

Дисциплина:

Оптические сети и квантовые коммуникации

Тема занятия: Изучение способов защитного кодирования в транспортной сети OTN-OTN и реализации в оборудовании

Лабораторно-практическое занятие.

Общее время занятия 2 часа

Назначение этой работы – системные **знания** будущих специалистов

Подготовить обучающихся к восприятию технических решений по криптографической защите информационного трафика в каналах оптических транспортных сетей с высокими скоростями передачи на основе оборудования OTN/OTN различных производителей.

Цель работы, порядок выполнения и содержание работы

- Цель работы: изучить способы защиты оптических каналов от несанкционированного съёма информации физическими и криптографическими решениями на основе стандартных протоколов.
- Порядок выполнения: изучить возможности защиты соединений в пяти вариантах; преимущества криптографической защиты трафика оптических каналов; способы и средства шифрования трафика в оборудовании транспортных сетей; оборудование для шифрования отечественных и зарубежных производителей; возможные сертификационные решения для транспортных сетей связи.
- Содержание работы: изучить теоретические разделы и ответить на контрольные вопросы, решить задачу.

Содержание отчёта

- 1. Название работы. Ф.И.О. исполнителя с подписью. Руководитель занятия. Дата выполнения.
- 2. Цель занятия.
- 3. Содержание занятия с перечнем изучаемых разделов.
- 4. Краткие ответы на контрольные вопросы.
- 5. Решение задач и выводы по результатам выполнения работы.

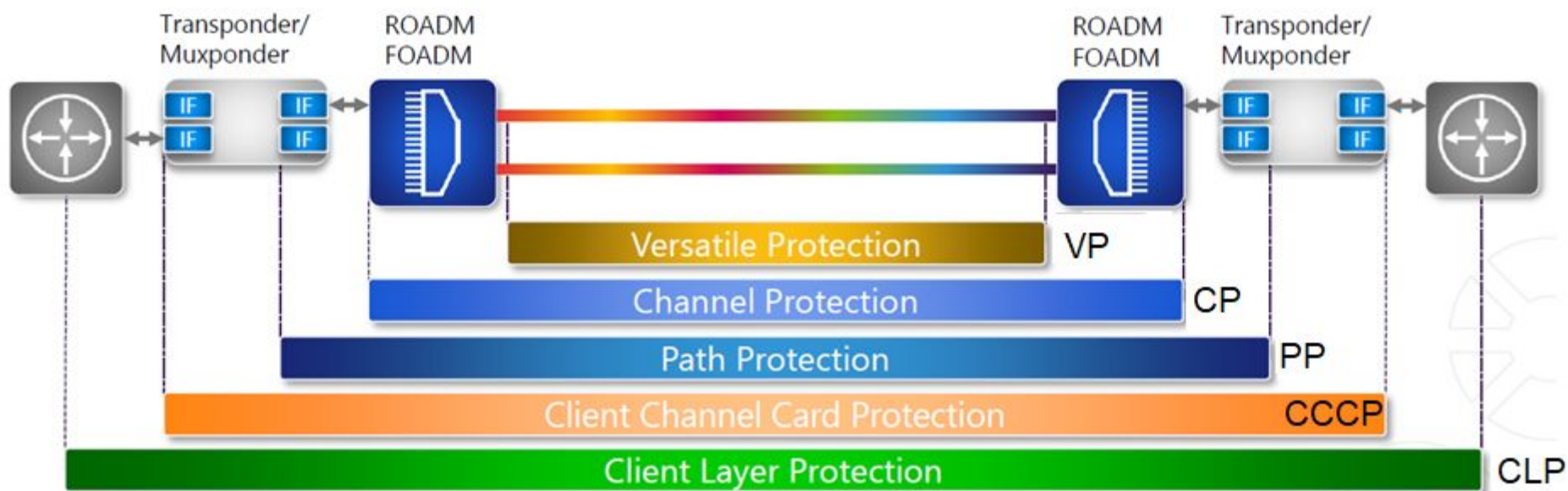
Рекомендуемая литература для самостоятельного изучения

- 1. Обзор линейки Квazar, модулей шифрования для криптографической защиты каналов связи. Источник: <https://www.anti-malware.ru/reviews/Kvazar>
- 2. Оборудование для шифрования на уровне L1 . Источник: <https://packetlight-russia.ru/products/layer-1-encryption>.
- 3. Supplement 76 to ITU-T G-series Recommendations (12/2021) Optical transport network security
- 4. ГОСТ Р 34.12– 2015 Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ Блочные шифры. М.: Стандартиформ. 2015.-25с.
- 5. ГОСТ Р 34.13 – 2015 Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Режимы работы блочных шифров.- М.: Стандартиформ. 2016.- 30с.
- 6. Соболев М.А.. СРАВНИТЕЛЬНЫЙ АНАЛИЗ РОССИЙСКОГО СТАНДАРТА ШИФРОВАНИЯ ПО ГОСТ Р 34.12–2015 И АМЕРИКАНСКОГО СТАНДАРТА ШИФРОВАНИЯ AES // Политехнический молодежный журнал. 2022. № 04
- 7. Каталог продукции компании Т8. <https://t8.ru>
- 8. <https://skzi.ru> Каталог продукции средств криптографической защиты информации (СКЗИ) [МШ-TPfc](#) [МШ-MUXs](#) [ВМШ-TP-1U](#) [ВМШ-MUXfc-1U](#) [АРМ ИКД](#) [Совместимость оборудов](#)

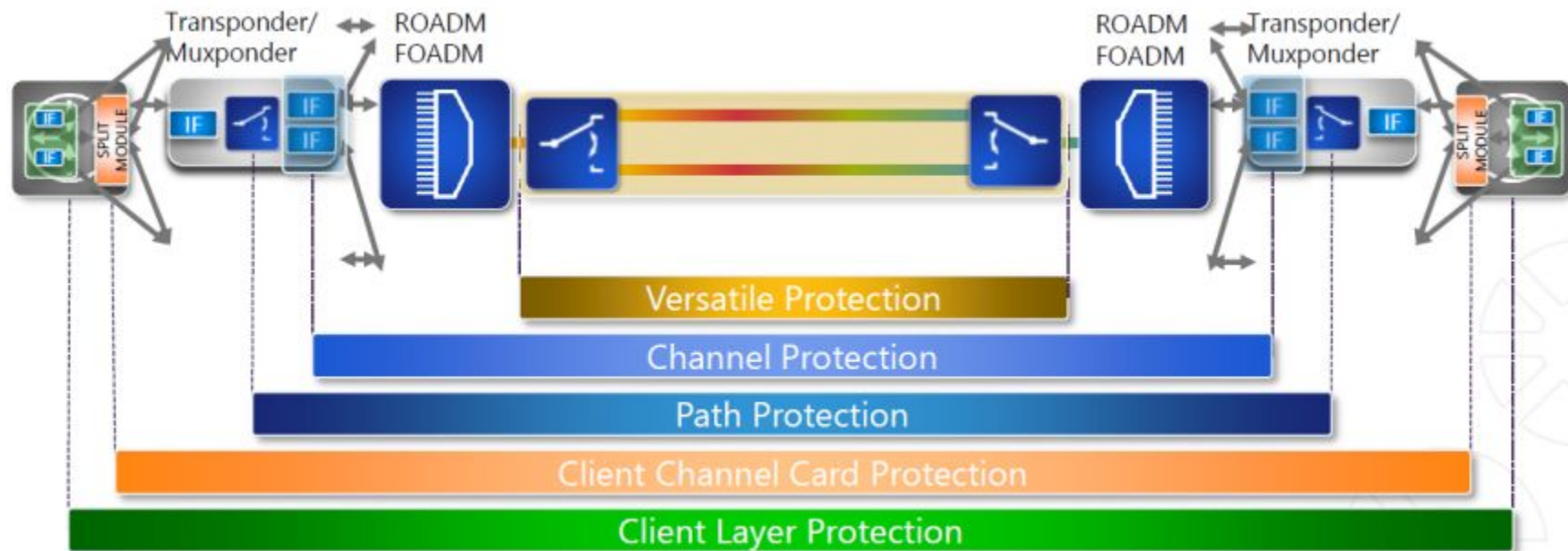
Уровни защиты соединений и информационной нагрузки (трафика) транспортной сети и сети доступа

- Защита может быть реализована на любом из четырёх уровней оптической сети (согласно модели ISO/OSI):
- **Сетевой уровень, маршрутизация**
- • Layer 3: IP/MPLS: IP Fast Reroute (FRR) (link, path, and node) and equivalent MPLS FRR (изменение маршрутов виртуальных соединений). *Криптографическая защита соединений VPN (виртуальных частных сетей)*
- **Канальный уровень пакетной сети**
- • Layer 2: Carrier Ethernet: G.8032
- • Layer 2: MPLS-TP: 1:1 LSP protection (коммутация виртуальных соединений в сетях любых конфигураций). *Криптографическая защита соединений VPN*
- **Физический уровень оптической сети**
- • Layer 1: OTN: Subnetwork Connection Protection (SNCP/I and SNCP/N), 1+1 and 1:N (**цифровая коммутация ODUk, ODUCn в линейных и кольцевых сетях**)
- **+ криптографическая защита соединения на скоростях 10/100 Гбит/с и квантово-криптографическая защита соединения (применение квантового распределения ключей)**
- **Физический уровень сети синхронной цифровой иерархии**
- • Layer 1: SONET/SDH: 1+1 APS/MSP, 1+1 UPSR/SNCP, 2F-BLSR/MS-SPRING (**цифровая коммутация VC-3/4, VC-12 в линейных и кольцевых сетях**). *Криптографическая защита соединений SDH*
- **Оптический уровень сети**
- • Layer 0 (WDM): Y-cable at transponder and muxponder level (**оптическая коммутация волновых каналов в ROADМ, ОХС и транспондерах/мукспондерах**), квантовая оптическая сеть

Варианты защиты соединений и клиентского трафика в оптической сети: универсальная гибкая двухсторонняя защита VP; канальная защита CP; защита тракта (PP); защита канальной карты клиента (CCCP); защита на уровне клиента (CLP)



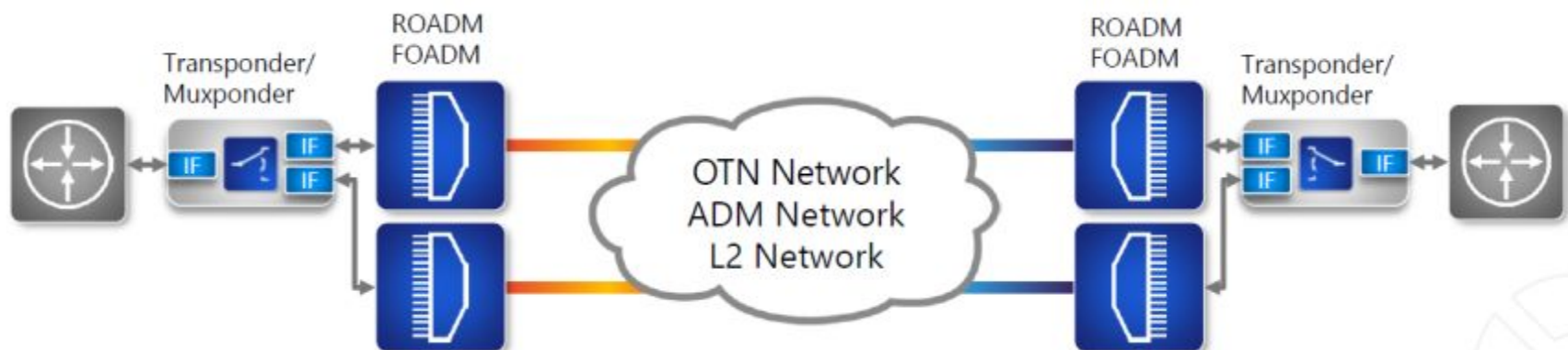
Защита волоконно-оптической линии (переключение волокон) VP. Время коммутации до 15мс



