ТЕХНО infotecs ФЕСТ 2019

ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

12 09 2019

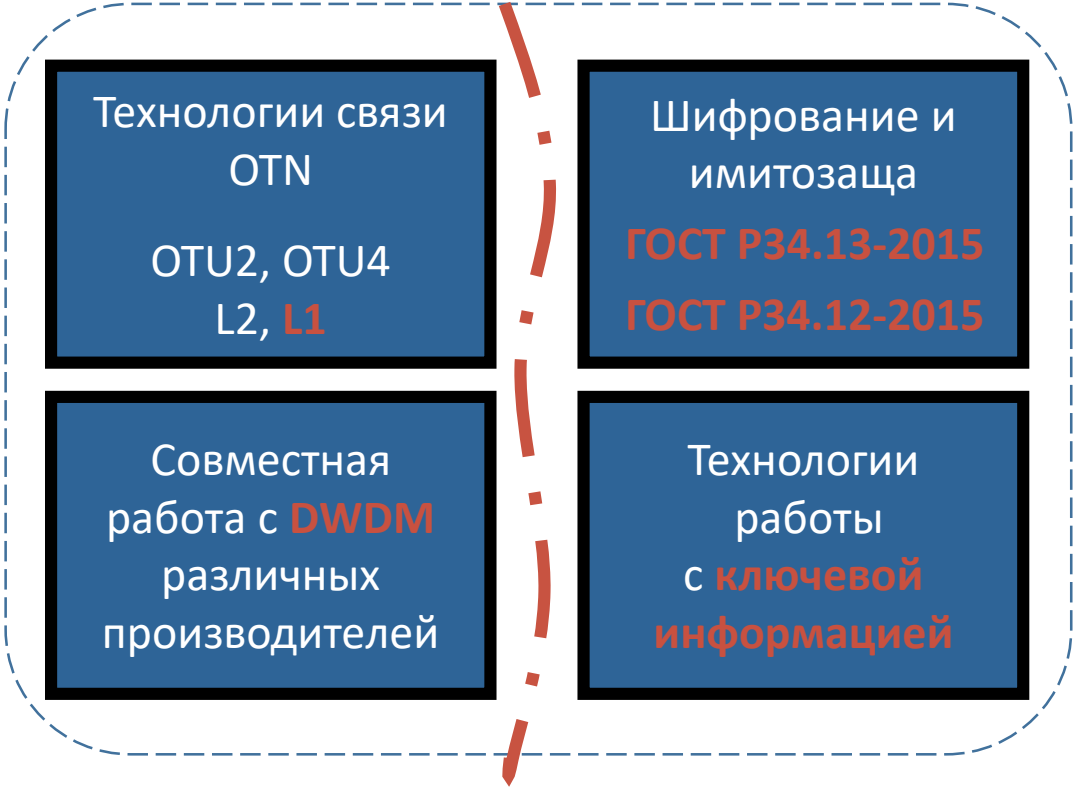
Высокопроизводительный модуль шифрования оптических каналов связи Квазар

О компании

ООО «Системы практической безопасности» *- www.systempb.ru*

- *Отечественный разработчик и производитель программных и программно-аппаратных средств защиты информации. Основное направление деятельности разработка криптографических средств защиты, средств защиты каналов связи.*
- *Лицензиат ФСБ России.*
- *Компания была основана в 2014 году. Головной офис компании расположен в Санкт-Петербурге, также имеется региональное представительство в Москве.*
- *В компании работает 51 человек.*
- *С 2018 года входит в группу компаний ОАО «Инфотекс»*

Решение на стыке технологий



Модуль шифрования

Модули шифрования «Квазар» *устройство предназначено для обеспечения защиты от навязывания ложной информации, несанкционированного доступа и компьютерных атак (включая защиту от скрытых логических каналов передачи) по отношению к информации, передаваемой между клиентами оптических волоконных сетей и узлами связи.*

Модули шифрования «Квазар» *подключаются между клиентским оборудованием и каналообразующим оборудованием и обеспечивают выполнение функций криптоимитозащиты с производительностью* ***10Gbit/s*** *при передаче информации по волоконно-оптическим линиям связи.*

