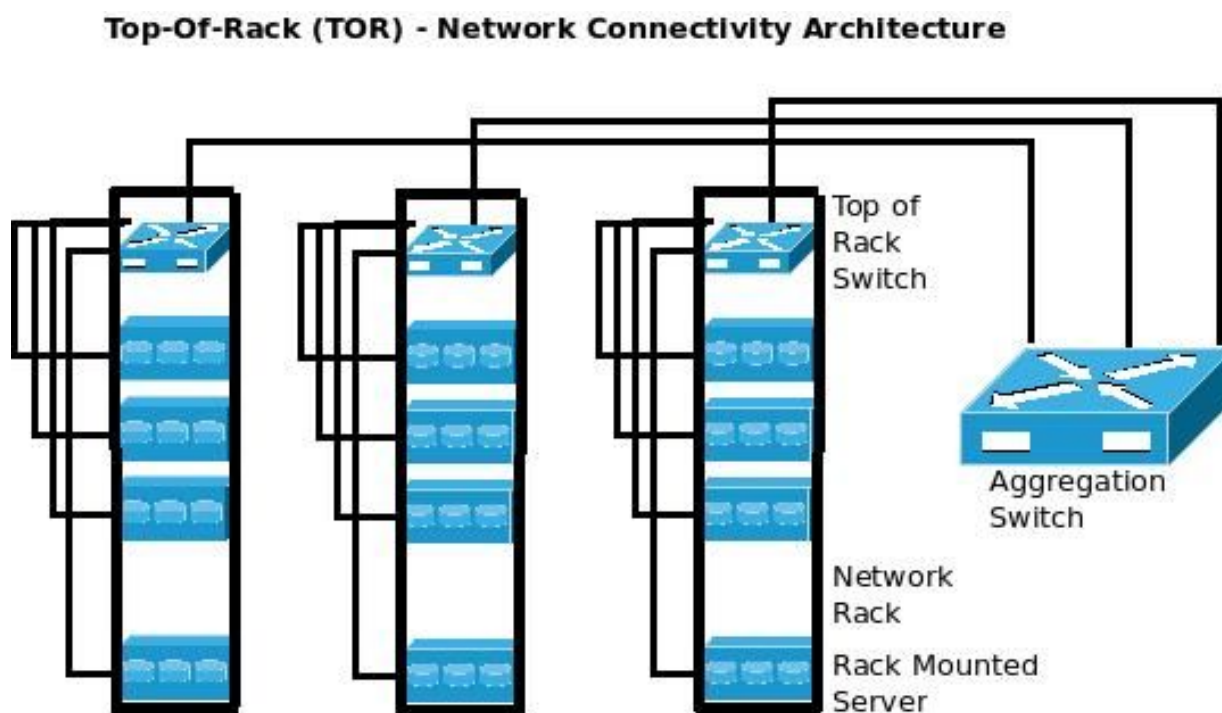


Рис.4.23. Вариант включения коммутаторов ToR

В конструкции ToR, по крайней мере, один [сетевой коммутатор](#) размещен в каждой стойке, а серверы в стойке подключены к коммутатору, обычно, с помощью медного кабеля. После этого, коммутаторы в каждой стойке подключаются к ToR switch.

Преимущества ToR: медные кабели остаются “в стойке”; снижены затраты на прокладку кабелей; поддерживается модульная и гибкая “в стойке” архитектура; перспектива на более высокие скорости. При реализации

архитектуры Top of Rack задача резервирования связей отдельных серверов с сетью может решаться двумя различными способами. Согласно первому из них, основной и резервный порты сетевых интерфейсов сервера подключаются к различным коммутаторам, которые находятся в одном шкафу. Во втором случае коммутаторы для поддержки основной и резервной связей размещаются обязательно в разные конструктивы (рис.4.24).

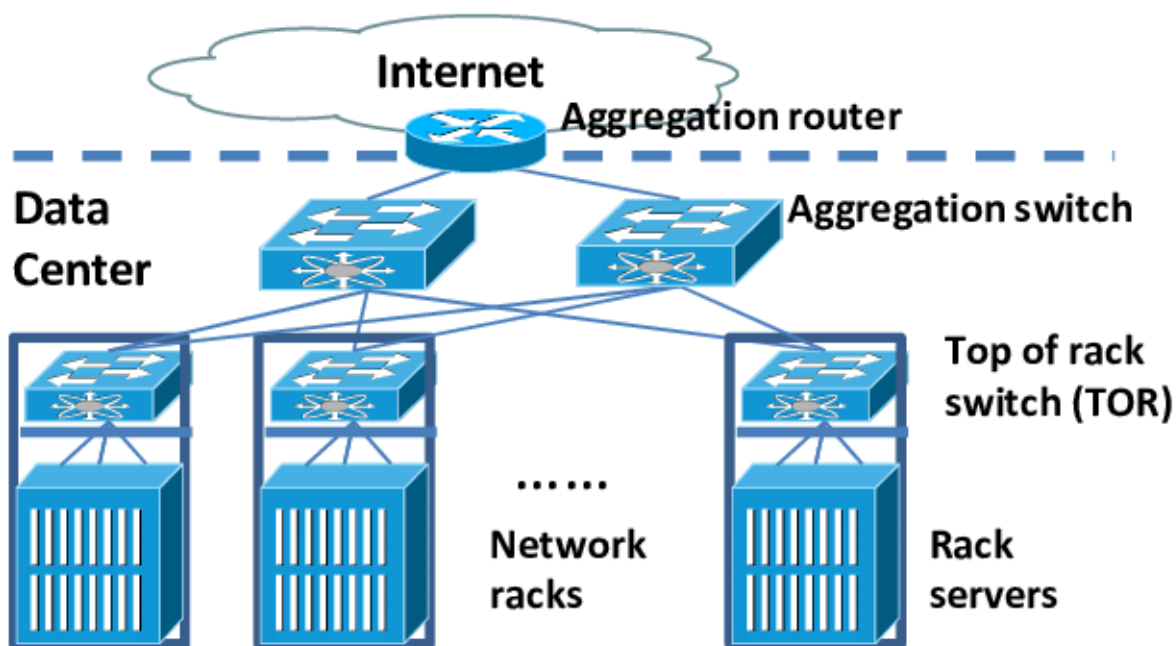


Рис.4.24. Архитектурное решение ToR для ЦОД с резервированием и выходом на интернет

Архитектурные решения EoR, MoR и кабельная инфраструктура

Если говорить о перспективах использования высокоскоростных (25 и 40 Гбит/с) технологий на базе витопарной проводки Категории 8, то они предназначены в первую очередь для аппаратных областей сетей, построенных по архитектурам ToR, EoR и MoR. В случае EoR (рис.4.25) расстояние от серверов до коммутаторов не превышает длины ряда стоек, а в варианте MoR (рис.4.26) — половины длины ряда, что укладывается в уже упомянутые ограничения 30 м. Универсальные кабельные системы Категории 8 могут стать эффективной заменой кабелей прямого подключения (Direct-Attach Cable, DAC), которые, помимо своей нестандартности (они привязаны к конкретному оборудованию), весьма дорого стоят. Однако однозначно ответить на вопрос, сможет ли Категория 8 стать хорошей заменой многомодовой оптике на небольших расстояниях, пока невозможно.

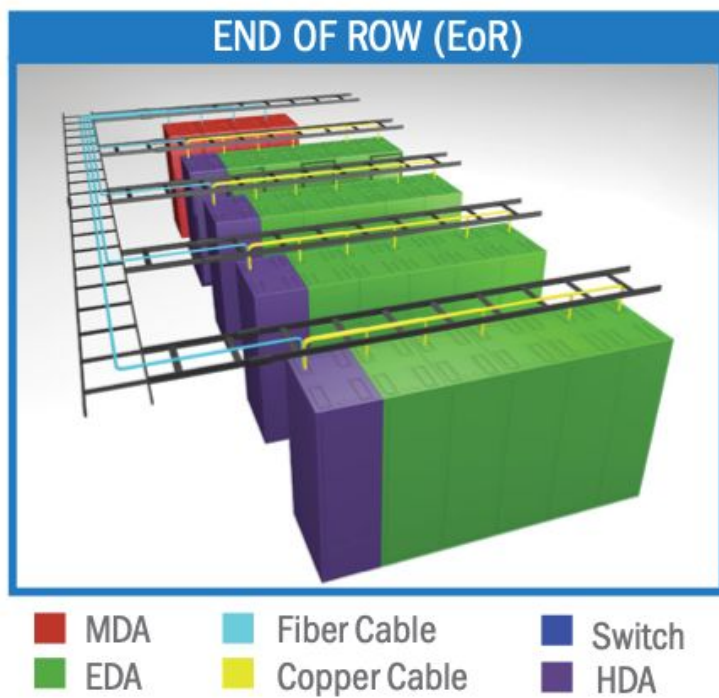


Рис.4.25. Архитектурное решение EoR для ЦОД

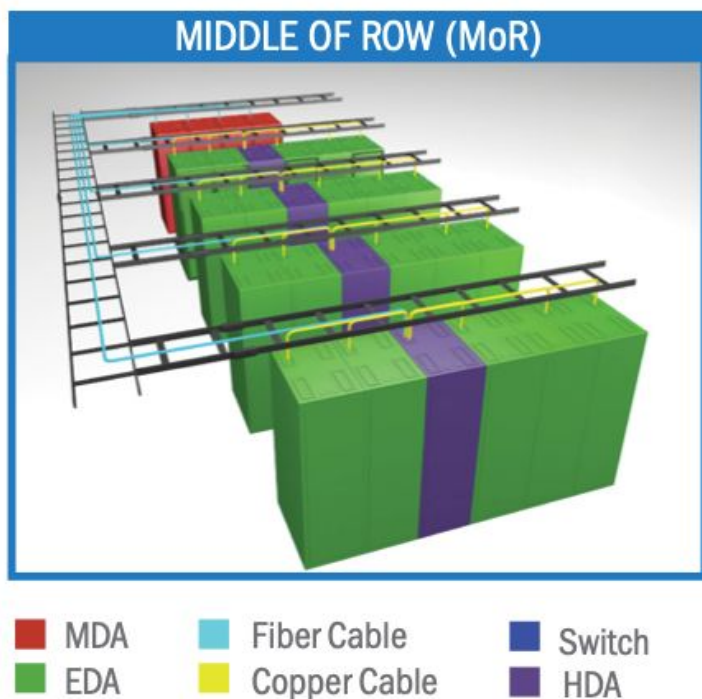


Рис.4.26. Архитектурное решение MoR для ЦОД

Сокращения на рис.4.25, 4.26.

MDA (Main Distribution Area) – Space where core layer equipment such as routers, LAN/SAN switches, PBXs, and Muxes are located. **HAD (Horizontal Distribution Area)** – Space where aggregation layer equipment such as LAN/SAN/KVM switches are located. **EDA (Equipment Distribution Area)** – Space where access layer equipment such as LAN/SAN/KVM switches and servers are

located. **ZDA (Zone Distribution Area)** – Space where a consolidation point or other intermediate connection point is located.

На рис. 4.27 и 4.28 представлены оценочные значения по выбору инфраструктуры коммутации и физической среды соединений в ЦОД.