Защита оптического канала с коммутацией в транспондере CP



Защита маршрута с коммутацией на уровне ODUk, L2 Ethernet и т.д. PP



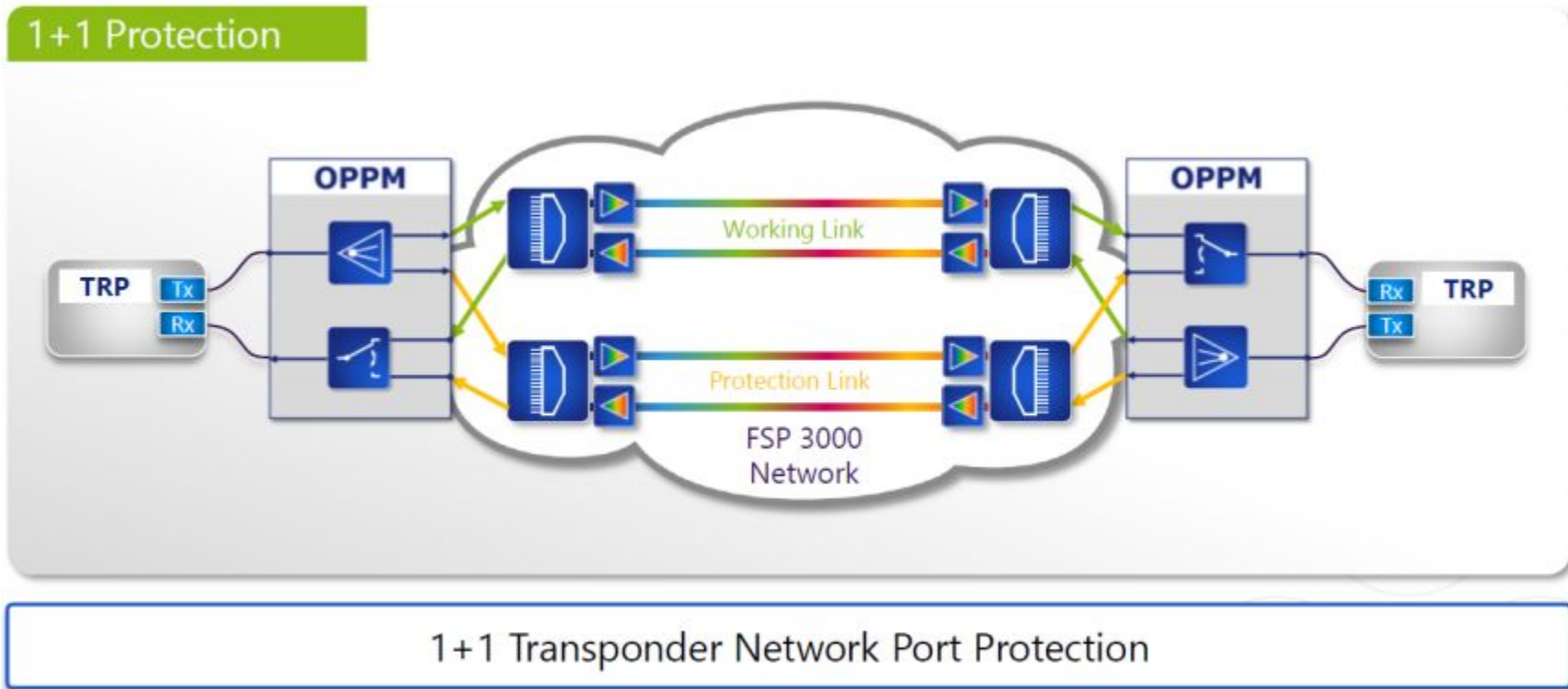
Защита карты клиента (интерфейса) с использованием двух транспондерных блоков СССР



Защита на уровне оборудования клиента CLP

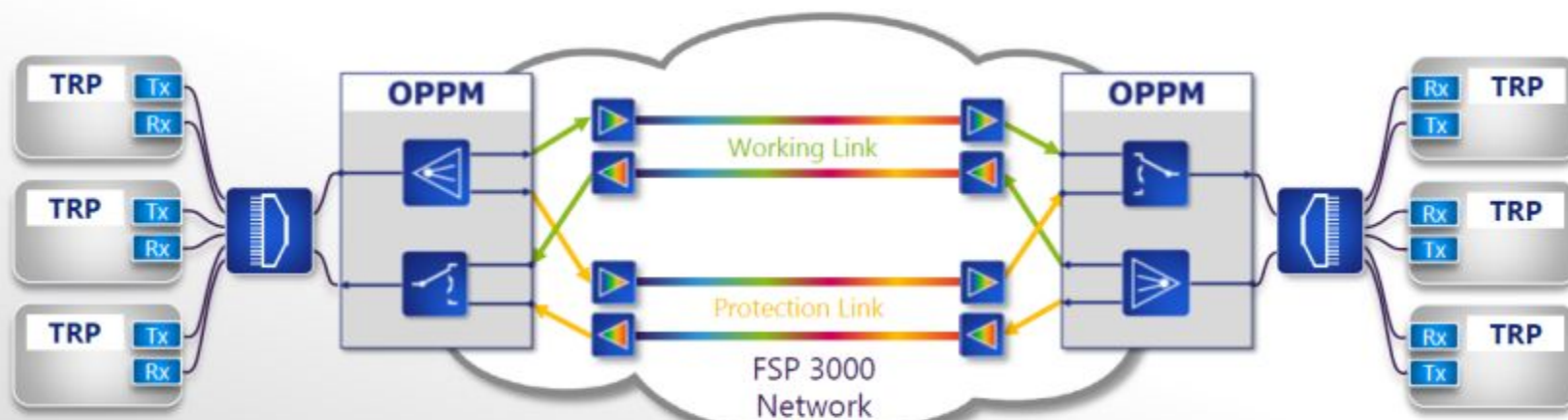


Защита оптического канала уровня транспондера с использованием отдельного блока коммутации OPPM (Optical Port Protection Module)



Защита оптических соединений блоком OPPM

1+1 Protection

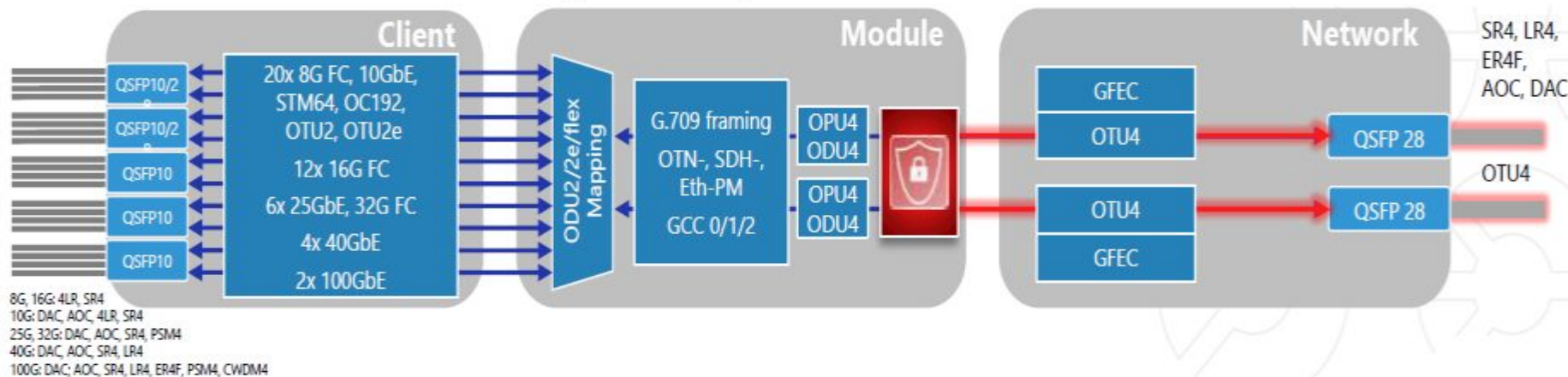


Криптографическая защита в модулях транспондеров и мукспондеров оптических каналов транспортной сети

Интерфейсы клиентов транспортной сети

Транспондеры и мукспондеры с шифрованием в модульном исполнении

Сетевые интерфейсы для линий различной протяженности



Преимущества использования шифрования данных в каналах оптической транспортной сети OTN/OTH (ODU2, 4) для нагрузки со скоростью 10 Гбит/с и 100 Гбит/с в поле OPU2, OPU4

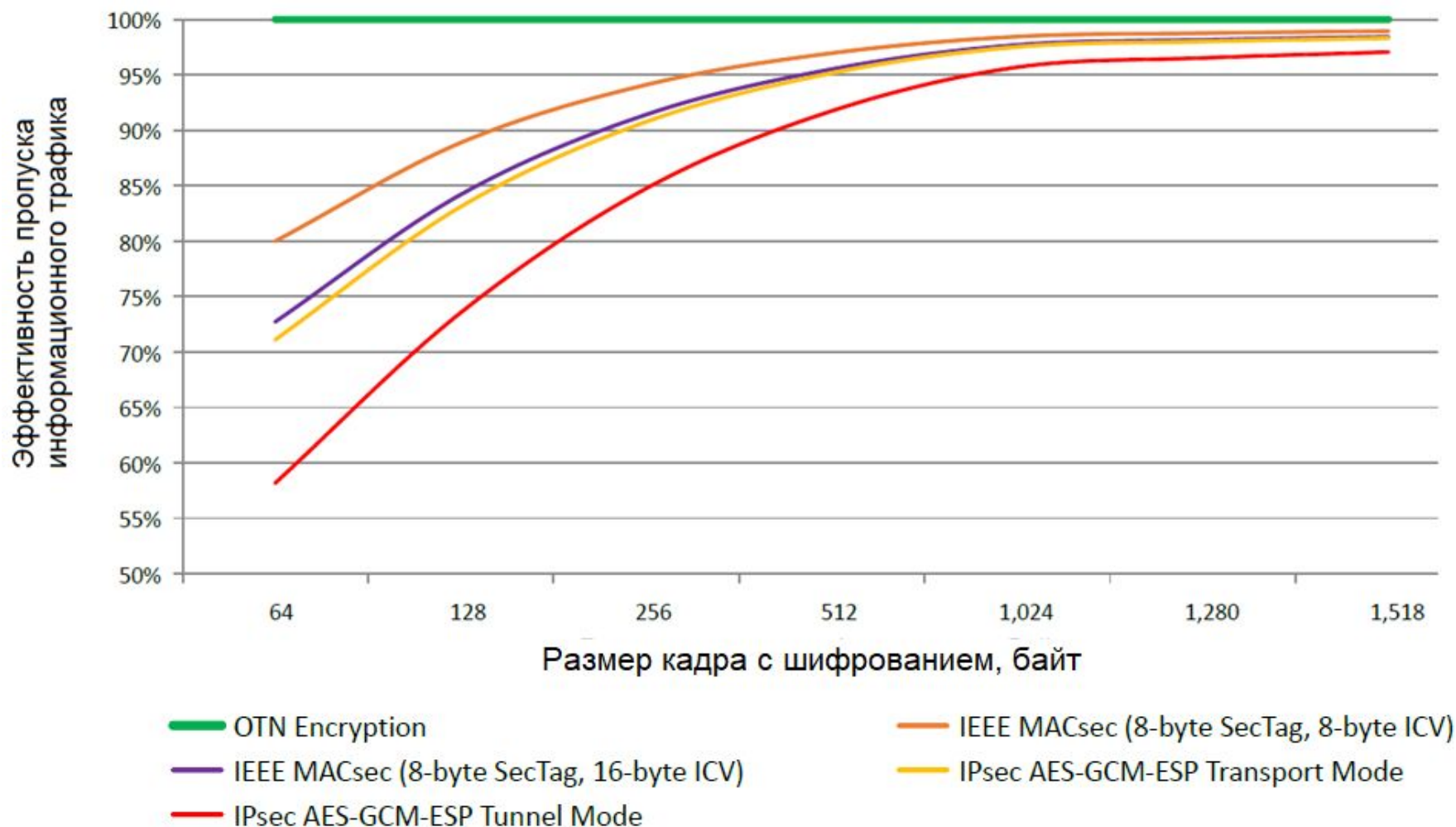
Шифрование	IP sec	MAC sec	ODU sec
Уровень	Уровень 3 (IP)	Уровень 2 (Eth)	Уровень 1 (OTN)
Высокая производительность и низкая цена	✗	✓	✓
Малое время ожидания	✗	✓	✓
Заголовок протокола	Большой	Малый	Нет
Мультипротокольность	✗	✗	✓

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)

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



Преимущества использования шифрования данных в каналах оптической транспортной сети OTN Encryption