Состав комплекса

- ***Модули шифрования***

  2 варианта конструктивного исполнения:

  - транспондер ***10Gbit Ethernet / FiberChanel8*** *в OTU-2e*

  - агрегирующий транспондер (мукспондер) ***10Gbit*** *8 x 1 в OTU-2e*

  2 варианта исполнения:

  - для установки в специализированное шасси;
  - для установки в стандартную стойку 19/21"

- ***Средство изготовления ключевых документов (АРМ ИКД).***

- ***Комплект смарт-карт***

Продукт лицом

Моноблок - исполнение в корпусе 1U

КВАЗАР

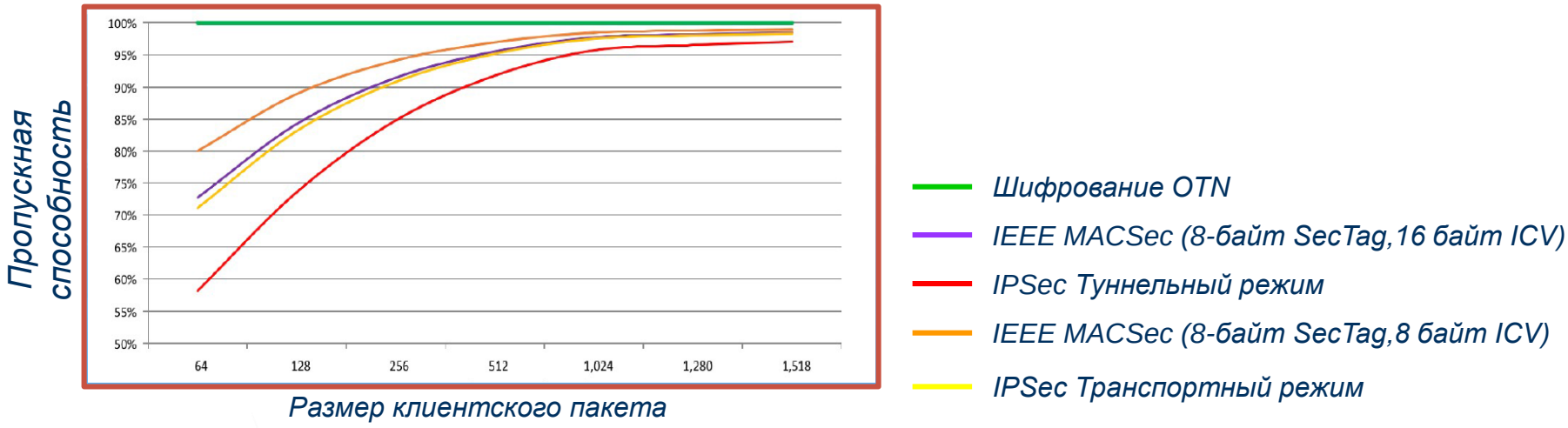
Вставной блок установки в шасси

АРМ ИКД

Носители ключевых документов

Основные преимущества решения

- Шифрование на уровне L2/L1
- Клиентский интерфейс 10G Ethernet/FiberChanel 8
- Линейный интерфейс OUT-2e с резервирование
- Задержка (Latency) - 0.05 ms
- Работа с DWDM различных производителей
- Работа до 80 км по паре «темных» волокон
- Отсутствие зависимости пропускной способности и задержки от размера клиентских пакетов