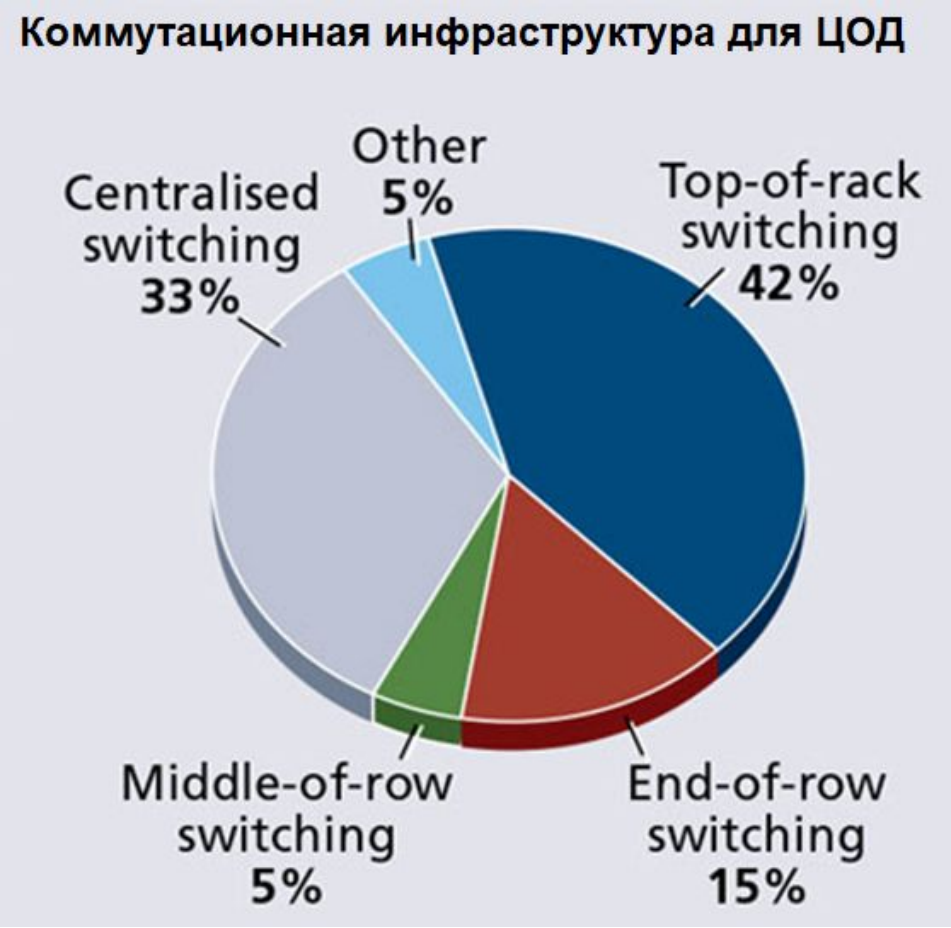


Рис.4.27. Предпочтения в выборе коммутационной инфраструктуры ЦОД



Рис.4.28. Рекомендация по применению физической среды соединений в ЦОД

4.12. Претерминированные соединения в ЦОД

Претерминированные кабельные решения для волоконно-оптической подсистемы СКС реализуется преимущественно в виде модульно-кассетных решений (рис.4.29). Стимулом к их внедрению стало использование оборудования 10GbE и заложенные в такие решения возможности перехода на более высокоскоростные технологии. Претерминированные решения для ЦОД рассчитаны на быстрый и качественный монтаж. Такие системы тестируются в заводских условиях. Они могут включать в себя коммутационные панели, претерминированные кассеты и модули, специальные крепления и кронштейны для организации точек коммутации в пространстве под фальшполом, над монтажными шкафами, объединять различные среды передачи при эффективном использовании полезного пространства в ЦОД.

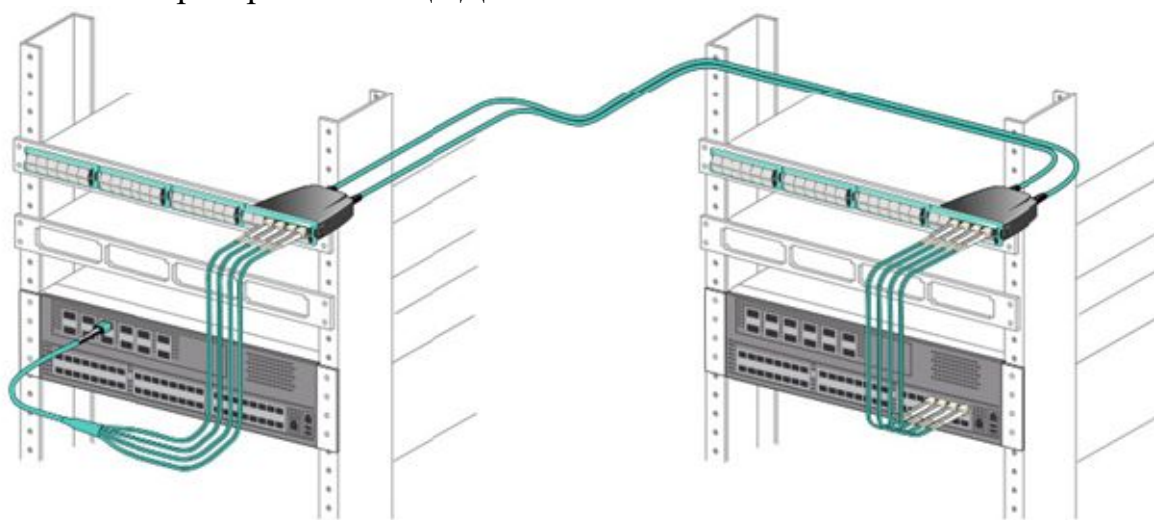


Рис.4.29. Пример использования претерминированного оптического кабеля OM5 для соединений в ЦОД с модулем SWDM



Рис.4.30. Претерминированные компоненты для ЦОД

Новинки претерминирования (рис.4.31) предназначены для создания двенадцати волоконных трактов со скоростью передачи до 400Гбит/с, а в их основе лежат

коннекторы MTP PRO классов: Standard и Elite. Первые подходят для одномодовых волокон, вторые – для OM3 и OM4. Это обеспечивает минимальные потери по линиям прямой и обратной передачи, что удовлетворяет протокол 100GBASE, где бюджет потерь на одно соединение на должен превышать 0,35дБ. Примеры использования претерминированных решений представлены рис.4.32, 4.33, 4.34., 4.35.