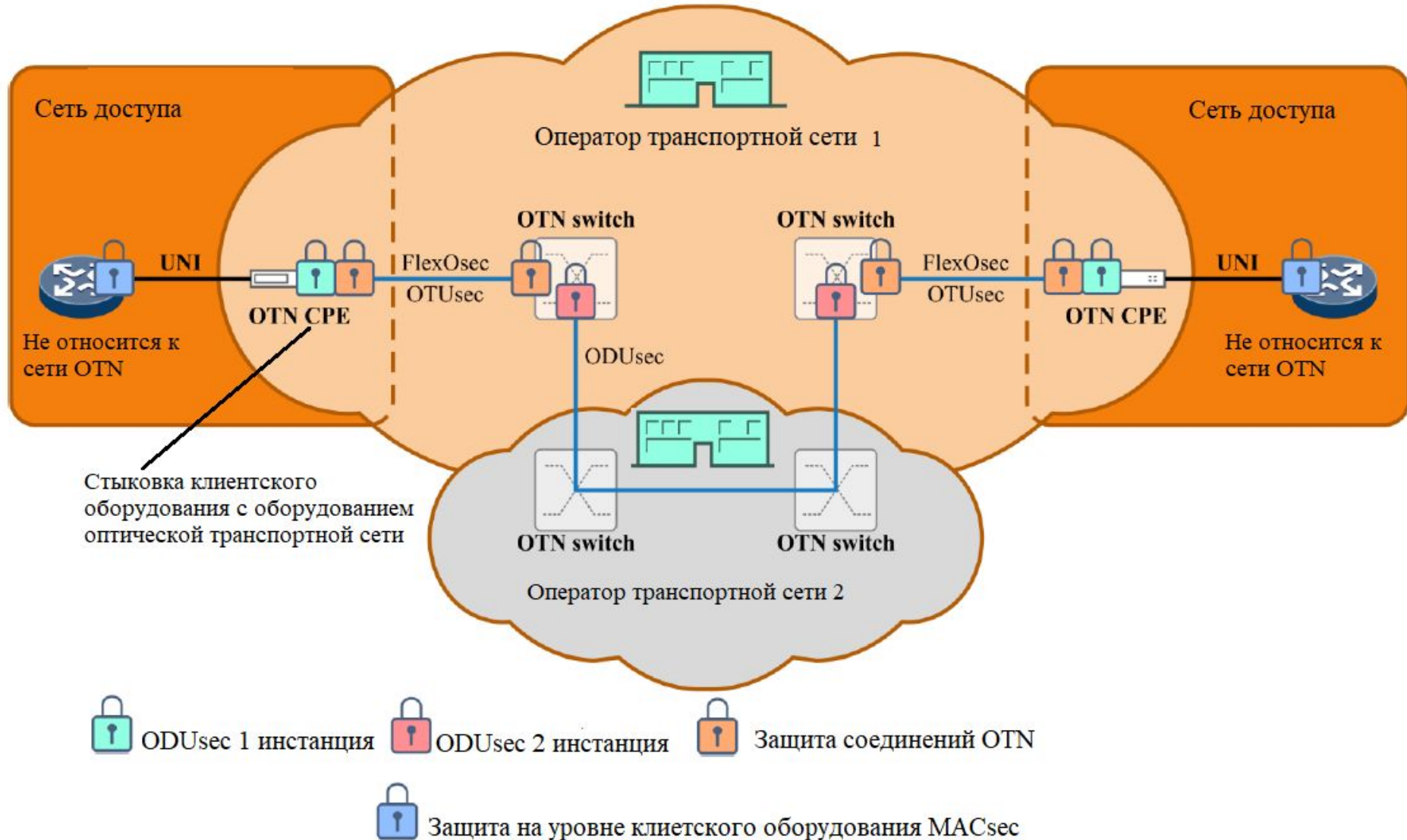
- В мире для защиты оптических каналов уже давно применяются устройства класса L1 Services Encryption. Перемещение криптографической защиты с уровней L2 / L3 на более низкий уровень L1 приводит к предельно малому влиянию функциональности информационной безопасности на ИТ-сервисы. Для передачи данных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

Обзор шифрования в оптических каналах OTN/OTH

В рекомендации МСЭ-Т Sup.76 (12/2021) по защите оптических транспортных сетей OTN/OTH 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.1). 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 $n \times \text{FlexOsec}$ и в отдельном блоке ODUsec ODUk ($k=2, 4$) (рис.2).

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.3). 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).

Зоны применения криптографической защиты Layer-1 (OTU/ODUsec) для сетей OTN/OTH (рис.1)



Варианты мультиплексирования информационной нагрузки клиента в защищаемый оптический канал сети OTN/OTN по рек. G.709.1 (рис.2)

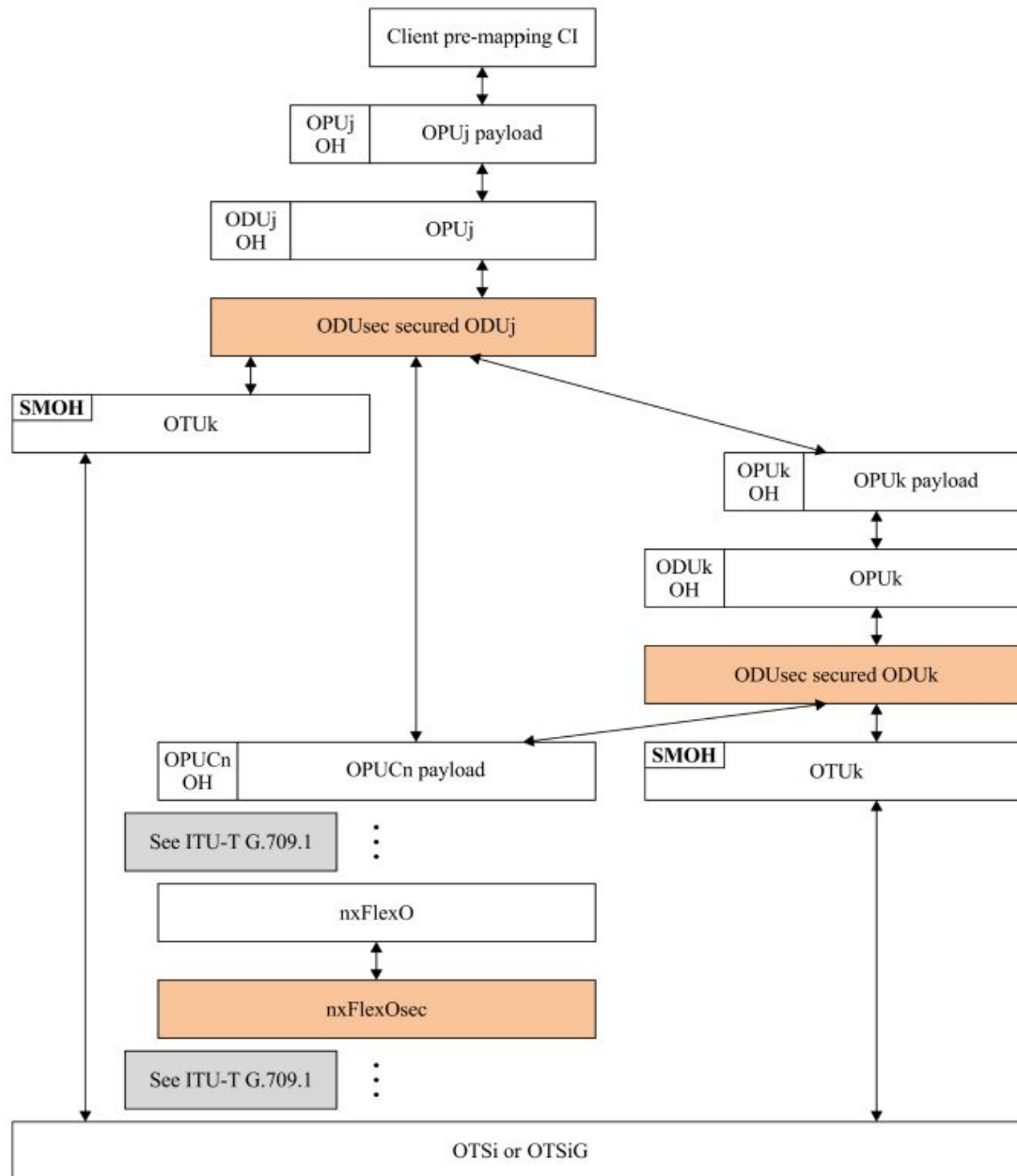
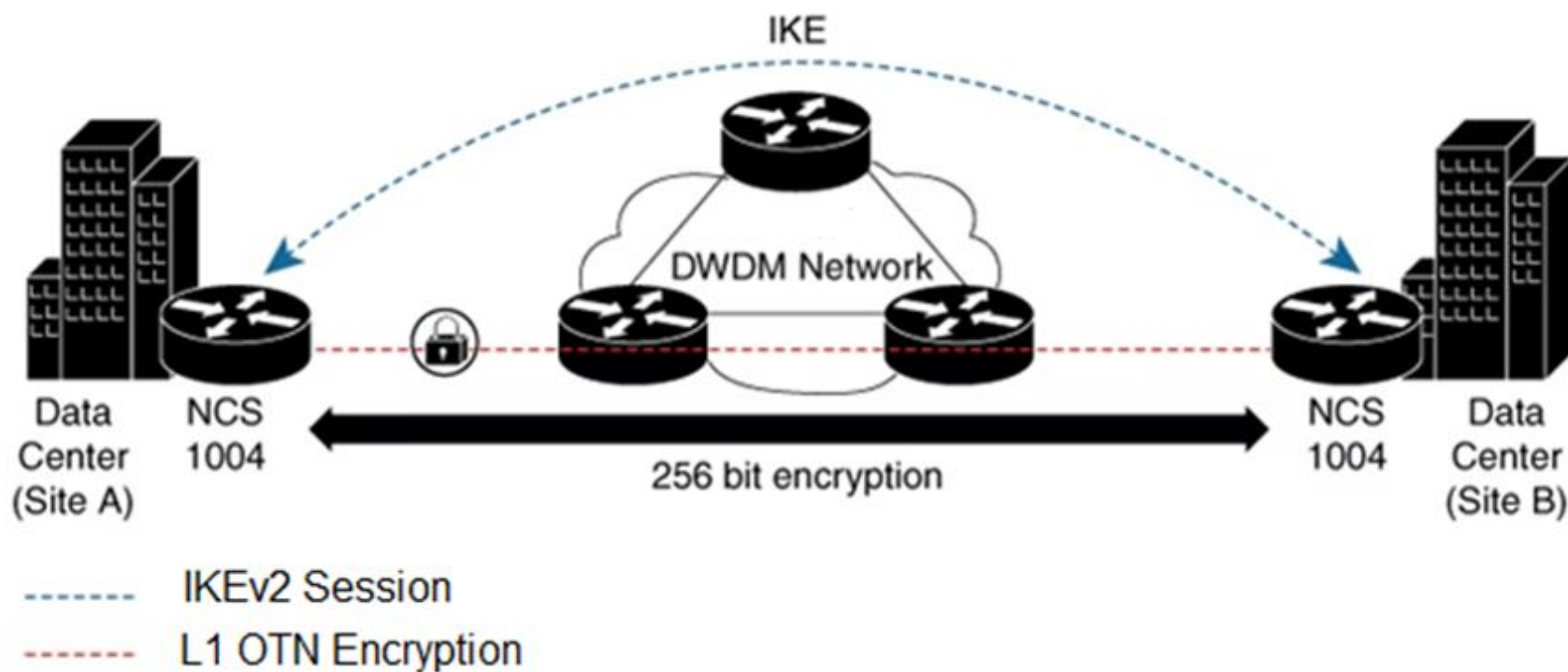
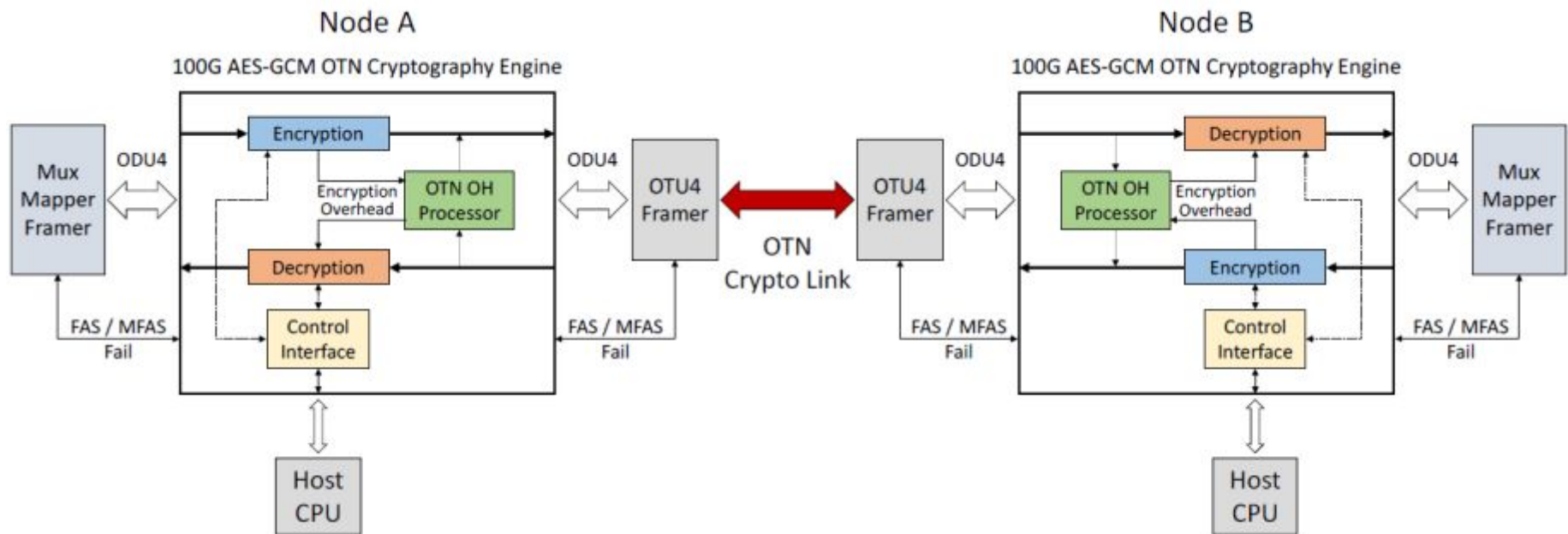