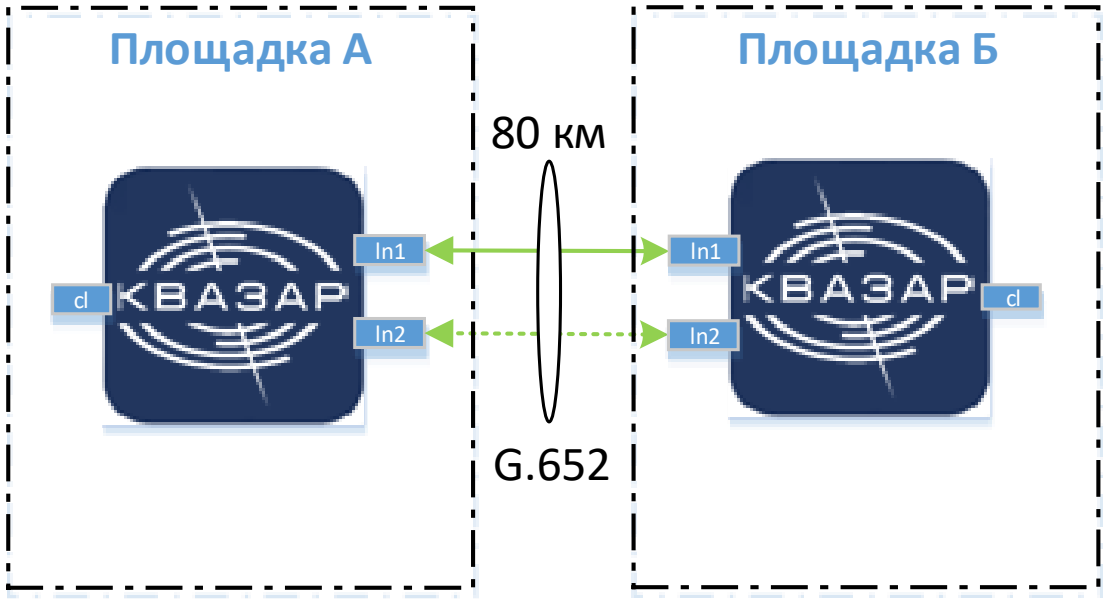


Какой уровень выбрать при организации каналов 10G с высокой пропускной способностью???

Характеристика	IPSec(L3)	MACSec(L2)	OTN (L1)
Сложность и стоимость	Высокая	Низкая	Низкая
Задержка	Высокая	Низкая	Низкая
Мульти-сервис	Нет	Нет	Да
Пропускная способность	Низкая	Средняя	Высокая
Гибкость встраивания	Низкая (только IP-сети)	Низкая (только Ethernet)	Высокая (любые оптические сети, различные длины волн)
Размер зашифрованной части	Малый (<1500 байт)	Малый (~1500 байт)	Большой (~14000 байт)