Рис.4.31. Претерминирование 12-волоконных трактов

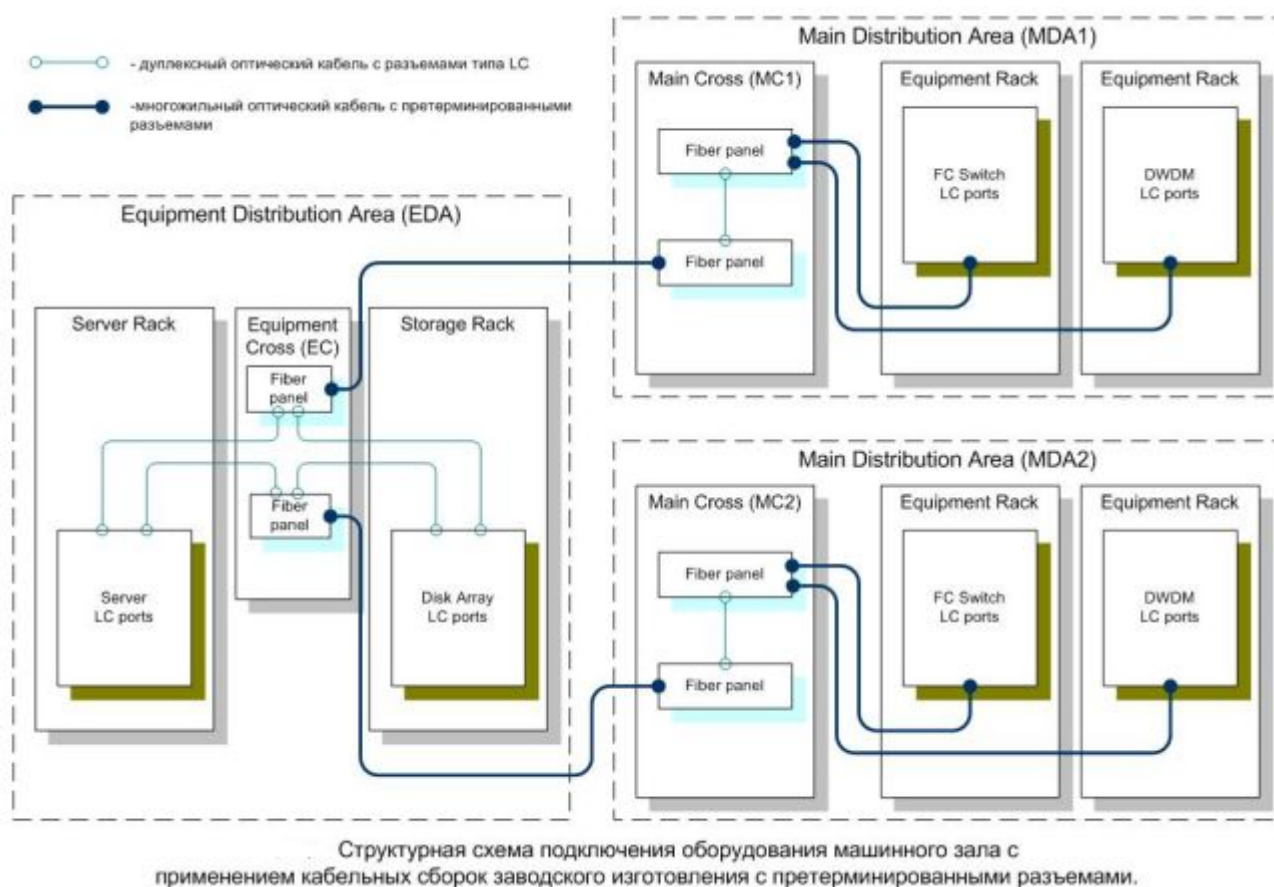


Рис.4.32. Пример схемы кабельных соединений ЦОД с претерминированными разъёмами

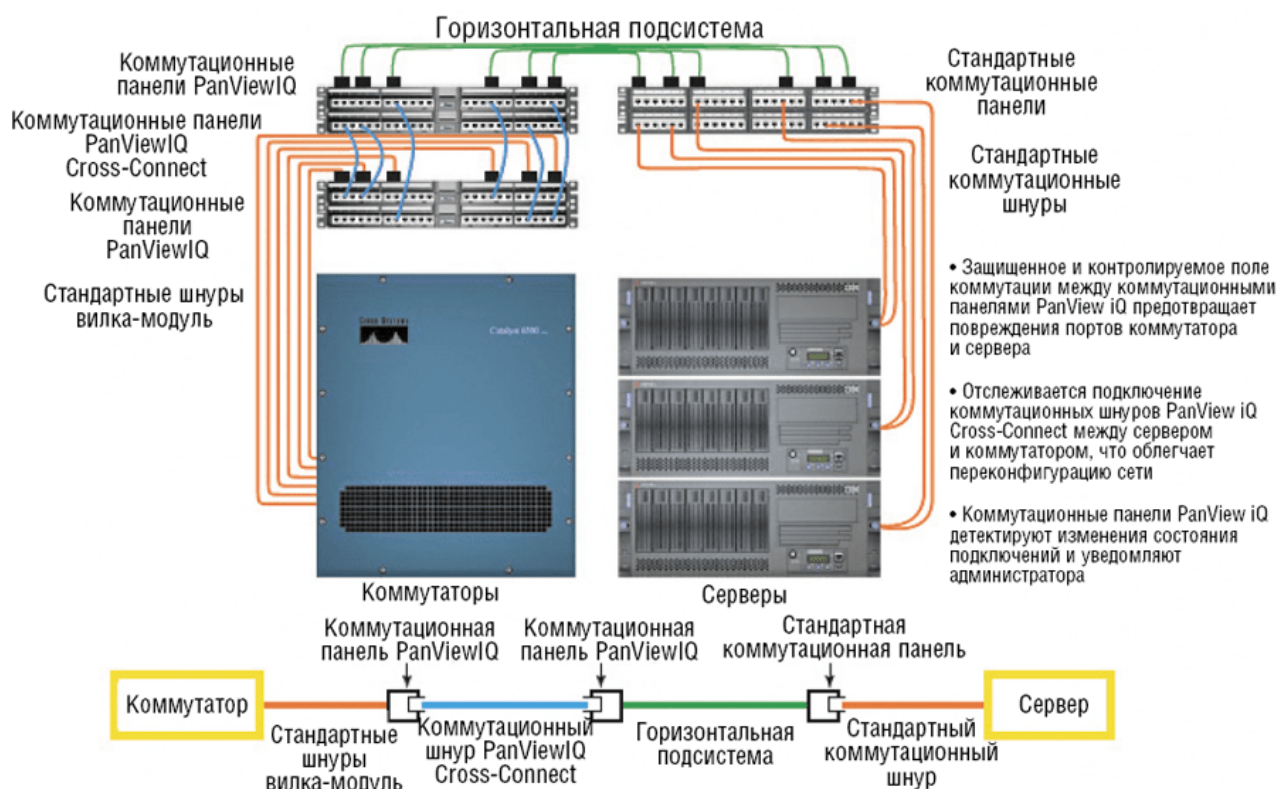


Рис.4.33. Пример схемы соединений сервера и коммутатора ЦОД

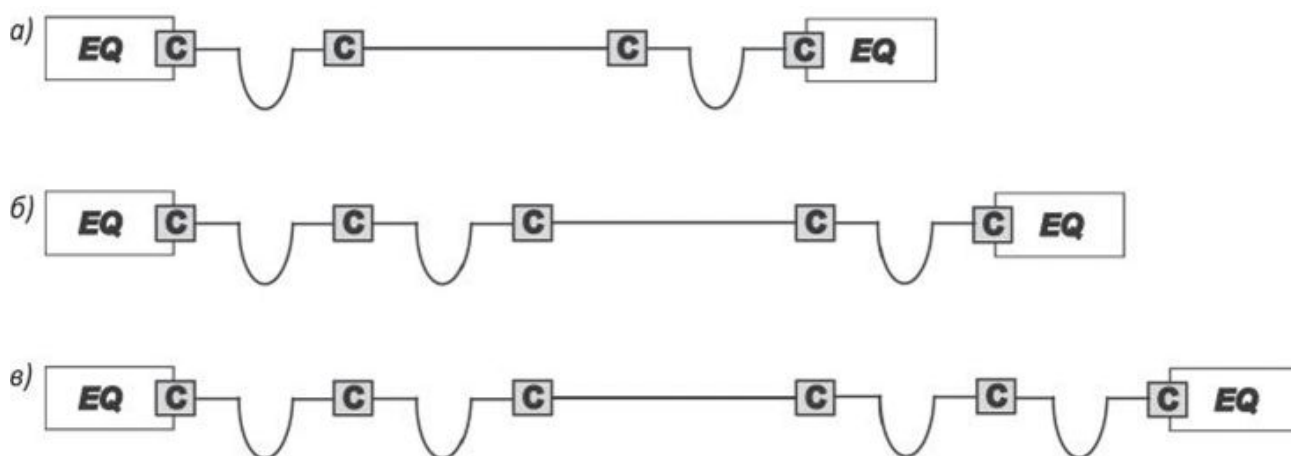


Рис.4.34. Примеры вариантов схем претерминированных соединений в СКС:
а) двухконнекторная; б) трёхконнекторная; в) четырёхконнекторная

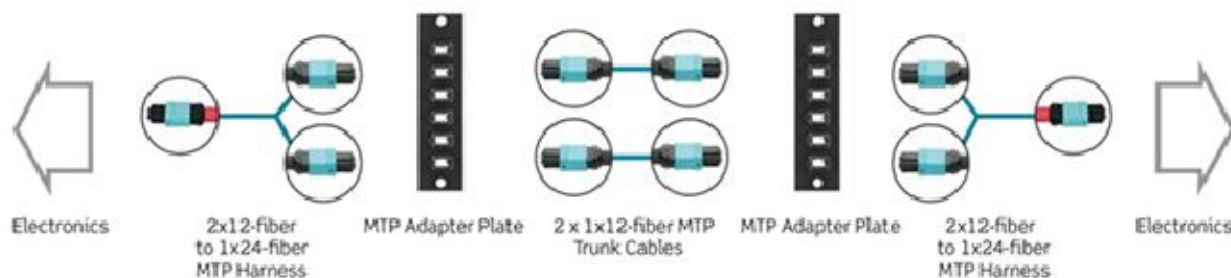


Рис.4.35. Пример соединительной 12 волоконной системы на скорость 100 Гбит/с

4.13. Соединения между ЦОД (на примере комплекса оборудования ВОЛГА, Т8)

Особенность инфраструктуры центров обработки данных — это наличие холодного и горячего коридоров и соответствующая схема охлаждения оборудования в ЦОД. Важным требованием к телеком-оборудованию является поддержка высокоскоростных клиентов, их эффективная агрегация в канале с высокой пропускной способностью.

Шасси для ЦОД (DCI) позволяют операторам организовать DWDM-каналы высокой емкости для соединения центров обработки данных в рамках города или на более удаленные расстояния (рис.4.36-4.38). Компактная платформа позволяет не только эффективно разместить до двух (V3 DCI) или шести (V6 DCI) высокоскоростных агрегаторов, но и оптическую линейную систему в одном шасси.

С помощью линейных карт семейства M1200 в DCI-исполнении можно в одном шасси V3 DCI организовать передачу информации до 2.4 Тбит/с, а в шасси V6 DCI — до 7.2 Тбит/с.

Отвечая на потребности ЦОД-клиентов, в рамках DCI-линейки, компания Т8 разработала карты с широким набором мультисервисных клиентских интерфейсов. Так блок агрегатора M400-2C2-20P2Q поддерживает высокоскоростные опции СХД-протоколов FibreChannel наряду с Ethernet-клиентами до 400GE.

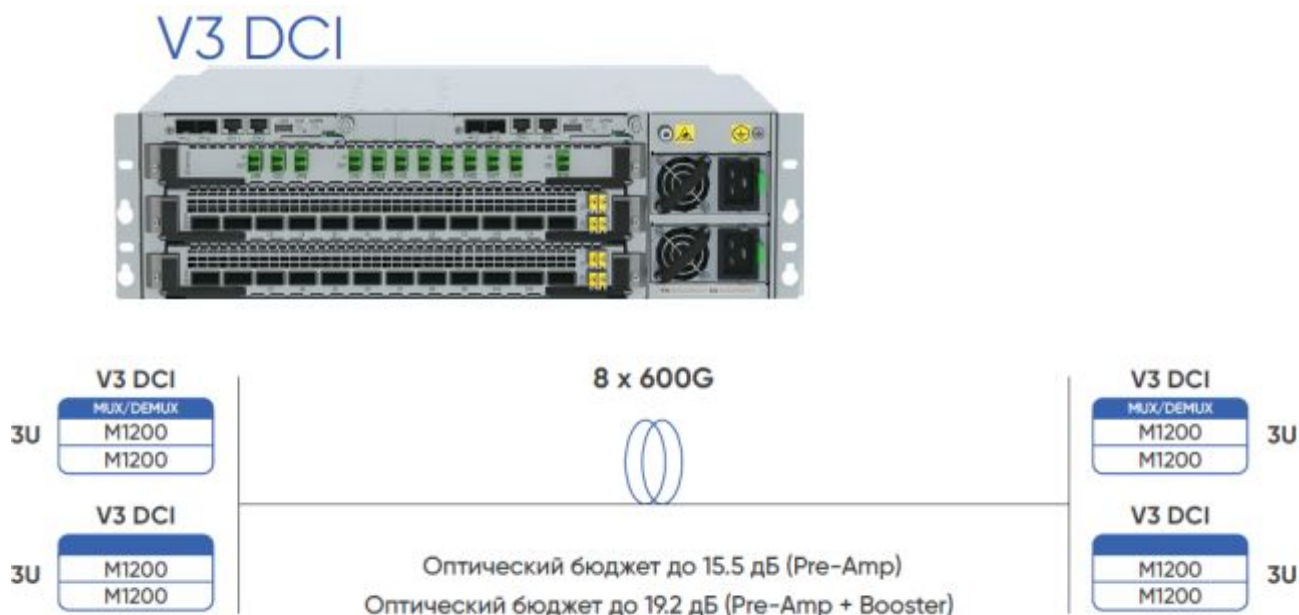


Рис.4.36. Пример оборудования и схемы включения для между ЦОД соединений

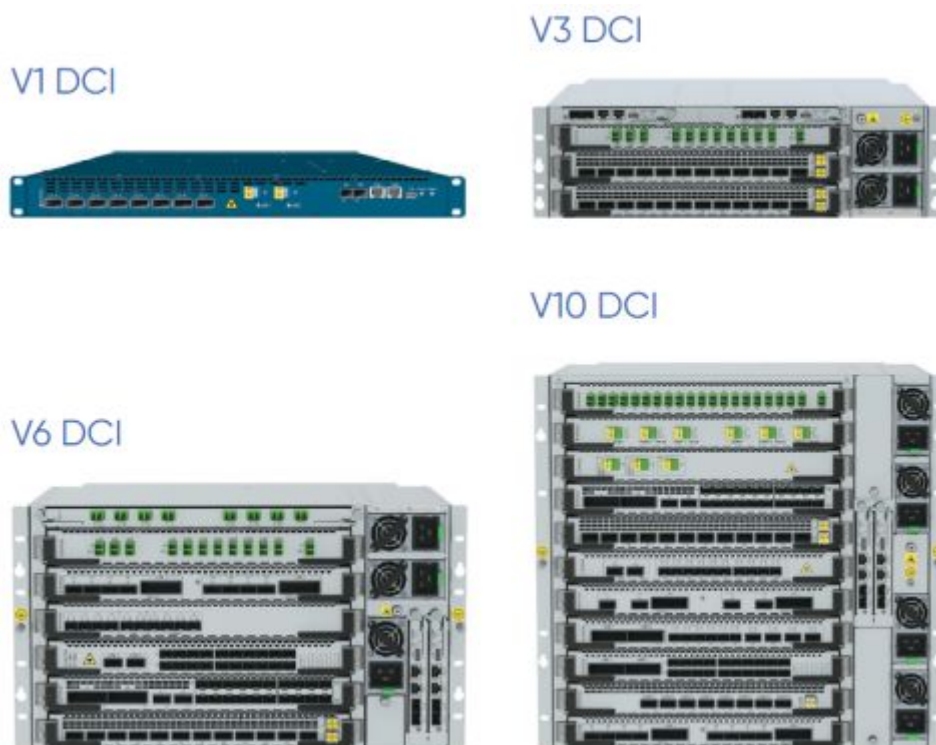


Рис.4.37. Оборудование для организации высокоскоростных межсоединений ЦОД. Варианты комплектования для ЦОД

Блок агрегатора M800-1-8Q

Агрегация до 8 x 100G клиентов и передача до 800 Гбит/с по одной длине волны



Рис. 4.38. Оборудование для организации высокоскоростных межсоединений ЦОД – мукспондер 8×100Гбит/с

Для проведения экспериментальных исследований по между ЦОДовым соединениям в 2023 году использовалась передовая отечественная DWDM-платформа «Волга» компании «Т8». Рассматривается применение разработки для создания квантозащищенных каналов связи между ЦОДами.