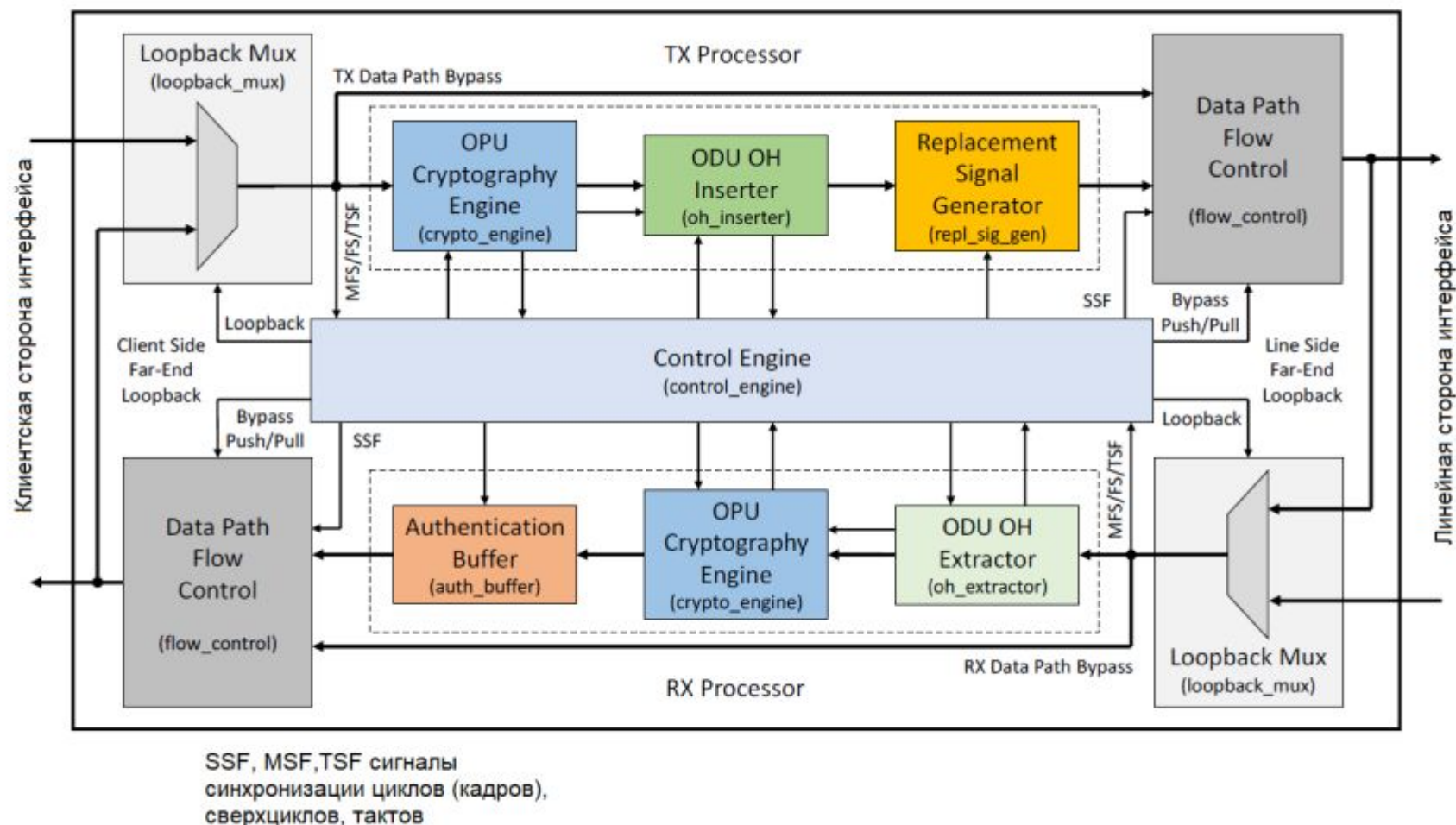
Схема взаимодействия по обмену ключами шифрования IKEv2 в канале оптической сети с оборудованием NCS 1004 (Cisco) (рис.3)



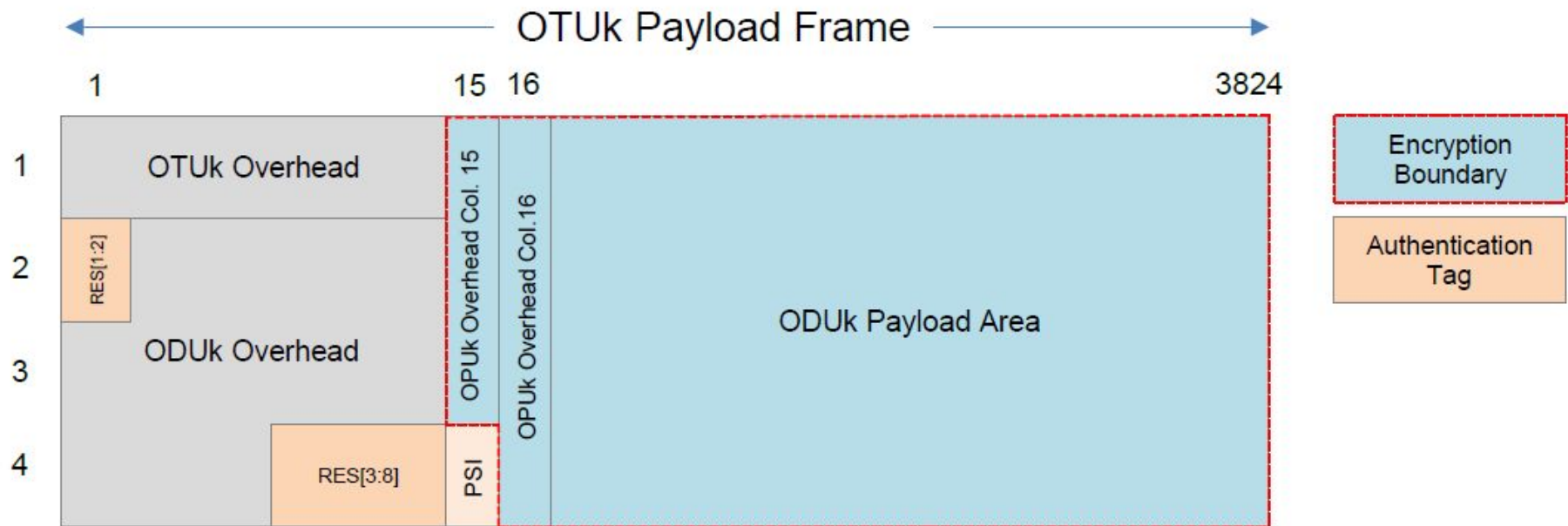
Типовая блок-схема с криптографической защитой оптического канала на уровне OTU4 100 Гбит/с AES-GCM



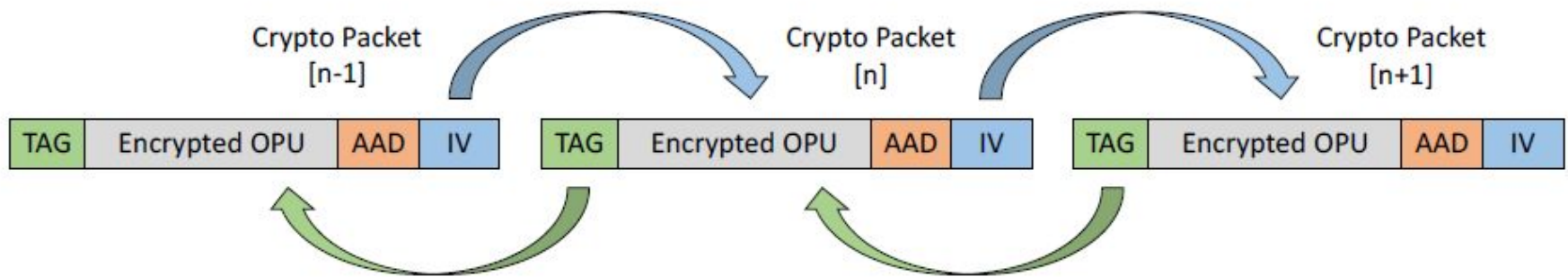
Структура функционального блока шифрования (микросхемы шифрования)



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 рисунке



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

Назначение полей криптопакета

- 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 2^{32} и умноженное на 64, при криптопериоде 4,672мкс, т.е. длительность использования сессии шифрования 14,86 дней. Реально такой период не требуется.

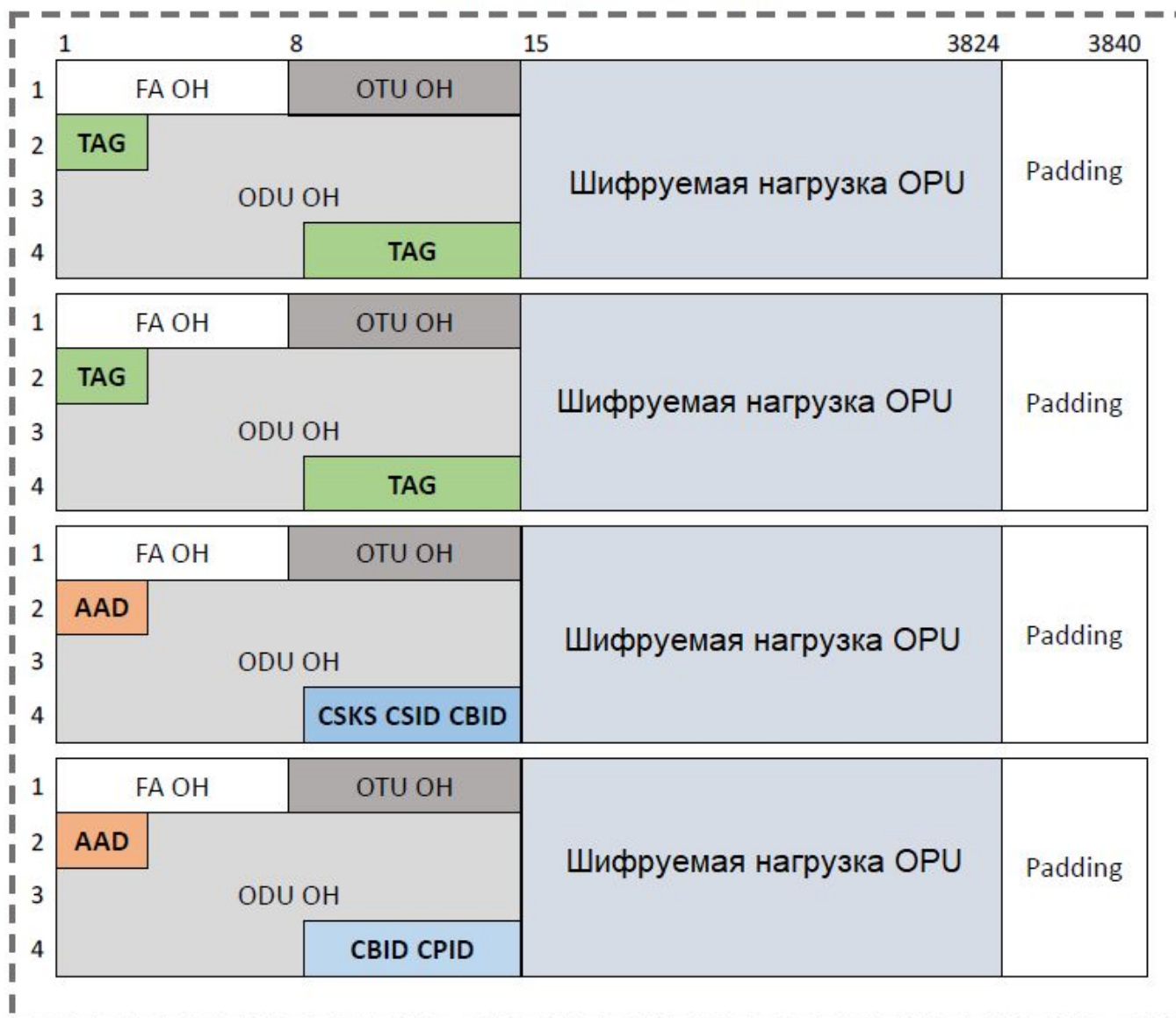
Образование криптопакета с его опознанием происходит в четырёх кадрах по сверхциклам (индикация MFAS в заголовке OTUk) на позициях байт, ранее зарезервированных (RES) в заголовке ODUk