Варианты включения

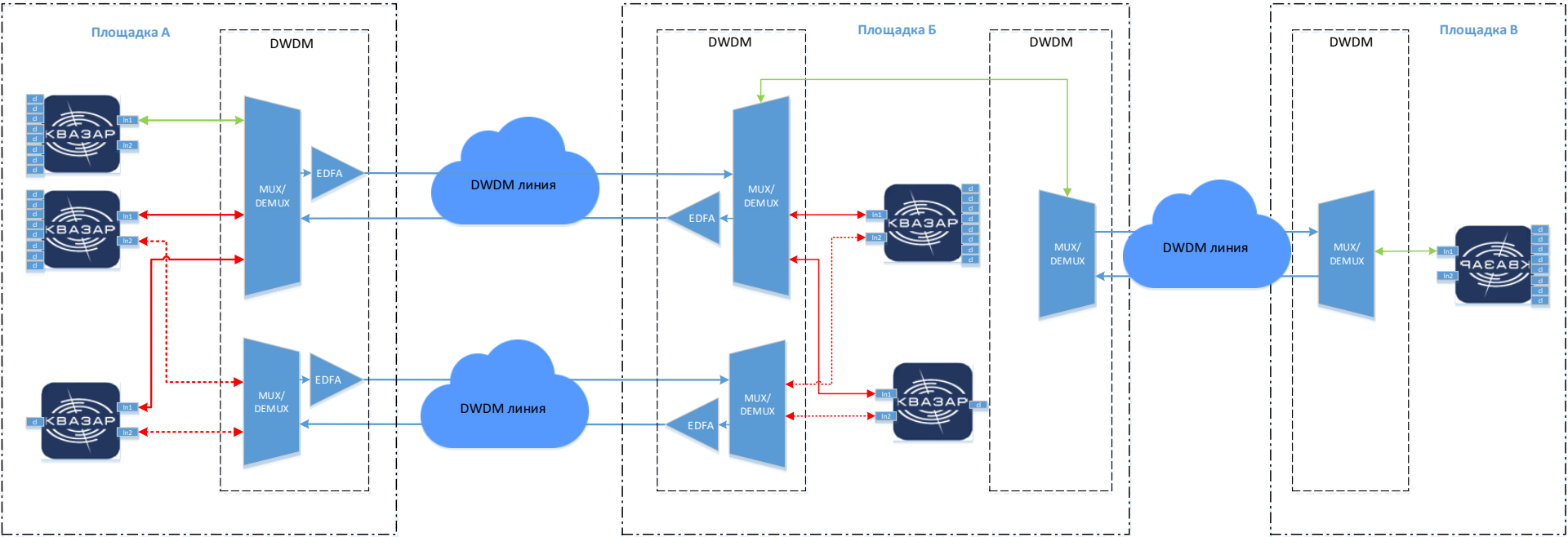
- По паре темных волокон



До 80 км, ограничение по дисперсии и затуханию.

Варианты включения

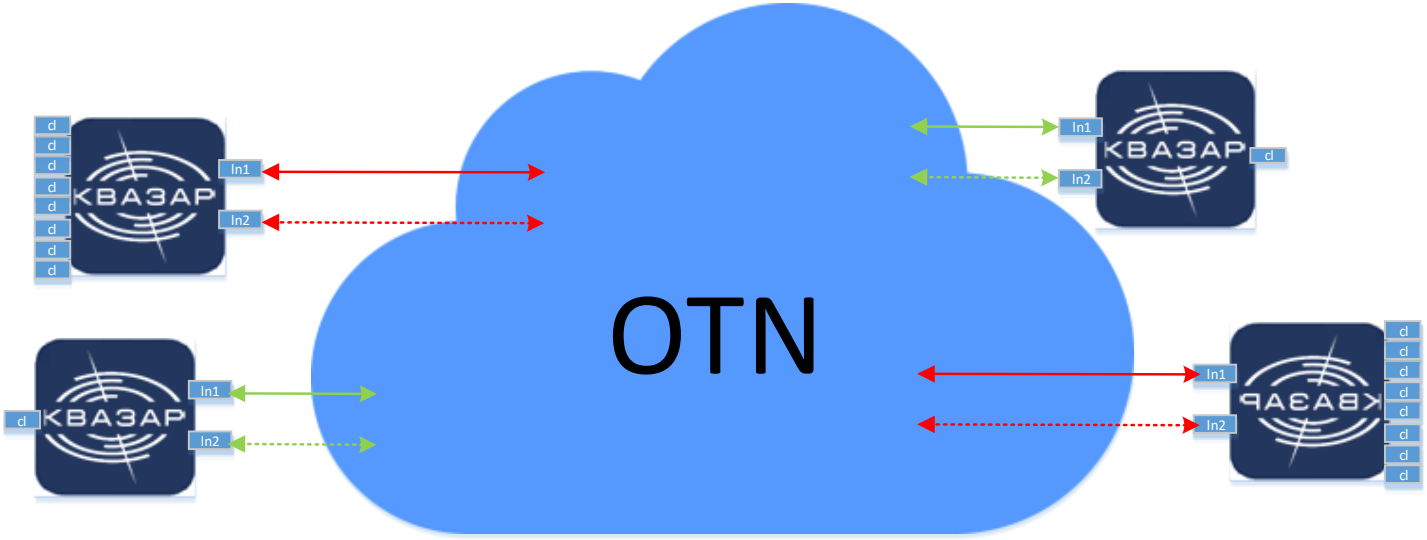
- В DWDM линию



Соответствие сетке частот DWDM

Варианты включения

- В OTN



Поддержка протокола OTU-2e со стороны OTN

Криптографические характеристики

- Класс СКЗИ — КС3
- Алгоритм шифрования: ГОСТ Р34.12-2015
- 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
- Модификации ключа через определённое количество кадров
- Защита от «чтения назад» - периодическая нереверсивная модификация ключей