4.14. Безопасность коммутаций в ЦОД

Человеческий фактор

Как показывают многочисленные исследования, одним из основных факторов, приводящих к отказам в сети, является человеческий фактор. А представьте, какие финансовые потери могут ожидать компанию, если кто-то из техников по ошибке выдернет шнур подключения из гнезда какого-нибудь активного оборудования в ЦОД? Вероятность такого события увеличивается тем обстоятельством, что в ЦОД могут работать не только инженеры-кабельщики, но и специалисты, занятые обслуживанием каких-либо других инженерных систем или основного оборудования.

Очевидно, что защита точек физического подключения от не санкционированных и случайных действий является важнейшим элементом обеспечения безопасности ЦОД. Для этого компании производители реализуют трехуровневую систему безопасности, которая построена на основе концепции "умных отверстий". Все коммутационные панели и розетки выпускаются с такими отверстиями, подготовленными для установки средств безопасности.

Уровень 1, визуальное кодирование

Цветовое кодирование разъемов, розеток и коммутационных панелей, осуществляемое с помощью специальных клипс, крышечек и рамок, "подсказывает" обслуживающему персоналу, как правильно подключать медные и оптические шнуры (рис.4.39): синюю вилку в синюю розетку, красную в красную и т. д.

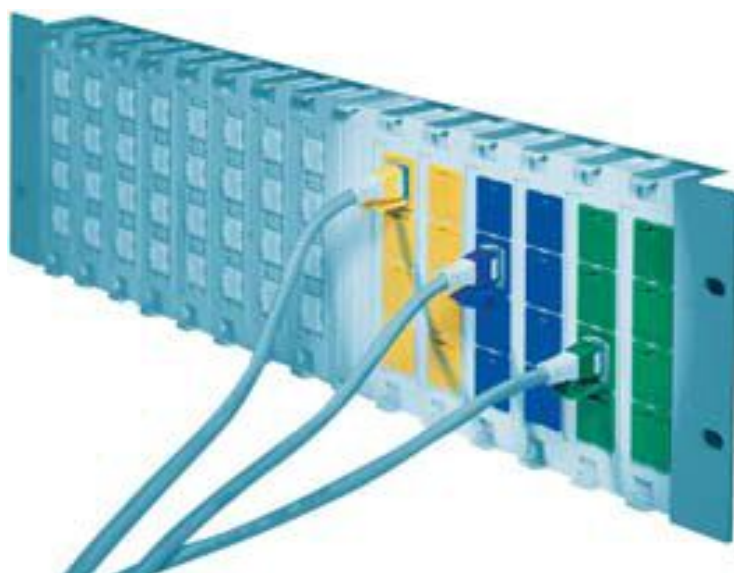


Рис.4.39. Пример визуального кодирования

Уровень 2, к цветному добавляется механическое кодирование (рис.4.40)

Механическое кодирование реализуется с помощью элементов Data Safe Lock, которые механически препятствуют неправильному подключению разъемов.



Рис.4.40. Пример механического кодирования разъемов

Уровень безопасности 3 блокировка разъемных соединений

Третий уровень безопасности, предохраняющий от случайного разъединения, содержит блокирующее устройство (рис.4.41-4.44). Защитные пластиковые рамки "Plug Guard" и "Fiber Guard",надежно защищающие разъемные соединения в розетках и на панелях переключения, могут быть открыты только при помощи специального ключа. Только авторизованный персонал может осуществить переподключение устройств. Потеря данных уже невозможна. "Plug Guard" производится в трех различных цветах, "Fiber Guard" имеет дополнительные сменные цветные клипсы. Когда же нам необходимо защитить ту или иную розетку RJ45 от подключения используется специальная защитная вставка "Jack Guard". Она устанавливается в модульную рамку "Plug Guard" и может быть извлечена из нее только при помощи ключа. Это лучшая защита от подключения к Вашей сети. "Safe Clip" используется на шнурах переключения RJ45. Данная клипса блокирует язычок разъема, что делает невозможным его извлечение из модуля. Может с успехом использоваться с активным оборудованием."Patch Guard" " новое решение. Устройство устанавливается на шнуры переключения, и после подсоединения надежно блокирует язычок RJ45 разъема. Разблокировать устройство можно только при помощи специального ключа. Разноцветные клипсы помогут закодировать различные сервисы. Компактная форма устройства обеспечивает возможность использования его при работе с активным оборудованием, где плотность подключения необычайно высока.



Рис.4.41. "Plug Guard" надежно защищает разъемные соединения RJ45. Блокирующий механизм может быть открыт только при помощи специального ключа.



Рис.4.42. "Jack Guard" - защитная вставка в розетки и панели RJ45. Может быть извлечена только при помощи специального ключа.

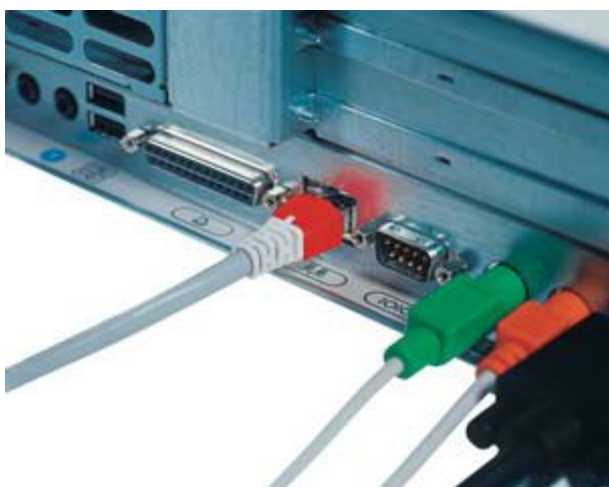


Рис.4.43. "Safe Clip" - решение для медных разъемов, защита от отключения, в том числе и от активного оборудования.



Рис.4.44. "Patch Guard" новое слово в безопасности при работе с активным оборудованием.

Защита корпоративной информации стоит на первом месте для многих компаний. И здесь нельзя идти на компромиссы: потеря важной информации или ее попадание в руки злоумышленников чреватые громадными убытками, а, возможно, и разорением компании. Нужно учитывать все возможные уязвимости (рис.4.45).



Рис.4.45. Компоненты ЦОД, уязвимые для несанкционированного доступа к информационным сигналам

4.15. Системы обеспечения безопасности ЦОД

Центры обработки данных являются местом хранения и обработки критически важных данных организаций, включая информацию, которая должна быть надежно защищена. Перемещение все большего количества данных в цифровой формат, растущий объем трафика, генерируемого населением планеты, Интернетом вещей и онлайн-транзакциями, увеличение числа предприятий, внедряющих платформы облачных вычислений, распространение новых технологий, таких как виртуализация рабочих мест, появление программно определяемых хранилищ, программно определяемых сетей умножают совокупный объем информации, которая становится все более уязвимой для атак вредоносных программ и угроз вторжения, вызывают потребность в усилении защитных мер и модернизации существующих систем безопасности ЦОД (рис.4.46). Комбинация нескольких решений для физической безопасности с системами информационной безопасности позволяет центрам обработки данных реализовать эффективную защиту данных.

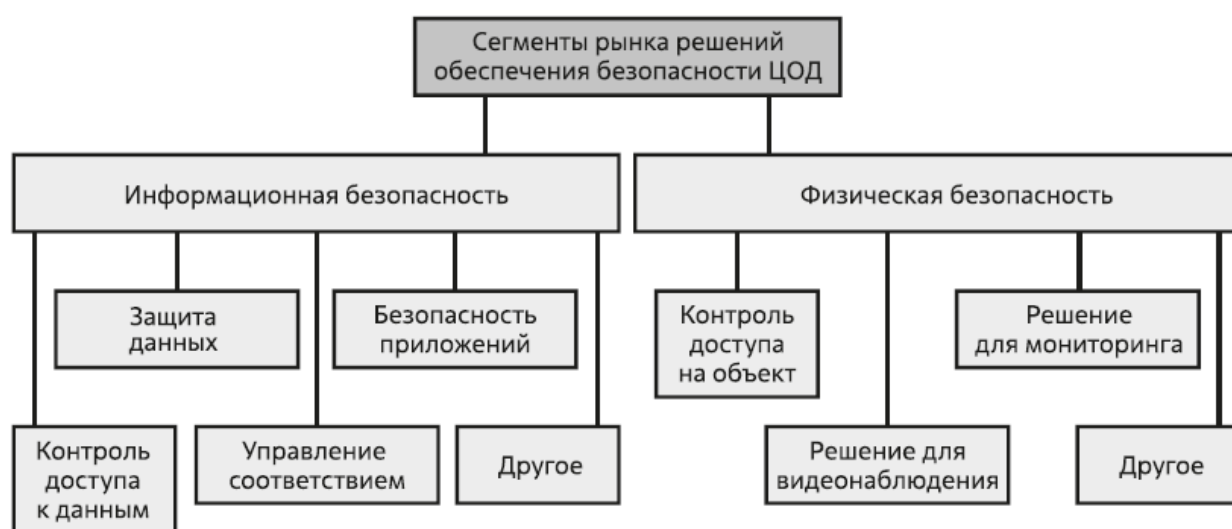


Рис.4.46. Сегментация решений по обеспечению безопасности ЦОД

Информационная безопасность. К средствам защиты данных относятся средства шифрования (шифрование во время передачи данных, хранение в зашифрованном виде), резервное копирование и восстановление данных, архивирование, аварийное восстановление, токенизация, средства предотвращения потери данных и т. п. Токенизация – процесс замены конфиденциального элемента данных на неконфиденциальный эквивалент, называемый токеном. Токен – идентификатор, который сопоставляется с конфиденциальными данными через систему токенизации. Сопоставление исходных данных с токеном использует методы, которые делают невозможным обратное преобразование токенов в исходные данные вне системы токенизации.

Средства обеспечения безопасности приложений – это набор методов и инструментов защиты приложений от угроз, включая несанкционированный

доступ к коду приложений и его изменение на протяжении жизненного цикла приложения. Большинство успешных атак производится путем эксплуатации уязвимостей на уровне приложений, и инструменты обеспечения безопасности приложений служат для исключения подобных атак.

Различают инструменты статического тестирования безопасности приложений, динамического тестирования и средства самозащиты в ходе исполнения. Инструменты статического тестирования безопасности приложений (SAST, Static Application Security Testing) позволяют выявить уязвимости в исходном коде на ранних этапах цикла разработки программного обеспечения. Системы динамического тестирования (DAST, Dynamic Application Security Testing) имитируют атаки на приложение в режиме реального времени. Системы самозащиты приложений (Runtime application self-protection (RASP)) в ходе их исполнения позволяют защищать работающие приложения, имеющие известные и неизвестные уязвимости. К подобным средствам безопасности относятся в том числе антивирусы.

Средства контроля доступа к информации в системах информационной безопасности включают средства идентификации, аутентификации, авторизации и составления отчетности. В отличие от контроля физического доступа, который осуществляется в физической среде, где используется оборудование, к которому нужен доступ, контроль доступа к информации может осуществляться удаленно. Различие между информационными и физическими системами безопасности заключается в характере объекта, в отношении которого осуществляется доступ: доступ к информации предполагает систему информационной безопасности – доступ к физической системе – систему физической безопасности. Средства контроля доступа встраиваются в операционные системы, приложения, системы управления базами данных и т. п. Для аутентификации и авторизации используются различные методы: пользователь может подтвердить свою подлинность (предъявить пароль, идентификационный номер, криптографический ключ, личное устройство аналогичного назначения или биометрический параметр (голос, отпечатки пальцев и т. п.)).