	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							

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

Структура криптопакета для оптического канала на основе блоков OTU2/4

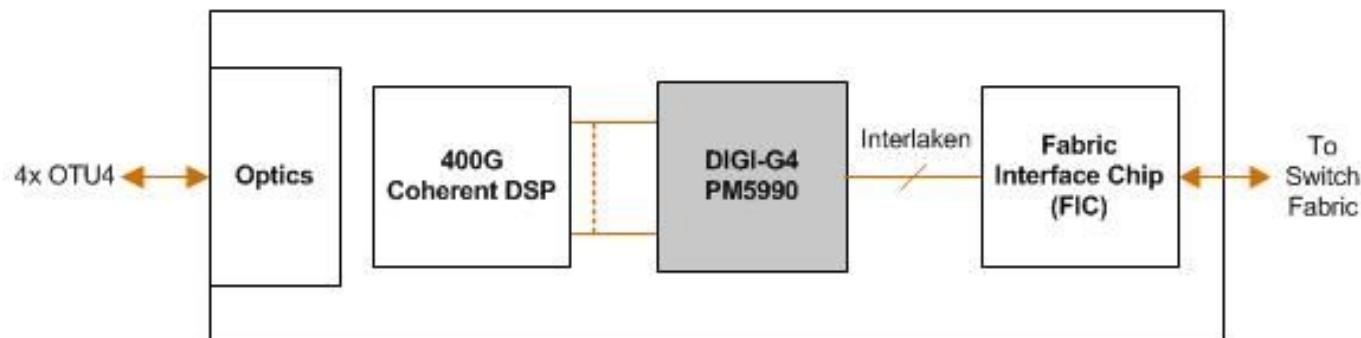
Криптопакет с метками



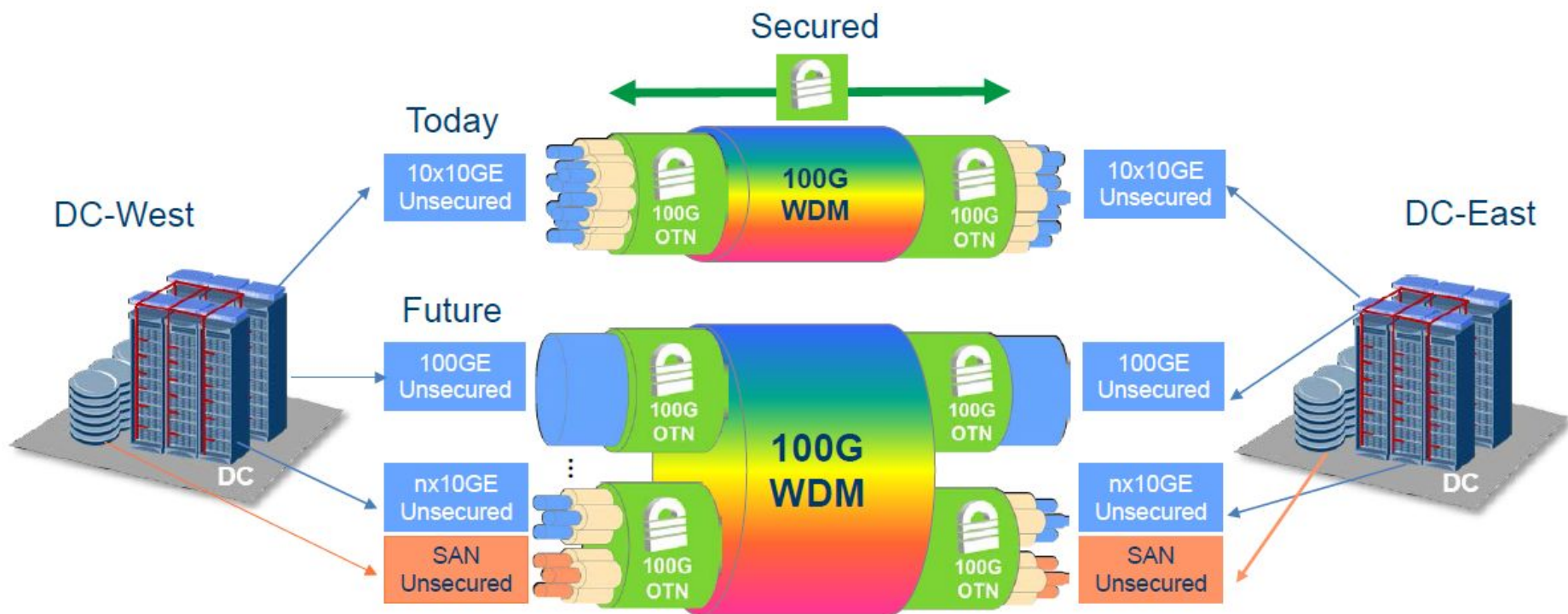
Реализация защиты микромодулем - PM5990 DIGI-G4 в блоках OTU4 для канала на скорости 400Гбит/с (<https://www.microsemi.com>)

- DIGI-G4 is Microsemi's fourth-generation OTN processing solution for next-generation OTN switching and packet-optical transport (POTP/P-OTN), WDM/ROADM, and hyperscale data center interconnect (DCI) equipment. Building on the innovations in Microsemi's DIGI-120G, which is widely deployed in service provider and hyperscale data center WAN networks today, DIGI-G4 is a 4x100G multi-service OTN processor, scaling line card capacity by 4x, while reducing power per port by 50 percent, as compared to previous generation OTN processors.
- DIGI-G4 addresses the requirements of SDN-ready, encrypted optical transport infrastructure. Reusing Microsemi's proven, service provider-qualified DIGI family OTN switching software development kit (SDK), DIGI-G4 can be leveraged across multiple applications and equipment platforms, providing OEMs with the lowest risk, fastest time-to-market and lowest cost of development.
- High-density 400G single-chip line card solution for OTN switching on P-OTP/P-OTNs
- Sub-wavelength Layer 1 OTN encryption solution to secure the cloud Supports 2nd-generation AES-256 OTN encryption Enables sub-wavelength ODUk encryption
- 25G granularity flexible OTN framer to DSP
- High density 10G, 40G and 100G multi-service support, including Ethernet, storage, IP/MPLS and SONET/SDH
- Transport SDN-ready features, enabling OpenFlow extensions such as network element neighbor discovery

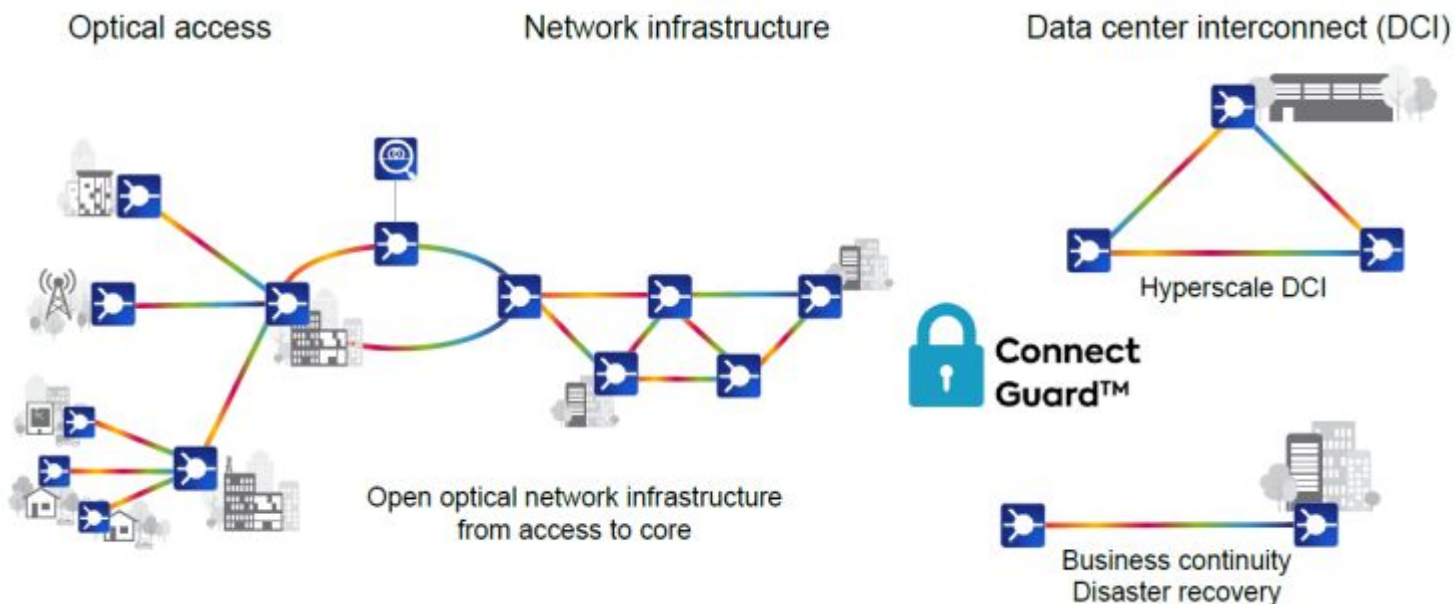
Single-Chip 400G OTN Line Card



Зона применения шифрования криптопакетами (соединение датацентров DC или ЦОД)



Физическое исполнение модуля шифрования и сетевое применение:
WCC-PCN-AES100GB-G is a WDM transponder for the transport of encrypted 100GbE and OTU4 client services over optical networks



Protection switching

- 1+1 unidirectional revertive and non-revertive switching
- Switching times < 50ms
- Automatic protection switching (APS) channel per sub-aggregate service for client channel card protection

Encryption

- Encryption of payload according to AES-GCM with 256bit key
- Diffie-Hellman 4096 key exchange every minute
- Protection against modification
- Far-end authentication

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 каналобразующим 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 каналобразующим 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.

Криптографическая защита оптических каналов связи уровня

L1. Модули «Квазар» в оптической транспортной сети

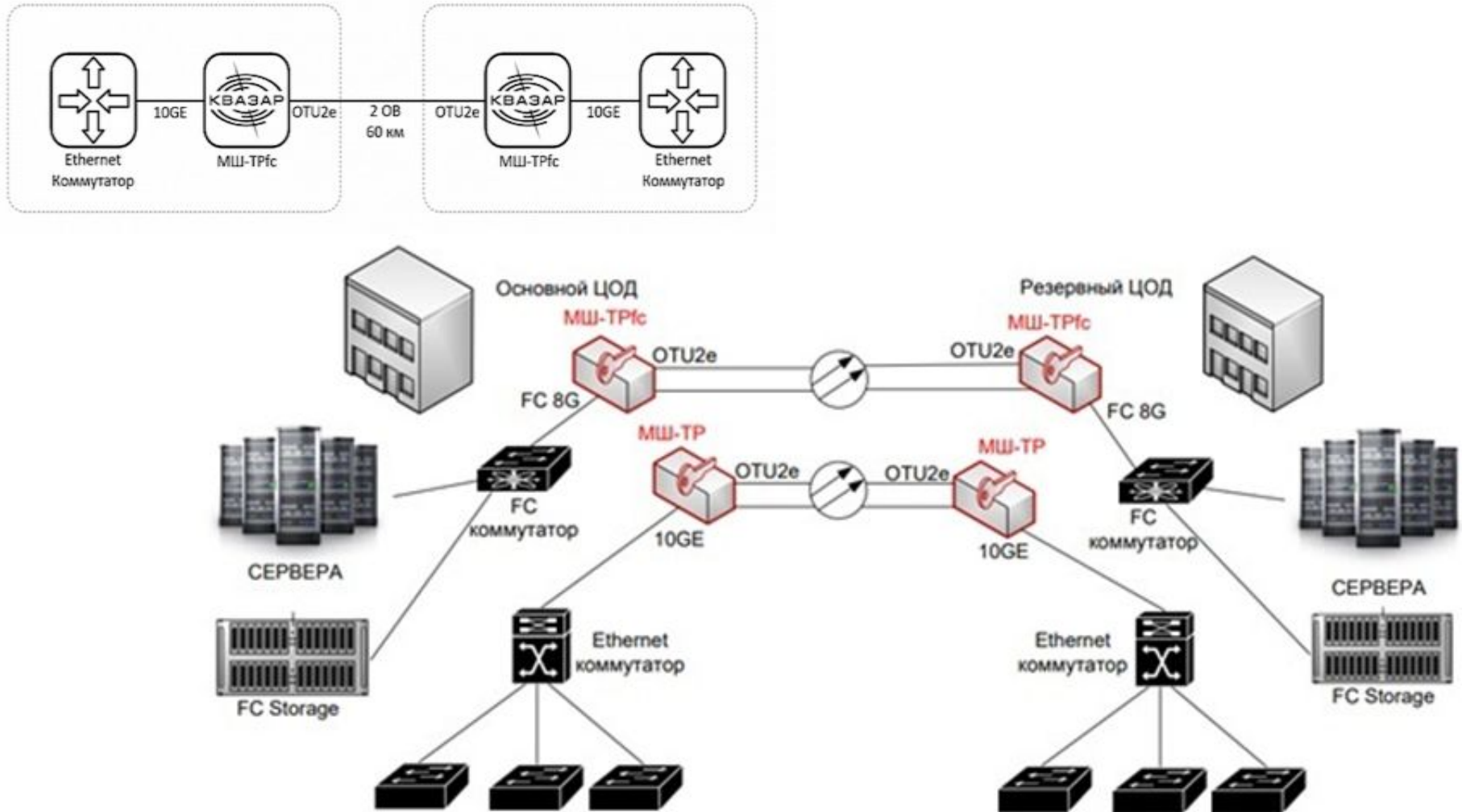
- **Технические характеристики модуля Квазар**
- Канал: оптика, OTN с форматом кадра OTU2 (10 Гбит/с)/OTU4 (100 Гбит/с).
- Клиент: оптика 10Gbit Ethernet или 8x1Gbit Ethernet.
- Производительность шифрования 10/100 Гбит/с.
- Алгоритм шифрования: ГОСТ Р34.12-2015 (Магма или Кузнечик). Шифр имеет 128-битный 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-TRfc и МШ-TRfc-1U (транспондеры), МШ-MUXs и МШ-MUXs-1U (агрегирующие транспондеры), обеспечивает криптоимитозащиту и преобразование клиентского потока информации по интерфейсам 10 Gbit Ethernet или 8 Gbit Fibre Channel;
- СКЗИ «Квазар-100» — модули шифрования ВМШ-TR-1U для организации защиты высокоскоростного канала 100 Гбит/с.