Сертификаты соответствия

- **Сертификаты ФСБ** – *на средства криптографической защиты информации (СКЗИ) из состава средств «Комплекса криптографической защиты конфиденциальной информации для работы в OTN-сетях:*
  - *СКЗИ МШ-MUX (от 04 октября 2017г. №СФ/124-3211),*
  - *СКЗИ МШ-MUX-1U (от 04 октября 2017г. №СФ/124-3210),*
  - *СКЗИ МШ-TP (от 04 октября 2017г. №СФ/124-3209),*
  - *СКЗИ МШ-TP-1U (от 04 октября 2017г. №СФ/124-3208),*
  - *СКЗИ МШ-TPfc (от 28 марта 2019г. №СФ/124-3666),*
  - *СКЗИ МШ-TPfc-1U (от 28 марта 2019г. №СФ/124-3667).*
- **Сертификат ФСБ** – *на СКЗИ «Автоматизированное рабочее место изготовления ключевой информации» от 04 октября 2017г. №СФ/123-3212 из состава средств «Комплекса криптографической защиты конфиденциальной информации для работы в OTN-сетях.*

Совместимость

ТехноInfotecs Фест 2019

+ КВАЗАР =

infotecs

ADVA Optical Networking

ПАК

(Программно-аппаратный комплекс)

ЕКИПОРС JUNIPER NETWORKS

CISCO ZTE HUAWEI

и другие 😁

КВАЗАР

Потребители

- Операторы связи
- Коммерческие банки
- Федеральные органы исполнительной власти
- Государственные корпорации
- Силовые ведомства
- Частные компании

Сценарии применения

- Организация каналов связи в защищенном исполнении;
- Построение защищённых каналов передачи данных между ЦОД;
- Защита различных мультисервисных сетей (территориально распределенные системы виртуализации, потоковое видео, ВКС, телефония, передача данных в СХД).

Почему Квазар???

- организация передачи большого объема данных с обязательным обеспечением ее защиты при невозможности можно выделить защищаемую информацию из общего потока;
- обеспечение работоспособности инфраструктуры при условии критичности к пропускной способности каналов и задержкам на них;
- обеспечение защиты созданной ранее и развивающейся (модернизируемой) инфраструктуры;
- необходимость защиты каналов передачи данных, согласно новым требованиям федеральных законов;
- модернизация действующей инфраструктуры под новые требования ФЗ (требования для КИИ);
- не возможность изменения существующей оптической сети у Заказчика;
- резервирование 1+1;
- бесшовная имплементации СКЗИ в схемы сетей DWDM;
- оборудование российского производителя (импортозамещение).

Требования ФЗ - Правовой аспект применения

Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от **26.07.2017 №187-ФЗ**

Положение Банка России от **09 июня 2012 г. № 382-П (с изменениями от 7 мая 2018 г. №4793-У)** «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

«Пакет Яровой»:

- Федеральный закон от **06 июля 2016 г. № 374-ФЗ** «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»
- Федеральный закон от **06 июля 2016 г. № 375-ФЗ** «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»

Планы развития

2019

- Выпуск первых образцов для получения сертификата соответствия требованиям ФСБ России нового типа изделия СКЗИ МШ «Сотник» с пропускной способностью 100G
- Проектирование и создание опытного образца изделия нового СКЗИ МШ-ТР-КРК «Квазар» с системой квантового распределения ключей
- Проведение работ по расширению видов интерфейсов FiberChanel (FC16 и FC32)

2020

- Сертификация СКЗИ МШ «Сотник» с пропускной способностью 100G согласно требованиям ФСБ России
- Сертификация СКЗИ МШ-ТР-КРК «Квазар» с системой квантового распределения ключей

КВАЗАР

ТЕХНО 2019 infotecs Фест

Спасибо
за внимание!