Физическая безопасность.

Суть методов обеспечения физической безопасности сводится к решению двух задач – недопущение или обнаружение несанкционированного доступа на объект или в его определенные зоны (помещения). Наиболее эффективно физическая безопасность работает в форме комплексной многоуровневой стратегии. Обеспечение физической безопасности предполагает не только наличие перечисленных выше устройств и программного обеспечения, но также построение комплексных решений на их основе, использование пассивных средств безопасности, а также внедрение политик обеспечения безопасности и охраны объекта. В качестве примера можно привести нижеследующую модель организации нескольких периметров безопасности.

Основными являются три уровня доступа, или периметра безопасности. Первым, внешним периметром является граница участка, на котором расположен центр обработки данных. Территория земельного участка ЦОД обносится

ограждением, по периметру которого размещаются камеры видеонаблюдения. Ограждение может быть оснащено специальными средствами, препятствующими как преодолению ограды сверху (например, колючая проволока), так и под оградой (например, заглубления ограждения ниже уровня земли). В местах прохода и проезда на территорию организуются контрольно-пропускные пункты, которые могут быть оборудованы турникетами, тамбур-шлюзами, автоматическими воротами, боллардами и шлагбаумами, интегрированными с системами контроля и управления доступом. Камеры на КПП должны фиксировать номер автомобиля и лицо водителя. Каждый въезд и транзитный пункт должны перенаправлять посетителей от одного контрольно-пропускного пункта к другому, что позволяет предприятию сосредоточить доступный персонал службы безопасности в ключевых местах. Альтернативной мерой является сопровождение (эскортирование) посетителей по территории.

Второй периметр – пропускной пункт физической охраны на входе в здание. Входы в здание предусматривают наличие поста охраны; доступ осуществляется посредством турникетов, тамбур-шлюзов или иных устройств, допускающих проход в здание исключительно по одному человеку, а также не позволяющих использовать средства доступа другим лицом (то есть, например, разрешающих лишь однократный проход по карте-ключу в одну сторону). Целесообразно разделять вход для посетителей с зоной разгрузки автотранспорта. В любом случае внутренние подразделения должны контролировать все входы и выходы на объект. Пожарные выходы должны быть оборудованы дверями, которые нельзя открыть снаружи. Аварийные двери должны запираются изнутри, дверные петли также должны быть расположены внутри, чтобы нельзя было снять дверь. Количество окон надо минимизировать, окна в административных помещениях должны быть изготовлены из прочного многослойного стекла. Контроль доступа на базе биометрических идентификаторов необходим во всех ключевых точках как для персонала, так и для посетителей. Внутренний периметр безопасности это вход в машинный зал и технические помещения. Как правило, в дата центрах применяется несколько профилей прав доступа, основанных на его зонировании, что не позволяет, например, ИТ-персоналу ЦОД попасть в технологические помещения или административному персоналу проникнуть в машзал. Системы физической безопасности центров обработки данных могут включать до семи уровней защиты, в том числе различные формы ограждения, замки, биометрические сканеры, начиная от входа на территорию до замков на отдельных серверных шкафах.

4.16. ЦОДЫ в России

«Ростелеком-ЦОД» и DataLine начали строительство московского дата-центра уровня Tier IV на 2 000 стоек

«Ростелеком-ЦОД» строит в Москве новый дата-центр с максимальным уровнем надежности (Tier IV). Дата-центр появится на юго-востоке Москвы по адресу: Остаповский проезд, д. 22, стр. 4. Площадка в 10 150 м² вместит 2 000 стоек по 5 кВт каждая. Общая мощность дата-центра составит 17 МВт.

Строительство ведет объединенная команда «Ростелеком-ЦОД» и DataLine, по стандартам международного института Uptime Institute. В проекте заложен максимально возможный уровень надежности и безопасности дата-центра — Tier IV. Четвертый уровень означает, что все элементы систем и каналы распределения не только зарезервированы, но и защищены от физического разрушения: расположены в отдельных помещениях или проходят разными путями в защищенных коробах. Дата-центр такого уровня гарантирует бесперебойное электроснабжение и непрерывное охлаждение ИТ-оборудования при любом отказе систем дата-центра.

Сейчас список крупнейших операторов ЦОДов в России выглядит следующим образом:

- Ростелеком (35 ЦОДов в стране);
- IXcellerate (3 ЦОДа);
- DataPro (3 ЦОДа);
- Selectel (6 ЦОДов);
- МТС (2 ЦОДа).

Безоговорочным лидером сегмента является «Ростелеком» — у компании стойко-мест больше, чем у всех остальных представителей ТОП-5 вместе взятых. Первая пятерка по итогам 2022 года заняла больше 58% отечественного рынка.

Крупнейшие ЦОД России по количеству стойко-мест

№ 2022	№ 2021	Название компании	Количество стойко- мест на 31.12.2022	Количество стойко- мест на 31.12.2021	Стойки, запущенные в 2022 г.	Планы по запускам в 2023 г.
1	1	Ростелеком	15 461	14 109	1 352	6 909
2	2	DataPro	6 131	4 460	1 671	422
3	3	IXcellerate	5 443	4 044	1 399	836
4	4	Selectel	3 500	3 500	0	112
5	5	МТС	2 883	2 883	0	1 637

Источник: CNews Analytics, 2023

Контрольные вопросы

1. Что представляет собой ЦОД?
2. Для чего предназначены ЦОДы?
3. Какие типы ЦОД различают в классификации?
4. Чем отличаются типы ЦОД?
5. Что относится к кругу инженерной инфраструктуры ЦОД?
6. Что относится к функциональным элементам ЦОД?
7. Какое назначение имеет СКС в ЦОД?
8. Что входит в подсистемы СКС ЦОД?
9. Чем отличаются различные топологии ЦОД?
10. Какие подсистемы относятся к кабельной инфраструктуре ЦОД?
11. Что относится к функциональным узлам ЦОД?
12. Что обозначают сокращения в обозначениях структур СКС ЦОД: MDA, NAD, EDA?
13. В чём особенность соединения между MDA и NDA?
14. Какие стандарты определяют СКС ЦОД?
15. Что обозначает Tier Standard?
16. Какие оптические кабели предусмотрены для использования в ЦОД?
17. Что особенного у оптического кабеля OM5 для применения в ЦОД?
18. Чем отличаются оптические кабели OM1, OM2, OM3, OM4, OM5?
19. В чём преимущество использования одномодового оптического кабеля в ЦОД?
20. Какие преимущества и недостатки использования оптических соединителей MPO в СКС ЦОД?
21. Какие варианты одномодовых оптических интерфейсов предусмотрены в ЦОД?
22. Какие виды активного оборудования соединяются с помощью СКС в ЦОД?
23. Какие классы (категории) электрических кабелей применяются в ЦОД?
24. В чём состоят особенности конструкций и характеристик медных кабелей категорий 6,7,8?
25. Какие существуют предпочтения по использованию кабелей в ЦОД?
26. Чем отличаются топологии кабельной инфраструктуры ЦОД: ToR, MoR, EoR, Centralized?
27. Какая из топологий кабельной инфраструктуры ЦОД наиболее востребована и почему?
28. Что представляют собой претерминированные кабельные решения для ЦОД?
29. Какие оптические модули могут применяться в составе оборудования ЦОД для поддержки высокоскоростной передачи данных?
30. Чем поддерживаются соединения между ЦОДами на коротких и протяженных дистанциях?
31. Какие компании ВАМ известны, как наиболее продвинутые по организации ЦОД в России?

32. Какие системы безопасности предусмотрены для ЦОД?

33. Чем отличаются системы информационной и физической безопасности ЦОД?

34. В чём состоит безопасность коммутаций в ЦОД?

Задача 4.

Составить схему кабельных соединений в ЦОД по варианту в таблицах 1 и 2. На схеме отобразите серверы, коммутаторы агрегации, коммутаторы ядра сети, типы кабельной продукции (медные и оптические), кросс-коммутационное оборудование с коннекторами. При выборе кабельной продукции учесть скоростные режимы передачи на каждом участке СКС и рекомендации по применению кабельной продукции.

Табл.1. Номер варианта соответствует предпоследней цифре студенческого билета или номера пароля

Вариант	0	1	2	3	4	5	6	7	8	9
Количество линий от серверов к коммутаторам	18	26	32	24	36	20	40	38	30	16

Табл.2. Номер варианта соответствует последней цифре номера студенческого билета или пароля

Вариант	0	1	2	3	4	5	6	7	8	9
Тип соединения	Централизованн	ToR	EoR	MoR	Централизованн	ToR	EoR	MoR	ToR	EoR
Скорость сервер-коммутатор	1,25 Гбит/с	1,25 Гбит/с			10 Гбит/с					
Скорость коммутатор - коммутатор		10 Гбит/с	40 Гбит/с	100 Гбит/с		10 Гбит/с	25 Гбит/с	100 Гбит/с	40 Гбит/с	100 Гбит/с

Методические указания:

1. Изучите типы соединений (рис.4.20-4.26) и схемы соединений, приведённые на рис.4.33, 4.34.
2. Используйте рекомендации по применению медных и оптических кабелей для каждого типа соединения.

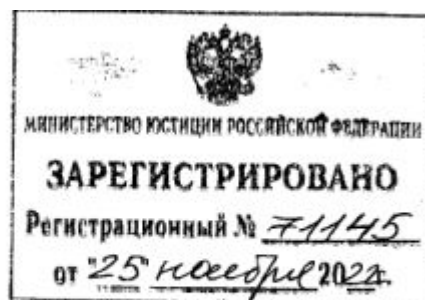
5. Профессиональные стандарты направления оптических сетей и квантовых коммуникаций для специалистов

5.1. Специалист по монтажу и технической эксплуатации квантовых сетей 06.050

Монтаж и техническая эксплуатация сетей квантовых коммуникаций

Основная цель вида профессиональной деятельности:

Обеспечение исправного состояния и функционирования в заданных режимах оборудования и сетей квантовых коммуникаций непосредственно при вводе в эксплуатацию и в течение последующего использования по назначению



МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНТРУД РОССИИ)

ПРИКАЗ

24 октября 2022

Москва

№ 685н

Об утверждении профессионального стандарта «Специалист по монтажу и технической эксплуатации квантовых сетей»

В соответствии с пунктом 16 Правил разработки и утверждения профессиональных стандартов, утвержденных постановлением Правительства Российской Федерации от 22 января 2013 г. № 23 (Собрание законодательства Российской Федерации, 2013, № 4, ст. 293; 2014, № 39, ст. 5266), п р и к а з ы в а ю:

1. Утвердить прилагаемый профессиональный стандарт «Специалист по монтажу и технической эксплуатации квантовых сетей».
2. Установить, что настоящий приказ вступает в силу с 1 марта 2023 г. и действует до 1 марта 2029 г.