Линейка оборудования «Квазар»

- 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.
- **«Квазар» защищает весь направляемый в транспортную сеть трафик.**
- Линейка «Квазар» включает в себя:
- СКЗИ «Квазар» — модули шифрования МШ-TRfc и МШ-TRfc-1U (транспондеры), МШ-MUXs и МШ-MUXs-1U (агрегирующие транспондеры);
- СКЗИ «Квазар-100» — модули шифрования ВМШ-TR-1U для организации защиты высокоскоростного канала 100 Гбит/с;
- **СКЗИ «Квазар-СКР» — модули шифрования с квантовой криптографической системой выработки и распределения ключей МШ-TR-СКР;**
- СКЗИ «Квазар-Э» — экспортные варианты модулей шифрования МШ-TRfc-1U и МШ-MUXs-1U.

Совместимость модулей «Квазар»

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.



Пример оборудования. Внешний вид модуля шифрования МШ-TRfc-1U

Модуль шифрования МШ-MUXs — агрегирующий транспондер (мукспондер), выполненный на основе платы с установленными на ней лицевой панелью и верхней защитной крышкой. Представляет собой вставной блок, устанавливаемый в специализированное шасси. Здесь также возможны два варианта исполнения — с боковым и фронтальным обдувом. Обеспечивает криптоимитозащиту и преобразование клиентского потока информации по интерфейсам 8x1Gbit Ethernet либо 8xSTM-1 / 8xSTM-4 / 4xSTM-16.

Источник: <https://www.anti-malware.ru/reviews/Kvazar>



ЗАЩИТА КАНАЛОВ

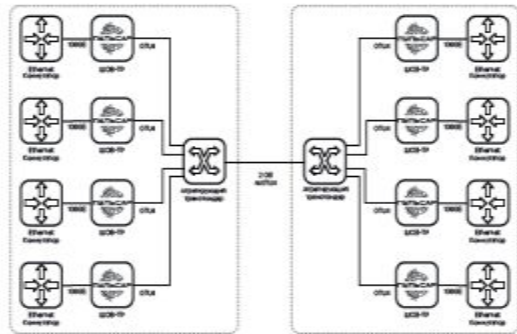
100GE БЕЗ ПРИМЕНЕНИЯ WDM
БЕЗ РЕЗЕРВИРОВАНИЯ



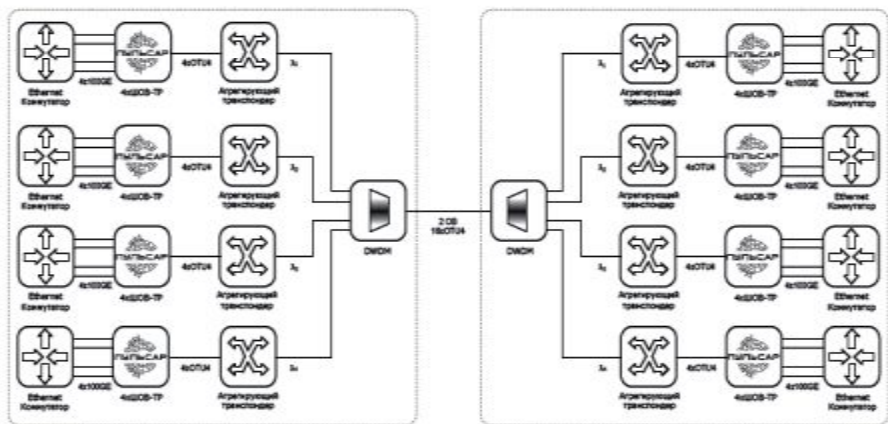
Данное решение позволяет защитить один оптический канал со скоростью до 100 Гбит/с с типом сервиса 100GE по одной паре волокон

Данное решение позволяет защитить четыре оптических канала со скоростью до 100 Гбит/с с типом сервиса 100GE по одной длине волны (λ) или по одной паре волокон с применением активного мультиплексирования сигнала

4x100GE ПО ПАРЕ ВОЛОКОН С ПРИМЕНЕНИЕМ
АКТИВНОГО МУЛЬТИПЛЕКСИРОВАНИЯ СИГНАЛА



16x100GE ПО ПАРЕ ВОЛОКОН С ПРИМЕНЕНИЕМ АКТИВНОГО И ПАССИВНОГО МУЛЬТИПЛЕКСИРОВАНИЯ СИГНАЛА




Данное решение позволяет защитить 16 и более оптических каналов со скоростью до 100 Гбит/с с типом сервиса 100GE по одной паре волокон с применением активного и пассивного мультиплексирования сигнала

В состав комплекса «Пульсар» помимо шифраторов оптических высокоскоростных (ШОВ) входит Центр Управления Сетью, состоящий из серверной и клиентской компонент. Серверная компонента (сервер ЦУС) — обеспечивает постоянный мониторинг ШОВ. Клиентская компонента (АРМ ЦУС) — рабочее место оператора для мониторинга и управления сетью ШОВ. Также на АРМ ЦУС производится формирование и запись первичных ключевых документов для ввода ШОВ в эксплуатацию.

ПОДРОБНЕЕ





Блок шифрования ШОВ-ТР

из состава комплекса средств криптографической защиты
конфиденциальной информации «Пульсар»

МОНОБЛОК 2U ДЛЯ УСТАНОВКИ В СТОЙКУ 19"



ПРЕИМУЩЕСТВА

- Шифрование на скорости линии 100 Гбит/с
- Минимальное влияние на характеристики сети передачи данных и сервисы
- Передача данных без изменения их исходной структуры и административной информации
- Поддержка мультисервисных сетей
- Быстрое внедрение без влияния на сетевую топологию (Transparent mode)
- Работа по «тёмному волокну» и с активным оборудованием DWDM различных производителей
- Самостоятельная генерация и удалённая смена ключей (в составе комплекса)
- Широкие возможности масштабирования

ХАРАКТЕРИСТИКИ

Клиентские интерфейсы	1x100Gbit Ethernet
Линейные интерфейсы	1xOTU-4
Производительность	100 Гбит/с
Задержка (Latency), мс	0,00043
Класс СКЗИ	КСЗ
Криптографический алгоритм	ГОСТ Р 34.12-2015 (блочный шифр «Кузнечик»)
Режим шифрования	ГОСТ Р 34.13-2015 (режим гаммирования)
Режим выработки имитовставки	ГОСТ Р 34.13-2015
Дистанционное управление	Средствами АРМ-ЦУС, Веб-интерфейс с сервера ЦУС (только для мониторинга сети)
Сертификаты ФСБ	3 кв. 2022 года

Схема подключения модулей «Квазар» в сеть с DWDM

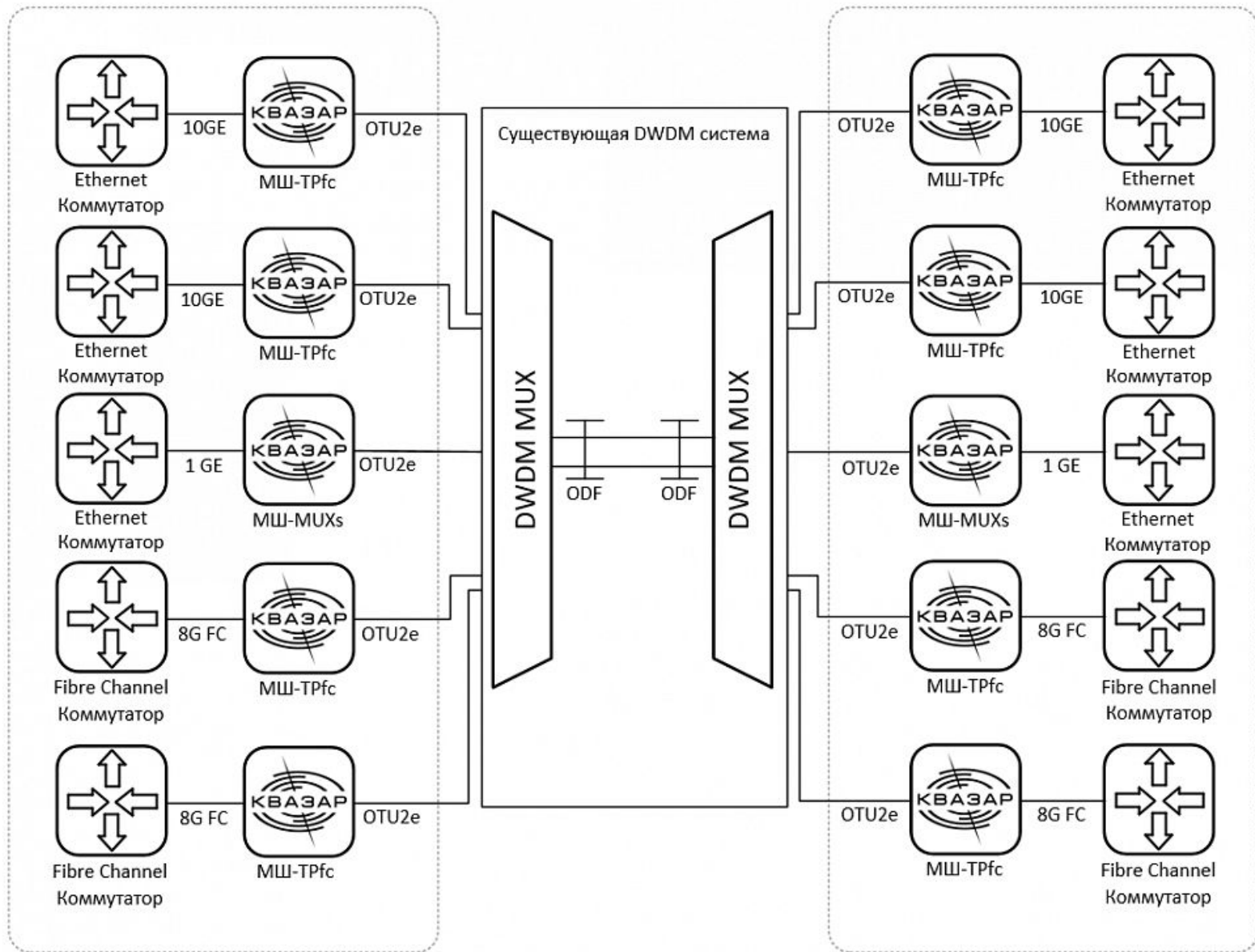
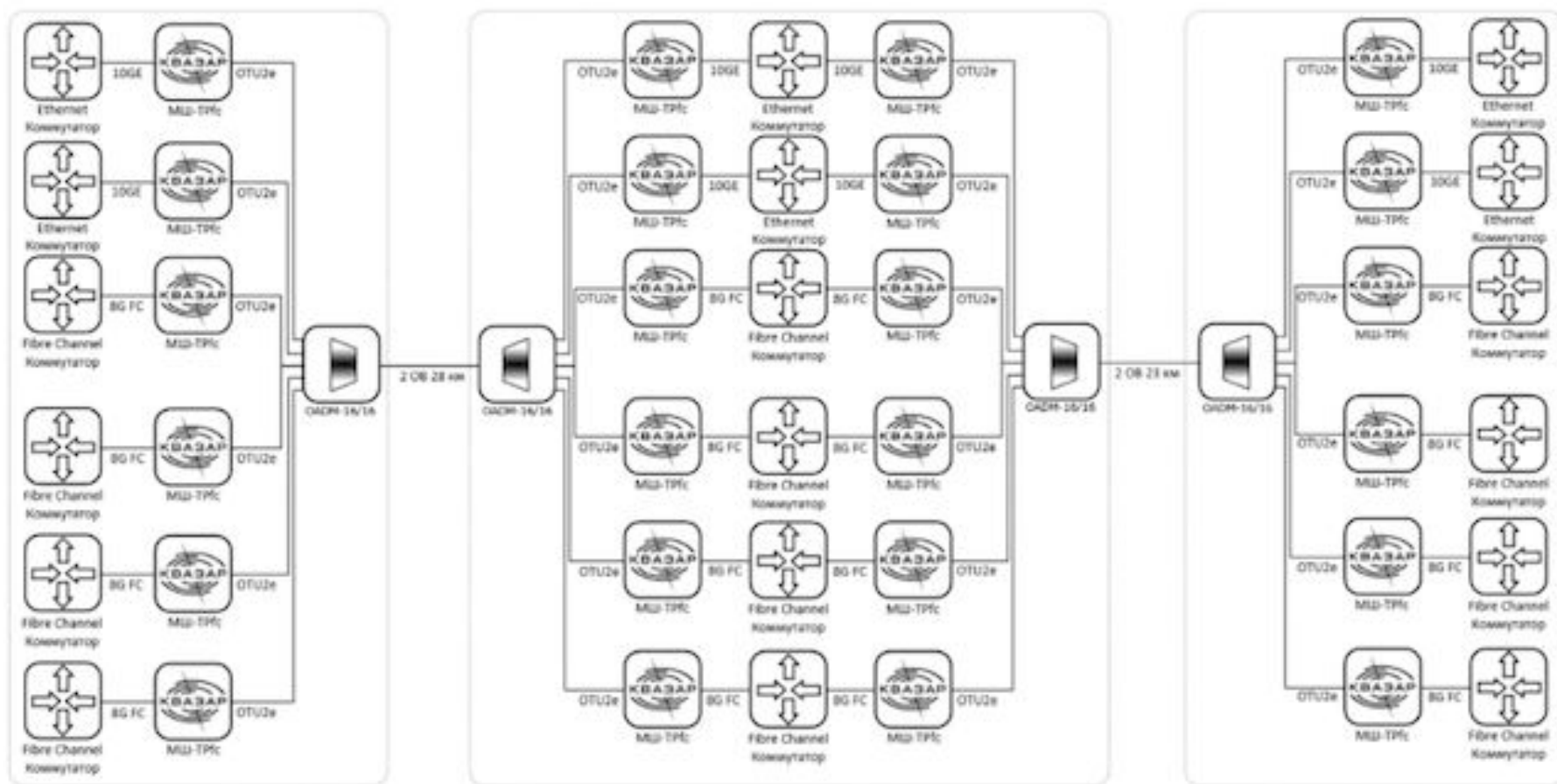


Схема защиты DWDM-решения для сетей 10G, 1G и 8GFC

Источник: <https://www.anti-malware.ru/reviews/Kvazar>



Выводы по возможностям модулей «Квазар»

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). 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 (потокное 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.

Оборудование зарубежных производителей с функцией криптозащиты трафика

- **Компания PacketLight** предлагает решения оптического шифрования данных уровня Layer-1 для сетей DWDM, OTN и тёмного волокна без снижения пропускной способности всех каналов.
- Решение обеспечивает конфиденциальность и целостность передаваемых данных, основанных на стандартах шифрования GCM-AES-256, поддерживая обмен ключами Диффи-Хеллмана (DH) с периодичностью до 1 минуты. Это решение поддерживает передачу данных GbE, 10/40/100Gb Ethernet и 4/8/16/32G FC для таких задач, как защищённое подключение центров обработки данных для финансового сектора, шифрование сервисов для операторов связи, создание защищенных сетей для государственных учреждений и коммерческих компаний.
- <https://packetlight-russia.ru/products/layer-1-encryption>
- **Компания Gemalto**, мировой лидер в области цифровой безопасности, объявила о запуске нового решения - шифратора SafeNet Ethernet CN9100, обеспечивающего организациям беспрецедентную скорость, производительность и безопасность во время шифрования данных в облачных и корпоративных приложениях, а также в высокоскоростных корпоративных сетях.
- SafeNet Ethernet CN9100 шифрует эквивалент 20,000 фильмов в высоком разрешении (HD) всего за одну секунду.
- Безопасно шифруя данные на скорости 100 Гбит в секунду, SafeNet Ethernet CN9100 обеспечивает мега безопасность данных и высокоскоростную производительность в сети со ультрамалой латентностью (время скрытого ожидания < 2 мкс).
- Обезопасив Ethernet трафик высокоскоростным шифрованием 2 уровня, CN9100 отвечает требованиям к сетям с низкой латентностью и без потери полной пропускной способности канала, обеспечивая бескомпромиссную безопасность для больших и даже мега данных, передаваемых **по сетям между ЦОД** и в облаках.
- Новейшее дополнение к семье высокоскоростных шифраторов HSE (High Speed Encryptor) SafeNet Ethernet CN9100 отвечает на постоянно увеличивающийся рост объемов данных и спрос на более высокую пропускную способность сети Ethernet. Он обеспечивает безопасное шифрование голосового и видео трафика, передачи массивов данных на скорости 100 Гбит/с по темному волокну, сетям MAN и WAN, а также Ethernet-сетям. Идеально подходит для шифрования провайдерских сетей, соединения центров обработки данных и резервных площадок, поддерживает все топологии сетей, включая топологию «мультиточка» - «мультиточка».
- <https://www.senetas.com/gemalto-launches-cn9100-100gbps-ethernet-network-encryptor/>

Оборудование компании PacketLight с применением криптозащиты

PL-4000M

400G Muxponder



Aggregation of flexible mix of services into a 400G DWDM uplink

Features Overview

- Flexible high capacity architecture based on 400G pluggable digital coherent optical modules
- Supported clients: 10/25/100Gb Ethernet, 16/32G Fibre Channel, OTU2/2e/4
- Flexible mix of client services mapped into a single 400G DWDM wavelength
- Supports O-FEC on the line side
- Uplinks: Dual 400G CFP2-DCO Open ROADM pluggable coherent modules
- Clients:
 - 4 x QSFP28 for 100GbE or OTU4
 - 24 x SFP+ / SFP28 for all others
- Layer-1 GCM-AES-256 encryption
- Elliptic Curve Diffie-Hellman key exchange
- Comprehensive line and service performance monitoring
- Integrated EDFAs pre-amp/booster (optional)

400G Metro and 200G Long Haul Applications

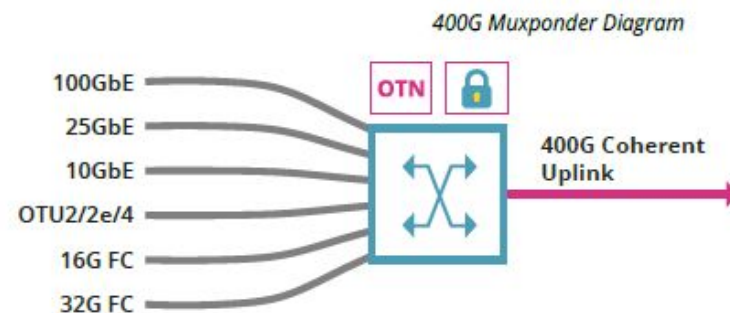
The PL-4000M is a modular and cost-effective solution for rolling out multi-rate 10/25/100GbE, 16/32G FC, OTU2/2e/4 services, or increasing existing network capacity. The device delivers 400G in a 1U chassis using dual 400G CFP2-DCO Open ROADM standard-based pluggable coherent modules for metro and long haul applications.

Main Benefits

- Cost-effective high capacity transport of 400G over single wavelength
- Supports flexible mix of client interface protocols
- Embedded Layer-1 GCM-AES-256 encryption
- Integrated EDFAs and optical switch in 1U chassis
- User-configurable 200G/400G operation mode

Flexible Architecture, Facility Protection Support

The PL-4000M provides full demarcation point between the service and the OTN/DWDM uplink, and is interoperable with any third party switch or router. This provides full visibility and performance monitoring of both line optical transport layer (OTN) and 10/25/100GbE, 16/32G FC, and OTU2/2e/4 service interfaces.



- Facility protection using an integrated optical switch (optional)
- Remote management using in-band GCC or out-of-band OSC

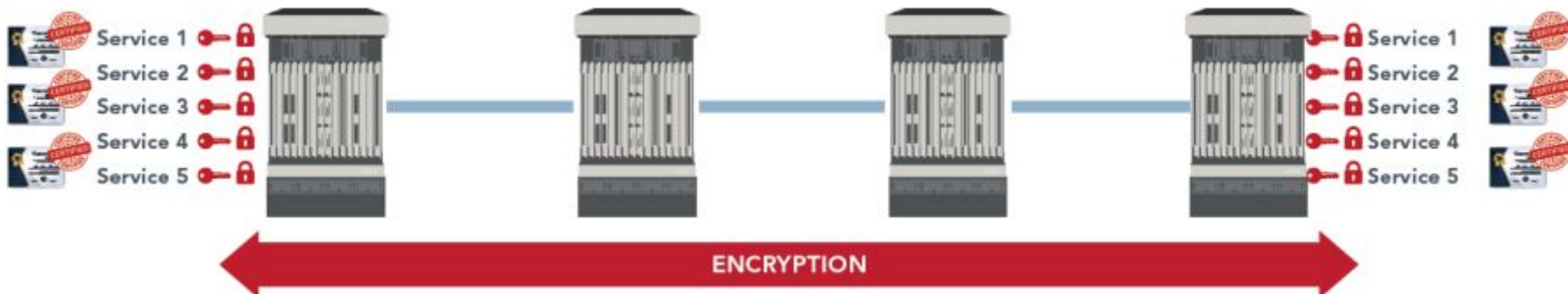
Сертификация – обязательный элемент криптографической защиты оптических каналов в примерах



Сервис шифрования с сертификацией оператора



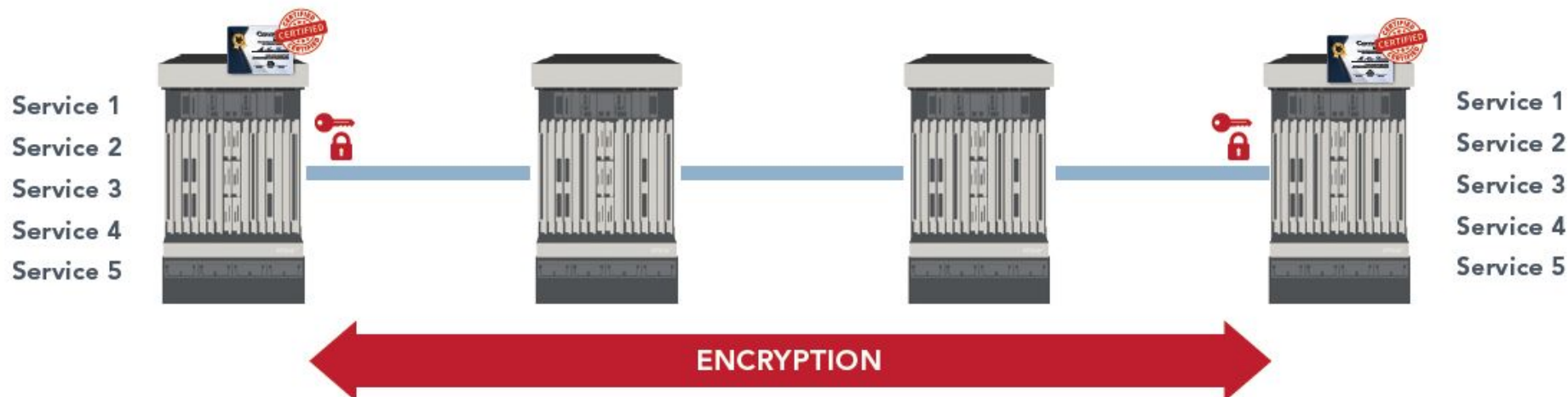
Сервис шифрования с сертификацией клиентского оборудования



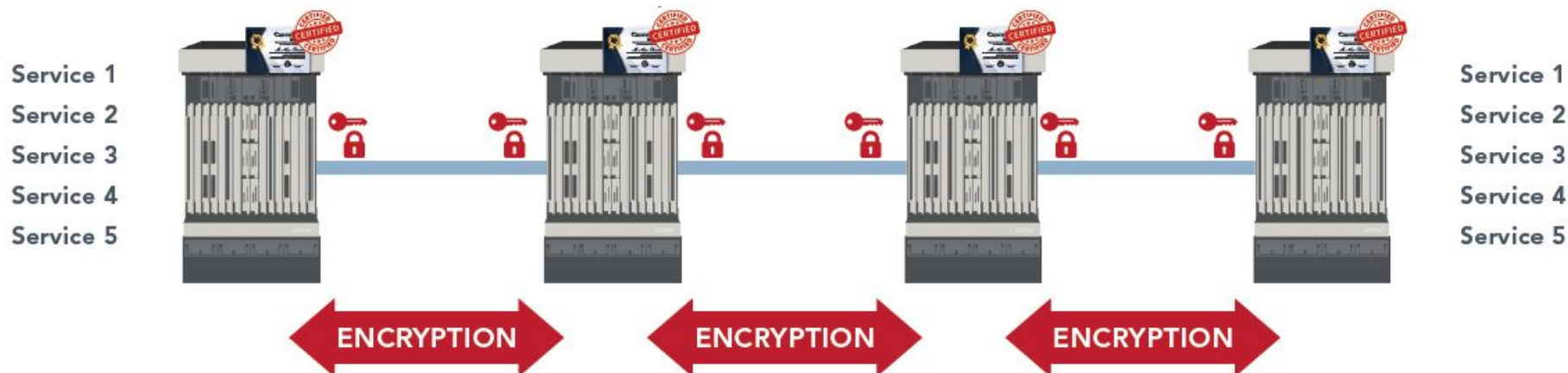
Сертификация – обязательный элемент криптографической защиты оптических каналов в примерах