Министр

А.О. Котяков

Группа занятий:

2153	Инженеры по телекоммуникациям	3522	Специалисты-техники по телекоммуникационному оборудованию
7422	Монтажники и ремонтники по обслуживанию ИКТ и устройств связи	-	-

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида профессиональной деятельности)

Обобщенные трудовые функции			Трудовые функции		
код	Наименование Что делает	уровень квалификации	наименование	код	уровень (подуровень) квалификации
А	Монтаж, контроль технических характеристик и техническое обслуживание оптической части сети квантовых коммуникаций	<p style="text-align: center;">3</p> <p>Должность: Кабельщик-спайщик волоконно-оптической линии связи 7-го разряда Кабельщик-спайщик волоконно-оптической линии связи 8-го разряда Монтажник волоконно-оптической линии связи Монтажник сети квантовых коммуникаций</p> <p>Образование: Профессиональное обучение - программы профессиональной подготовки по профессиям рабочих, должностям служащих, программы переподготовки рабочих, служащих, программы повышения квалификации рабочих, служащих</p> <p>Опыт: Не менее одного года по профессии кабельщик-спайщик</p>	Входной контроль волоконно-оптического кабеля (далее - ВОК)	А/01.3	3
			Монтаж ВОК, оптических кроссов, механических соединителей и коннекторов	А/02.3	3
			Выполнение работ по измерениям параметров оптической части сети квантовых коммуникаций	А/03.3	3
			Техническое обслуживание оптической части сети квантовых коммуникаций	А/04.3	3
В	Монтаж оборудования станционной части	<p style="text-align: center;">4</p> <p>Должность: Монтажник оборудования квантовых</p>	Приемка оборудования сети квантовых	В/01.4	4

	сети квантовых коммуникаций	коммуникаций 6-го разряда Монтажник оборудования квантовых коммуникаций 7-го разряда Образование: Среднее профессиональное образование - программы подготовки квалифицированных рабочих, служащих и дополнительное профессиональное образование по программам повышения квалификации рабочих, служащих по работе с обслуживаемым оборудованием Опыт:	коммуникаций на монтажной площадке с проверкой его соответствия проектным документам		
			Подготовка оборудования, узлов и деталей сети квантовых коммуникаций к монтажу в соответствии с рабочей документацией проекта и (или) схемой организации связи	В/02.4	4
			Монтаж ВОК станционной части сети квантовых коммуникаций	В/03.4	4
			Сборка и монтаж арматуры несущих систем	В/04.4	4
			Монтаж оборудования квантовых коммуникаций в несущие системы	В/05.4	4
С	Организация монтажных работ и комплексная проверка монтажа участка сети квантовых коммуникаций	5 Должность: Мастер по монтажу сети квантовых коммуникаций Техник по монтажу и технической эксплуатации квантовых сетей Образование: Среднее профессиональное образование - программы подготовки специалистов среднего звена (Сети связи и системы коммутации, Оптические и оптико-электронные приборы и системы) Опыт: Не менее одного года по профессии монтажник сети квантовых коммуникаций или	Организация монтажа участка сети квантовых коммуникаций	С/01.5	5
			Проверка соответствия результатов монтажа участка сети квантовых коммуникаций технической документации	С/02.5	5
			Проведение испытаний	С/03.5	5

		монтажник оборудования квантовых коммуникаций	смонтированного участка сети квантовых коммуникаций, предварительная настройка оборудования для обеспечения удаленного управления оборудованием		
D	Организация технического обслуживания и материально- технического обеспечения технической эксплуатации сети квантовых коммуникаций	6 Должность: Инженер Инженер по эксплуатации сети квантовых коммуникаций Инженер по телекоммуникациям Инженер электросвязи Образование: Среднее профессиональное образование - программы подготовки специалистов среднего звена и дополнительное профессиональное образование по программам повышения квалификации по работе с обслуживаемым оборудованием или Высшее образование – бакалавриат 11.03.02 Инфокоммуникационные технологии и системы связи, 12.03.03 Фотоника и оптоинформатика Опыт: Не менее трех лет работы по монтажу оборудования станционной части сети квантовых коммуникаций или по организации монтажных работ и комплексной проверки монтажа участка сети квантовых коммуникаций при наличии среднего профессионального образования Не менее одного месяца работы в области монтажа и эксплуатации квантовых сетей при наличии высшего образования - бакалавриат	Управление планово- профилактически ми работами на станционном оборудовании участка сети квантовых коммуникаций	D/01. 6	6
			Управление техническим обслуживанием линейной части сети квантовых коммуникаций	D/02. 6	6
			Материально- техническое обеспечение технической эксплуатации станционного оборудования сети квантовых коммуникаций	D/03. 6	6
E	Устранение технических проблем и технологическое обеспечение	6 Должность: Инженер Инженер по эксплуатации сети квантовых коммуникаций Инженер по телекоммуникациям	Устранение технических проблем на участке сети квантовых	E/01. 6	6

	технической эксплуатации участка сети квантовых коммуникаций	Инженер электросвязи Образование: Высшее образование – бакалавриат 11.03.02 Инфокоммуникационные технологии и системы связи, 12.03.03 Фотоника и оптоинформатика и дополнительное профессиональное образование по программам повышения квалификации по работе с обслуживаемым оборудованием Опыт: Не менее трех месяцев в области монтажа и эксплуатации квантовых сетей	коммуникаций		
			Технологическое обеспечение технической эксплуатации стационарного оборудования сети квантовых коммуникаций	Е/02.6	6

3.5.1. Трудовая функция (пример для инженера с образованием бакалавриат)

Наименование	Устранение технических проблем на участке сети квантовых коммуникаций	Код	Е/01.6	Уровень (подуровень) квалификации	6
--------------	---	-----	--------	-----------------------------------	---

Происхождение трудовой функции	Оригинал	X	Заимствовано из оригинала		
--------------------------------	----------	---	---------------------------	--	--

Код оригинала Регистрационный номер профессионального стандарта

Трудовые действия	Получение и формализация сообщений о наличии технических проблем в работе сети квантовых коммуникаций
	Перевод сети квантовых коммуникаций на резервную схему организации связи в соответствии с графиком обходов и замен
	Установление факта и локализация неисправности стационарного оборудования сети квантовых коммуникаций, вызвавшей техническую проблему в работе сети
	Замена неисправного элемента в соответствии с разработанными технологическими картами на обслуживаемое оборудование
	Контроль устранения неисправности стационарного оборудования сети квантовых коммуникаций
	Восстановление основной схемы организации связи (работы оборудования)
	Разработка предложений по улучшению процесса устранения технических проблем в работе сети квантовых коммуникаций

	Оформление отправки неисправного элемента на дополнительное исследование/ремонт в сервисный центр
	Документирование работ по решению технической проблемы в работе сети квантовых коммуникаций
Необходимые умения	Извлекать из сообщений о наличии технической проблемы в работе сети квантовых коммуникаций информацию, необходимую для устранения технических проблем на участке сети квантовых коммуникаций
	Локализовать неисправности стационарного оборудования сети квантовых коммуникаций
	Переходить на резервную схему организации связи (работы оборудования) в соответствии с графиком обходов и замен
	Проводить замену неисправных элементов
	Контролировать устранение неисправности стационарного оборудования сети квантовых коммуникаций в результате замены элемента
	Переходить после устранения неисправности заменой элемента на основную схему организации связи (работы оборудования)
	Описывать опыт устранения технических проблем в работе сети квантовых коммуникаций
	Оформлять отставку неисправного элемента на дополнительное исследование/ремонт в сервисном центре
	Документировать работы по решению технической проблемы на стационарном оборудовании сети квантовых коммуникаций
Необходимые знания	Теоретические основы электросвязи и инфокоммуникационных технологий
	Теория распространения света в направленной среде
	Теоретические основы квантовых коммуникаций, в том числе: математический анализ, теория вероятностей, квантовая механика, квантовая криптография
	Физико-технологические основы волоконно-оптической техники
	Предпосылки разработки, принципы и структура OSI
	Структура системы рекомендаций и стандартов в области телекоммуникаций
	Основные положения рекомендаций и стандартов в области квантовых коммуникаций
	Правила технической эксплуатации стационарного оборудования сети квантовых коммуникаций
	Состав и эксплуатационные характеристики обслуживаемого стационарного

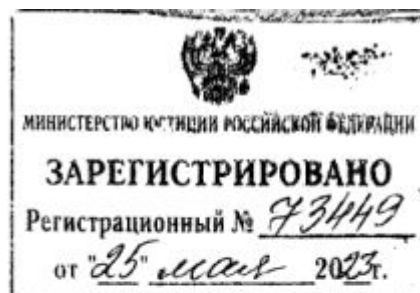
	оборудования сети квантовых коммуникаций
	Методы локализации неисправностей обслуживаемого оборудования квантовых коммуникаций
	Алгоритмы перехода на резервные схемы организации связи (работы оборудования)
	Основные неисправности стационарного оборудования сети квантовых коммуникаций и их признаки
	Порядок замены элементов обслуживаемого оборудования сети квантовых коммуникаций
	Алгоритм контроля устранения неисправности обслуживаемого оборудования сети квантовых коммуникаций
	Правила оформление отправки неисправного элемента на дополнительное исследование/ремонт в сервисном центре
	Правила документирования работ по устранению технических проблем в работе сети связи
	Правила технической эксплуатации, применимые к обслуживаемому оборудованию сети квантовых коммуникаций, установленные руководящими документами отрасли
	Правила информационной безопасности при работе с оборудованием квантовых коммуникаций
	Основные возможности программного обеспечения, применяемого при разработке, редактировании, экспертизе, согласовании и утверждении документов
	Требования нормативных правовых актов по защите охраняемой законом тайны
	Основные права и обязанности работника и работодателя в соответствии с трудовым законодательством Российской Федерации
	Общие требования охраны труда, противопожарной защиты и экологической безопасности
	Межотраслевые требования охраны труда при эксплуатации электроустановок
	Правила технической эксплуатации электроустановок потребителей
	Требования охраны труда при работах на обслуживаемом оборудовании
	Правила и порядок оформления технической и технологической документации

5.2. Специалист по исследованиям и разработкам в области квантовых коммуникаций 06.054

Разработка оборудования, приборов и комплексов для систем квантовых коммуникаций, исследования в указанной сфере

Основная цель вида профессиональной деятельности:

Обеспечение развития техники и технологий квантовых коммуникаций



**МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНТРУД РОССИИ)**

ПРИКАЗ

25 апреля 2023

Москва

№ *327н*

**Об утверждении профессионального стандарта
«Специалист по исследованиям и разработкам в области квантовых
коммуникаций»**

В соответствии с пунктом 20 Правил разработки и утверждения профессиональных стандартов, утвержденных постановлением Правительства Российской Федерации от 10 апреля 2023 г. № 580, п р и к а з ы в а ю:

1. Утвердить прилагаемый профессиональный стандарт «Специалист по исследованиям и разработкам в области квантовых коммуникаций».

2. Установить, что настоящий приказ вступает в силу с 1 сентября 2023 г. и действует до 1 сентября 2029 г.