Сервис шифрования с сертификацией всего объёма трафика между конечными точками с оборудованием



Сервис шифрования с сертификацией по отдельным секциям мультиплексирования



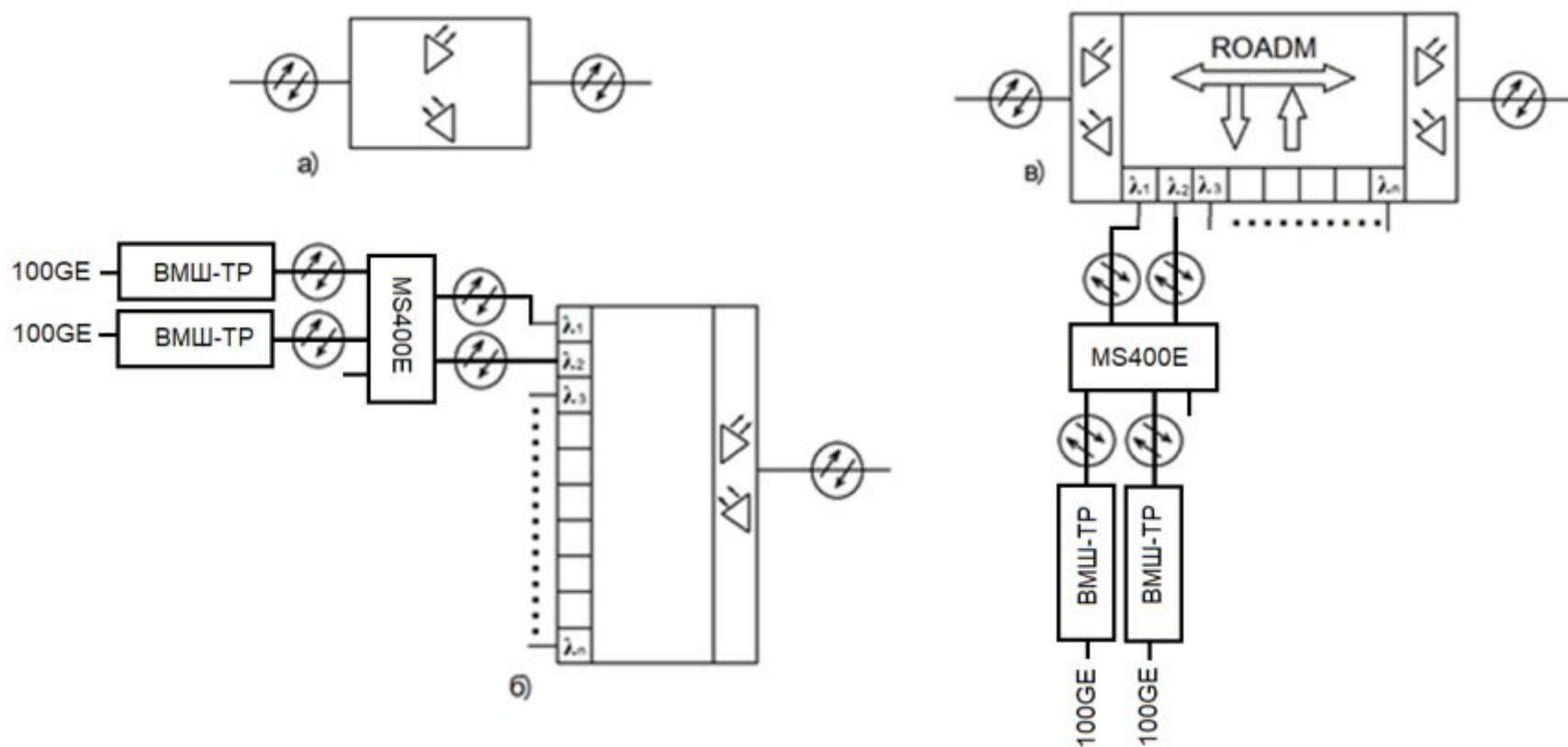
Контрольные вопросы. Отвечать кратко и по существу!

- 1. Какие виды защиты информационного трафика предусмотрены на физическом и оптическом уровнях сети связи?
- 2. Какие пять уровней защиты трафика предусмотрены в транспортной оптической сети?
- 3. Что обозначает защита вида 1+1 OPPM?
- 4. В каком оборудовании транспортной оптической сети устанавливаются элементы криптографической защиты?
- 5. В чём состоят преимущества шифрования (криптозащиты) данных в каналах оптической транспортной сети OTN/OTH?
- 6. Где выше эффективность пропуска трафика при шифровании в OTN/OTH? В MAC sec? В IP sec?
- 7. Что предусмотрено рекомендацией ITU-T Sup.76?
- 8. Для чего нужны IKEv2?
- 9. Какая часть кадра OTUk подлежит шифрованию с целью защиты клиентского трафика?
- 10. Для чего нужны поля TAG, Encrypted OPU, ADD, IV в криптопакете?
- 11. Что входит в криптопакет L1?
- 12. Какой вид шифрования реализуется в схеме PM5990 DIGI-G4?
- 13. На каких участках оптической транспортной сети наиболее актуально применение шифрования?
- 14. Какие защищаемые решения для оптических сетей может поддерживать модуль WCC-PCN-AES100 GB-G?
- 15. Что обозначает DH 4096 key?
- 16. Для чего предназначены модули «Квазар»?
- 17. Где должны применяться модули «Квазар»?
- 18. Какие клиентские скоростные режимы передачи поддерживают модули «Квазар»?
- 19. Какой вид шифрования используется в модулях «Квазар»?
- 20. Что относится к линейке модулей «Квазар»?
- 21. С каким оборудованием транспортных сетей совместимы модули «Квазар»?
- 22. Что в оборудовании компании Packet Light относится к элементам криптографии?
- 23. Что обозначает GCM-AES-256?
- 24. какие виды сертификации обязательны для защиты трафика клиентов в оптических каналах?
- 25. Какая государственная структура РФ обеспечивает сертификацию защиты информации в телекоммуникациях?

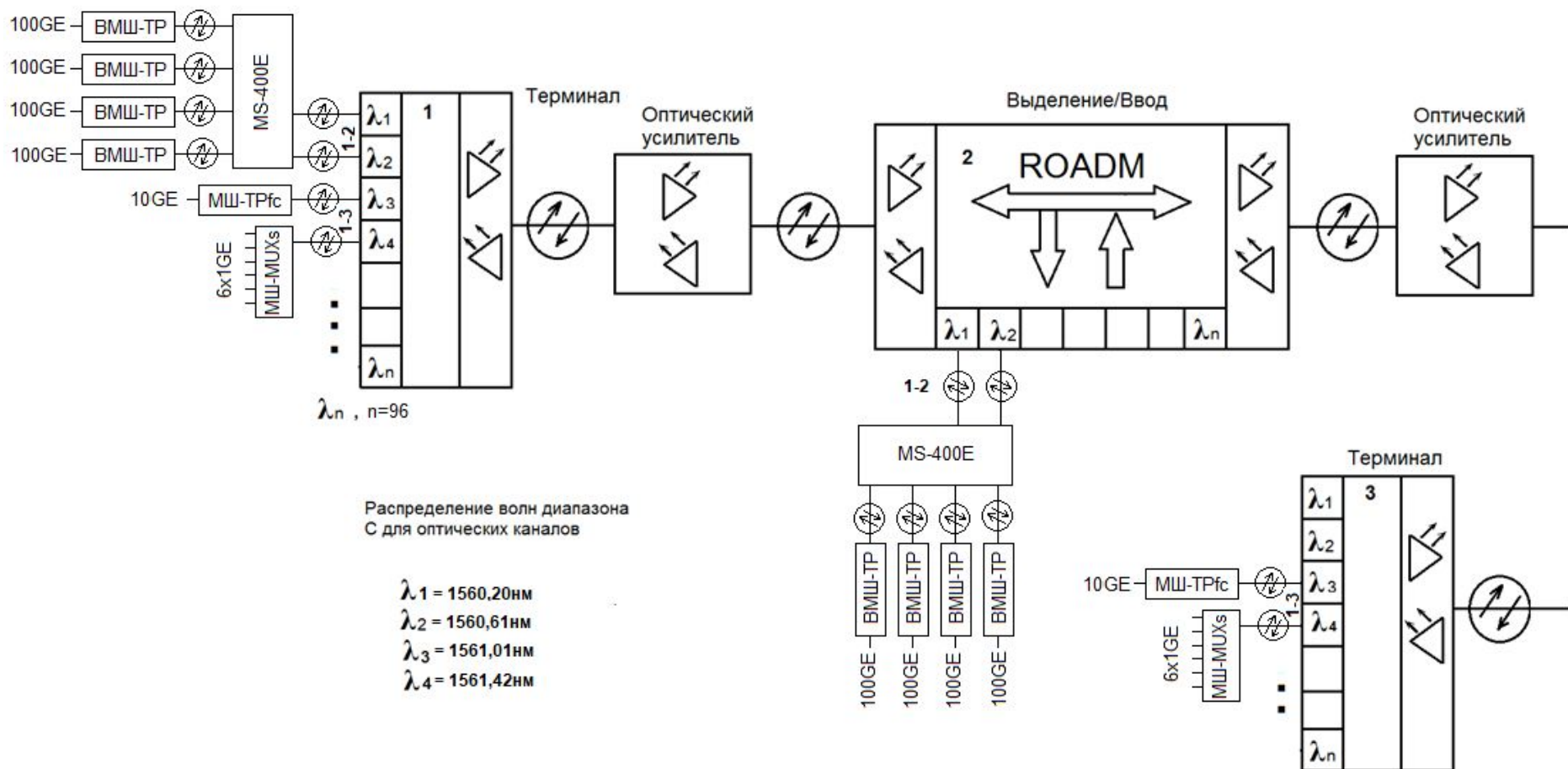
Задача: составить схему организации связи транспортной сети с применением оборудования Т8 ВОЛГА и модулей криптозащиты (МКЗ) по направлениям согласно вариантам. Минимизировать число волн и назначить волны для оптических каналов по данным оборудования ВОЛГА. Составить таблицы комплектации по каждому узлу (1,2,3,4,5,6). Указать название модулей, и в том числе шифрования «Квазар».

Параметры	Вариант соответствует последней цифре номера студ. билета или пароля									
	1	2	3	4	5	6	7	8	9	0
Структура физической сети и число мультиплексоров Терминал/Ввода-вывода (ROADM)	Линейная цепь	Кольцо	Линейная цепь	Кольцо	Линейная цепь	Кольцо	Линейная цепь	Линейная цепь	Кольцо	Линейная цепь
	2/2	0/5	2/3	0/4	2/3	0/5	2/2	2/4	0/4	2/3
Число и шифруемые нагрузки оптических каналов по направлениям										
1-2	1x100GE	4x100GE	6xSTM1	6xSTM4	12x1GE	8xSTM16	5xSTM1	3x100GE	16x1GE	9xSTM1
1-3	4xSTM16	8xSTM1	2x100GE	2xSTM16	4xSTM4	1x100GE	6x100GE	2x100GE	2x100GE	3x100GE
1-4	8x10GE	2xSTM16	4xSTM16	5x100GE	8x100GE	4xSTM1	9xSTM16	1x100GE	6x100GE	7xSTM16
1-5	-	1x100GE	7xSTM4	-	3x100GE	7x1GE	-	4xSTM16	-	2x10GE
1-6	-	-	-	-	-	-	-	4x100GE	-	-
Рекомендуемые мукспондеры оборудования ВОЛГА для объединения шифруемых цифровых потоков в оптические каналы	MS100EQ	MS400E MS100EQ	TD200E MS100EQ	MS800E MS400E MS100EQ	MS800E MS400E MS100EQ	MS100EQ	MS800E TD200E	MS400E TD200E	MS1200E MS800E TD200E	MS400E MS200E

Примеры обозначений на схеме организации связи с защищёнными оптическими каналами: а) оптические усилители на двухволоконной линии (2 усилителя); б) терминальный оптический мультиплексор/демультиплексор с двумя рабочими волнами, подключенными двухволоконными оптическими шнурами к агрегирующему мультиплексору (мукспондеру) MS400E, к другой стороне которого также оптическими шнурами подключены модули шифрования «Кварсис» ВМШ-ТР на клиентской скорости 100Гбит/с Ethernet, оптическая линия подключена к мультиплексору двумя волокнами, в которых используются оптические усилители передачи и приёма; в) оптический мультиплексор ввода/вывода с возможностью перестройки (ROADM) с оптическими усилителями (всего их 4) и доступом к двум оптическим каналам, в которых передаётся совокупный трафик до 400Гбит/с средствами мукспондера MS400E с шифрованием клиентских сигналов на скорости 100Гбит/с Ethernet модулями ВМШ-ТР. <https://skzi.ru>



Пример схемы организации связи в конфигурации «Линейная цепь» с применением оборудования ВОЛГА Т8 и модулей шифрования «Квазар»



Пример схемы организации связи в конфигурации «Двухволоконное кольцо» с применением оборудования ВОЛГА Т8 и модулей шифрования «Квазар»