Министр

А.О. Котяков

Группа занятий:

1223	Руководители подразделений по научным исследованиям и разработкам	2149	Специалисты в области техники, не входящие в другие группы
2153	Инженеры по телекоммуникациям	3119	Техники в области физических и технических наук, не входящие в другие группы
3522	Специалисты-техники по телекоммуникационному оборудованию	3323	Закупщики

Отнесение к видам экономической деятельности:

61.10	Деятельность в области связи на базе проводных технологий
72.19	Научные исследования и разработки в области естественных и технических наук прочие

(код ОКВЭД <2>)

(наименование вида экономической деятельности)

**II. Описание трудовых функций,
входящих в профессиональный стандарт
(функциональная карта вида профессиональной деятельности)**

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
A	Обеспечение элементной базой и конструктивными изделиями процесса разработки оборудования, приборов и комплексов для систем квантовых коммуникаций	5 Должность: Товаровед Специалист по снабжению производства оборудования квантовых коммуникаций Образование: Среднее профессиональное образование - программы подготовки специалистов среднего	Определение соответствия предложений предложений элементной базы и конструктивных изделий, предназначенных для сборки опытных образцов оборудования и приборов для систем квантовых коммуникаций, требованиям технической документации	A/01.5	5

		<p>звена и</p> <p>Дополнительное профессиональное образование - программы повышения квалификации в области электронных, оптических и оптико-электронных приборов, устройств и систем</p> <p>Опыт:.....</p>	<p>Обеспечение наличия материалов, комплектующих и оборудования, необходимых для разработки оборудования, приборов и комплексов для систем квантовых коммуникаций; сборки схемотехнических решений для систем квантовых коммуникаций; сборки, тестирования и настройки опытных образцов оборудования и приборов для систем квантовых коммуникаций</p>	A/02.5	5
В	Входной контроль качества элементной базы и конструктивных изделий для сборки оборудования и приборов для систем квантовых коммуникаций	<p>5</p> <p>Должность: Контролер комплектующих материалов для производства оборудования квантовых коммуникаций Оператор входного контроля</p> <p>Образование: Среднее профессиональное образование - программы подготовки специалистов среднего звена</p> <p>Опыт:....</p>	<p>Входной контроль элементной базы и конструктивных изделий, предназначенных для сборки опытных образцов оборудования и приборов для систем квантовых коммуникаций, на предмет соответствия требованиям технической документации</p>	В/01.5	5
			<p>Документирование результатов входного контроля и претензионная работа по вопросам качества элементной базы и приборов для систем квантовых</p>	В/02.5	5

			коммуникаций		
С	Сборка моделей схемотехнических решений для систем квантовых коммуникаций; сборка, тестирование и настройка опытных образцов оборудования и приборов для систем квантовых коммуникаций	<p>5</p> <p>Должность: Техник-конструктор оборудования квантовых коммуникаций Техник-тестировщик оборудования квантовых коммуникаций</p> <p>Образование: Среднее профессиональное образование - программы подготовки специалистов среднего звена</p> <p>Опыт:...</p>	Осуществление сборки моделей схемотехнических решений для систем квантовых коммуникаций	С/01.5	5
			Осуществление сборки опытных образцов оборудования, приборов и комплексов для систем квантовых коммуникаций	С/02.5	5
			Проведение тестирования и настройки моделей схемотехнических решений и опытных образцов оборудования, приборов и комплексов для систем квантовых коммуникаций	С/03.5	5
			Документирование результатов сборки, тестирования и настройки оборудования, приборов и комплексов для систем квантовых коммуникаций	С/04.5	5
D	Разработка оборудования и приборов для систем квантовых коммуникаций	<p>6</p> <p>Должность: Инженер-конструктор Конструктор</p> <p>Образование: Высшее образование – бакалавриат 11.03.02 Инфокоммуникационные технологии и системы связи, 12.03.03 Фотоника и</p>	Подготовка и проведение лабораторных исследований схемотехнических решений для систем квантовых коммуникаций	D/01.6	6
			Документирование лабораторных исследований	D/02.6	6

		оптоинформатика	схемотехнических решений		
			Проектирование и конструирование оборудования и приборов для систем квантовых коммуникаций	D/03.6	6
			Разработка проектной конструкторской документации, рабочей конструкторской документации при проектировании оборудования и приборов для систем квантовых коммуникаций	D/04.6	6
			Подготовка опытных образцов оборудования, приборов и комплексов для систем квантовых коммуникаций для передачи на этап эксплуатации	D/05.6	6
Е	Разработка инновационного оборудования и комплексов для систем квантовых коммуникаций	7 Должность: Ведущий конструктор Ведущий инженер - конструктор Образование: Высшее образование - специалитет, магистратура 11.04.02 Инфокоммуникационные технологии и системы связи, 12.04.03 Фотоника и оптоинформатика, 11.05.04 Инфокоммуникационные технологии и системы специальной связи Опыт: Не менее	Разработка схемотехнических решений для систем квантовых коммуникаций	Е/01.7	7
			Проектирование и конструирование инновационного оборудования и комплексов для систем квантовых коммуникаций	Е/02.7	7
			Разработка проектной конструкторской документации, рабочей конструкторской	Е/03.7	7

		<p>одного года на инженерно-технической должности в соответствующей профилю организации отрасли</p> <p>Особые условия допуска к работе:</p> <p>Наличие допуска к государственной тайне</p>	документации при проектировании инновационного оборудования и комплексов для систем квантовых коммуникаций, путей и средств их реализации		
			Патентное обеспечение разработки оборудования, приборов и комплексов для систем квантовых коммуникаций	E/04.7	7
			Оценка эффективности решения задач разработки оборудования, приборов и комплексов для систем квантовых коммуникаций с применением методов математического, физического, компьютерного моделирования и натурных испытаний	E/05.7	7
F	Проведение научных исследований в области квантовых коммуникаций и оформление их результатов	<p>7</p> <p>Должность: Научный сотрудник</p> <p>Ведущий научный сотрудник</p> <p>Образование: Высшее образование - специалитет, магистратура 11.04.02 Инфокоммуникационные технологии и системы связи, 12.04.03 Фотоника и оптоинформатика,</p>	Проведение теоретических и экспериментальных исследований в области создания и эксплуатации оборудования, приборов и комплексов для систем квантовых коммуникаций	F/01.7	7
			Подготовка рекомендаций по стандартизации	F/02.7	7

		11.05.04Инфокоммуни кационные технологии и системы специальной связи и др. Опыт: Не менее одного года на научной должности в соответствующей профилю организации отрасли Особые условия: Наличие допуска к государственной тайне Для ведущего научного сотрудника - наличие ученой степени	решений в области создания и эксплуатации оборудования, приборов и комплексов для систем квантовых коммуникаций		
			Подготовка публикаций в области создания и эксплуатации оборудования, приборов и комплексов для систем квантовых коммуникаций	F/03.7	7
			Оформление результатов научных исследований в области квантовых коммуникаций в соответствии с требованиями стандартов	F/04.7	7
G	Руководство разработкой оборудования, приборов и комплексов для систем квантовых коммуникаций и развитие технологии их производства	8 Должность: Главный конструктор Образование: Высшее образование - специалитет, магистратура и Дополнительное профессиональное образование - программы повышения квалификации, профессиональной переподготовки в области управления предприятием Опыт: Не менее пяти лет на инженерно- технических и руководящих	Определение цели и постановка задач развития технологий производства оборудования, приборов и комплексов для систем квантовых коммуникаций, путей и средств их реализации	G/01.8	8
			Разработка стратегии решения задач исследовательского и проектного характера, направленных на разработку и запуск производства	G/02.8	8

		должностях в соответствующей профилю организации отрасли Особые условия: Наличие допуска к государственной тайне	оборудования, приборов и комплексов для систем квантовых коммуникаций		
			Оценка экономической эффективности, необходимости и возможности инвестирования средств в создание технологической базы для выпуска оборудования, приборов и комплексов для систем квантовых коммуникаций	G/03.8	8
			Распределение ресурсов для ведения проектных и экспериментальных работ по созданию технологий, необходимых для подготовки производства оборудования, приборов и комплексов для систем квантовых коммуникаций	G/04.8	8
			Установление объема, порядка и графика финансирования проектных и экспериментальных работ в области производства оборудования, приборов и комплексов для систем квантовых коммуникаций	G/05.8	8
			Оценка	G/06.8	8

			возможности запуска производства оборудования, приборов и комплексов для систем квантовых коммуникаций, путей и средств его реализации на основе разработанной технологии и технологической базы		
--	--	--	--	--	--

3.4.1. Трудовая функция (пример для инженера с образованием бакалавриат)

Наименование	Подготовка и проведение лабораторных исследований схемотехнических решений для систем квантовых коммуникаций	Код	D/01.6	Уровень (подуровень) квалификации	6
--------------	--	-----	--------	-----------------------------------	---

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
--------------------------------	------------	---------------------------	--	--

Код оригинала Регистрационный номер профессионального стандарта

Трудовые действия	Ознакомление с отечественным и зарубежным опытом разработки систем квантовых коммуникаций и их составных частей
	Ознакомление с результатами ранее проведенных теоретических и экспериментальных исследований в области создания образцов систем квантовых коммуникаций
	Разработка инфраструктурного листа, программы и методики лабораторного исследования схемотехнического решения для систем квантовых коммуникаций
	Подготовка аппаратной и программной части лабораторного испытательного стенда в соответствии с инфраструктурным листом, программой и методикой лабораторного исследования схемотехнического решения для систем квантовых коммуникаций
	Проведение лабораторного исследования схемотехнического решения для систем квантовых коммуникаций

	Первичная регистрация результатов лабораторного исследования схемотехнического решения для систем квантовых коммуникаций
	Обработка результатов лабораторного исследования схемотехнического решения для систем квантовых коммуникаций
	Подготовка отчета о лабораторном исследовании схемотехнического решения для систем квантовых коммуникаций
	Разработка рекомендаций и заключений по использованию результатов лабораторного исследования схемотехнического решения для систем квантовых коммуникаций
Необходимые умения	Обрабатывать сведения об опыте разработки систем квантовых коммуникаций и их составных частей с целью выявления информации, полезной для проведения лабораторных исследований схемотехнических решений для систем квантовых коммуникаций
	Обрабатывать результаты ранее проведенных теоретических и экспериментальных исследований в области создания образцов систем квантовых коммуникаций с целью выявления информации, полезной для проведения лабораторных исследований схемотехнических решений для систем квантовых коммуникаций
	Разрабатывать программы и методики исследований в области создания образцов систем квантовых коммуникаций
	Описывать требования к аппаратной и программным частям стендов для проведения лабораторных исследований
	Программировать на функциональных языках
	Проводить исследования в соответствии с программой и методикой исследований в области создания образцов систем квантовых коммуникаций
	Проводить обработку экспериментальных данных с использованием электронных таблиц, баз данных и специализированного программного обеспечения
	Готовить заключения по использованию результатов теоретических и экспериментальных исследований в области создания образцов систем квантовых коммуникаций
	Разрабатывать отчеты о проведенных исследованиях
Необходимые знания	Теоретические основы электросвязи и инфокоммуникационных технологий
	Принципы функционирования систем и средств электросвязи и инфокоммуникационных систем, в том числе систем квантовых коммуникаций.
	Теоретические основы квантовых коммуникаций, в том числе:

	математический анализ, дискретная математика, теория вероятностей, основы квантовой механики и нелинейной оптики, физико-технологические основы волоконно-оптической техники
	Структура системы рекомендаций и стандартов в области телекоммуникаций
	Основы законодательства Российской Федерации в области интеллектуальной собственности
	Понятие жизненного цикла изделия
	Основные положения рекомендаций и стандартов в области квантовых коммуникаций
	Устройства распределения оптического сигнала (сплиттеры, циркуляторы, поляризаторы, фазовые модуляторы, уплотнители частоты, полосовые фильтры, аттенюаторы, волоконные брегговские решетки)
	Источники излучения: полупроводниковые лазеры, волоконные лазеры и усилители, однофотонные источники
	Измерительные устройства для исследования квантовых коммуникаций: волоконные интерферометры, спектрометры, измерители мощности, светодиоды, однофотонные детекторы
	Протоколы квантовой криптографии и их основные реализации
	Методы математической обработки данных
	Программное обеспечение визуализации и обработки данных
	Требования к системам квантовой коммуникации
	Основы проектирования, конструирования и производства интерферометров
	Основы проектирования, конструирования и производства систем квантовых коммуникаций
	Основы проектирования сложных систем
	Архитектура и основы применения процессорных модулей "система на модуле"
	Объектно-ориентированные и функциональные языки программирования
	Методы выполнения патентного поиска
	Технический английский язык в области связи
	Правовые основы инженерной деятельности

	Основы системы менеджмента качества
	Технологии информационной поддержки изделия
	Отраслевые стандарты и стандарты организации в области разработки и создания квантово-оптических систем
	Основы эргономики
	Языки программирования и способы разработки встроенного программного обеспечения
	Правила информационной безопасности при работе с оборудованием квантовых коммуникаций
	Требования нормативных правовых актов по защите, охраняемой законом тайны
	Основные возможности текстовых, табличных и графических редакторов и программного обеспечения, применяемого при разработке, редактировании, экспертизе, согласовании и утверждении документов
	Основные права и обязанности работника и работодателя в соответствии с трудовым законодательством Российской Федерации
	Общие требования охраны труда, противопожарной защиты и экологической безопасности
Другие характеристики	Языки программирования: - языки системного программирования, используемые для разработки встроенного программного обеспечения, - языки описания аппаратуры интегральных схем, - языки описания аппаратуры, - библиотеки для научных и инженерных расчетов

Контрольные вопросы

1. Какая основная цель вида профессиональной деятельности для специалиста профстандарта 06.050?
2. Когда и кем утверждены и введены в действие профстандарты 06.050 и 06.054?
3. Какие кодовые группы специалистов предусмотрены профстандартом 06.050?
4. Чем отличаются требования уровня квалификации в кодовых группах А, В, С, D, E?
5. К каким кодовым группам профстандарта 06.050 относятся выпускники бакалавриата 11.03.02?
6. Какие знания должны иметь специалисты кодовой группы E для занятия соответствующей должности?
7. Для чего разработан профстандарт 06.054?
8. С какой деятельностью связаны обязанности специалиста кодовой группы D профстандарта 06.054?
9. В каких кодовых группах профстандарта 06.054 требуется образование уровня специалитета и/или магистратуры?
10. В чём должна заключаться деятельность специалиста кодовой группы G профстандарта 06.054?

Заключение

Представленный сборно-обзорный лекционный материал дисциплины «Оптические сети и квантовые коммуникации» является первым шагом для ознакомления начинающих специалистов современных телекоммуникаций с новыми направлениями развития техники оптической связи. Это развитие обусловлено реальными потребностями информационного общества в наращивании скоростных режимов транспортировки информации и её безопасностью на всех этапах от клиентских терминалов до центров обработки и хранения информации, от источников информации до её потребителей. Нужно пожелать будущим отраслевым специалистам не останавливаться на пути профессионального совершенствования и обретения новых знаний, умений и навыков. Пусть эта дисциплина им в чем-то поможет принять решения.

Список литературы

Основная учебная литература:

1. Ветров Ю.В. Криптографические методы защиты информации в телекоммуникационных системах: учеб. пособие / Ю.В. Ветров, С.Б. Макаров. — СПб.: Изд-во Политехн. ун-та, 2011. — 174 с.
<https://elib.spbstu.ru/dl/2889.pdf/download/2889.pdf>
2. Козубов А.В., Гайдаш А.А., Кынев С.М., Егоров В.И., Иванова А.Е., Глейм, А.В., Мирошниченко Г.П., Основы квантовой коммуникации: часть 1. — СПб: Университет ИТМО, 2019. — 85 с.
https://books.ifmo.ru/book/2328/osnovy_kvantovoy_kommunikacii_chast_1_uchebno-metodicheskoe_posobie..htm
3. Кронберг, Дмитрий Анатольевич. Квантовая криптография [Текст] : учебное пособие / Д. А. Кронберг, Ю. И. Ожигов, А. Ю. Чернявский ; Московский гос. ун-т им. М. В. Ломоносова, Фак. вычислительной математики и кибернетики. - Москва : МАКС Пресс, 2011. - 111, <https://elibrary.ru/qmwhwz>
4. Румянцев К.Е. Квантовые технологии в телекоммуникационных системах: учебник/К.Е. Румянцев; Южный федеральный университет. Ростов-на Дону; Таганрог: Издательство Южного федерального университета, 2021.-346с.
<https://elibrary.ru/qmwhwz> (доступ из библиотеки СибГУТИ)

Дополнительная учебная литература:

1. Прохоров, Александр Николаевич. Центры обработки данных : анализ, тренды, мировой опыт : корпоративное издание / Александр Прохоров, Салават Рахматуллин ; научное редактирование: Константин Королев, Игорь Дорофеев. - Москва : АльянсПринт, 2021. — 414стр. <https://www.atomic-energy.ru/books/119898>
2. Риксон, Фред Бю Коды, шифры, сигналы и тайная передача информации/Фред Б. Риксон; пер. с англ. А.Галыгина. —М.: АСТ: Астрель; Владимир: ВКТ, 2011.-656с.
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, Т.А. Шмаонова. М.: Постмаркет, 2002. 376 с.
4. Шубин В.В. Информационная безопасность волоконно-оптических систем : монография / Шубин В.В.. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2015. — 257 с. — ISBN 978-5-9515-0242-1. — Текст : электронный // IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/89874.html> . — Режим доступа: для авторизир. пользователей

Электронные ресурсы:

1. <https://rb.ru/opinion/quantum-cybersecurity/>
Производство квантово-криптографических систем защиты

2. <https://systempb.ru/catalog/zakazy/kvaks/>
Квантово-криптографическая защита оптических каналов
3. <https://sphotronics.ru/solutions/quantum-cryptography/>
Системы для квантово-оптических криптографических коммуникаций
4. <https://www.anti-malware.ru/reviews/Kvazar>
Модули шифрования «Квазар»
5. <https://infotecs.ru/resheniya/zashchita-vysokoskorostnykh-kanalov-svyazi.html>
Программно-аппаратный комплекс Vip-Net L2-10 шлюз
6. <https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf>
Innovations in Ethernet Encryption (802.1AE - MACsec) for Securing High Speed (1-100GE) WAN Deployments
7. https://t8.ru/wp-content/uploads/2022/10/Last_mile_Kogan_5G_security_part_1,2.pdf
Коган С. СЕТИ 5G: обеспечение конфиденциальности и безопасности
8. <https://quanttelecom.ru>
Защищённая квантовая коммуникация в оптических сетях
9. <https://packetlight-russia.ru/products/layer-1-encryption>
Оборудование для шифрования на уровне L1
10. Суцев И. Атаки на системы квантового распределения ключей
<https://quantum-crypto.ru> 28.08.2023.

Справочная документация, стандарты и статьи:

1. Профессиональный стандарт 06.050 Специалист по монтажу и технической эксплуатации квантовых сетей. Вступил в силу 01.03.2023 г.
2. Профессиональный стандарт 06.054 Специалист по исследованиям и разработкам в области квантовых коммуникаций. Вступил в силу 01.09.2023.
3. Национальный стандарт ГОСТ Р 70139-2022 «Центры обработки данных. Инженерная инфраструктура. Классификация».
4. Национальный стандарт ГОСТ Р 58811-2020 "Центры обработки данных. Инженерная инфраструктура. Стадии создания"
5. Национальный стандарт ГОСТ Р 58812-2020 "Центры обработки данных. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация".
6. Международный стандарт **ISO/IEC 30134** «Информационные технологии - Центры обработки данных - ключевые показатели эффективности».
7. **ANSI/TIA-942-A** Telecommunications Infrastructure Standard for Data Centers, затрагивает в основном кабельную и сетевую инфраструктуру.
7. **EN 50600-2-4** Телекоммуникационная кабельная инфраструктура ЦОД.
8. Кабельная инфраструктура и эксплуатация ЦОДов// Журнал сетевых решений. LAN, №5-6, 2015.
9. Документ SP-3-0092: (Стандарт TIA-942, редакция 7.0, февраль 2005)

10. Медь и оптика в современном ЦОДе// Журнал сетевых решений LAN, №7-8, 2016.

11. Рекомендация МСЭ-Т X.805 (10/2003) Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами

12. Supplement 76 to ITU-T G-series Recommendations (12/2021) Optical transport network security

13. ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. ПНЕТ 829— 2023. Квантовые коммуникации. Общие положения.- М.: Российский институт стандартизации, 2023.-12с.

14. ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. ПНЕТ 830— 2023. Квантовые коммуникации. Термины и определения.-М.: Российский институт стандартизации, 2023.-24с.

15. ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. ПНЕТ 831— 2023. Квантовый интернет вещей. Общие положения.-М.: Российский институт стандартизации, 2023.-12с.

16. ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. ПНЕТ 832— 2023. Квантовый интернет вещей. Термины и определения.-М.: Российский институт стандартизации, 2023.-16с.

Рекомендации МСЭ-Т:

1. Recommendation ITU-T Y.3800 (10/2019) Overview on networks supporting quantum key distribution

2. Recommendation ITU-T Y.3801 (04/2020) Functional requirements for quantum key distribution networks

3. Recommendation ITU-T Y.3802 (12/2020) Quantum key distribution networks – Functional architecture

4. Recommendation ITU-T Y.3803 (12/2020) Quantum key distribution networks – Key management

5. Recommendation ITU-T Y.3804 (09/2020) Quantum key distribution networks – Control and management

6. Recommendation ITU-T Y.3805 (12/2021) Quantum key distribution networks – Software-defined networking control

7. Recommendation ITU-T Y.3806 (09/2021) Quantum key distribution networks – Requirements for quality of service assurance

8. Recommendation ITU-T Y.3807(02/2022) Quantum key distribution networks – Quality of service parameters

9. Recommendation ITU-T Y.3808 (02/2022) Framework for integration of quantum key distribution network and secure storage network

10. Recommendation ITU-T Y.3809(02/2022) A role-based model in quantum key distribution networks deployment

11. Recommendation ITU-T Y.3810 (09/2022) Quantum key distribution network interworking – framework

12. Recommendation ITU-T Y.3811 (09/2022) Quantum key distribution networks - Functional architecture for quality of service assurance
13. Recommendation ITU-T Y.3812 (09/2022) Quantum key distribution networks – Requirements for machine learning based quality of service assurance
14. Recommendation ITU-T Y.3813 (01/2023) Quantum key distribution network interworking – Functional requirements
15. Recommendation ITU-T Y.3814 (01/2023) Quantum key distribution networks – Functional requirements and architecture for machine learning enablement
16. Recommendation ITU-T X.1702 (11/2019) Quantum noise random number generator architecture
17. Recommendation ITU-T X.1710 (10/2020) Security framework for quantum key distribution networks
18. Recommendation ITU-T X.1712 (10/2021) Security requirements and measures for quantum key distribution networks – key management
19. Recommendation ITU-T X.1714 (10/2020) Key combination and confidential key supply for quantum key distribution networks
20. Recommendation ITU-T X.1715 (07/2022) Security requirements and measures for integration of quantum key distribution network and secure storage network
21. Recommendation Y.3815 (09/2023) Quantum key distribution networks - overview of resilience
22. Recommendation Y.3816 (09/2023) Quantum key distribution networks – Functional architecture enhancement of machine learning based quality of service assurance
23. Recommendation Y.3817 (09/2023) Quantum key distribution networks interworking – Requirements of quality of service assurance
24. Recommendation Y.3818 (09/2023) Quantum key distribution networks interworking – Architecture

Владимир Григорьевич Фокин

ОПТИЧЕСКИЕ СЕТИ И КВАНТОВЫЕ КОММУНИКАЦИИ

Практикум

Редактор:

Корректор:

Подписано в печать

Формат бумаги 60×84/16, отпечатано на ризографе, шрифт №10

Изд.л., заказ №....., тираж . СибГУТИ

630102, Новосибирск, ул. Кирова 86