

Модули шифрования «Квазар»

Криптографическая защита и организация высокоскоростных каналов
СВЯЗИ

Маркевич Кирилл Викторович

Руководитель направления высокопроизводительных СКЗИ,
ООО «Системы практической безопасности»

<https://skzi.ru/>

О производителе

Компания «Системы практической безопасности» (ООО «СПБ») образована в 2014 г.



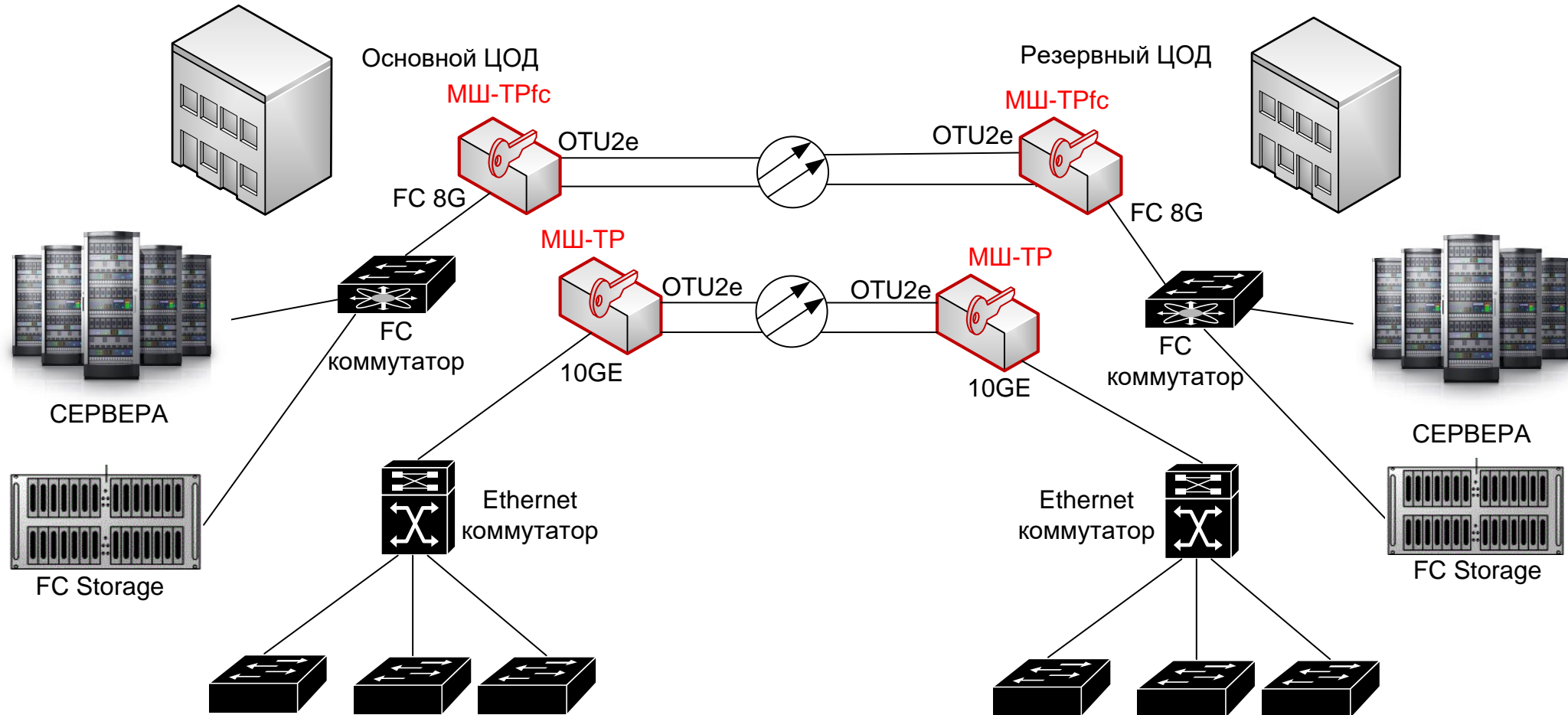
СПБ вошла в группу компаний «ИнфоТекС» и является ее официальным партнером.

Основные направления деятельности компании «СПБ»:

- разработка СКЗИ высокого класса на базе программно-аппаратных решений собственной разработки;
- разработка программного обеспечения для защищенных систем различного назначения;
- производство СКЗИ;
- создание защищенных сетей обмена данными на базе СКЗИ собственной разработки;
- внедрение и сопровождение эксплуатации СКЗИ и защищенных систем.

Высокоскоростные каналы передачи данных

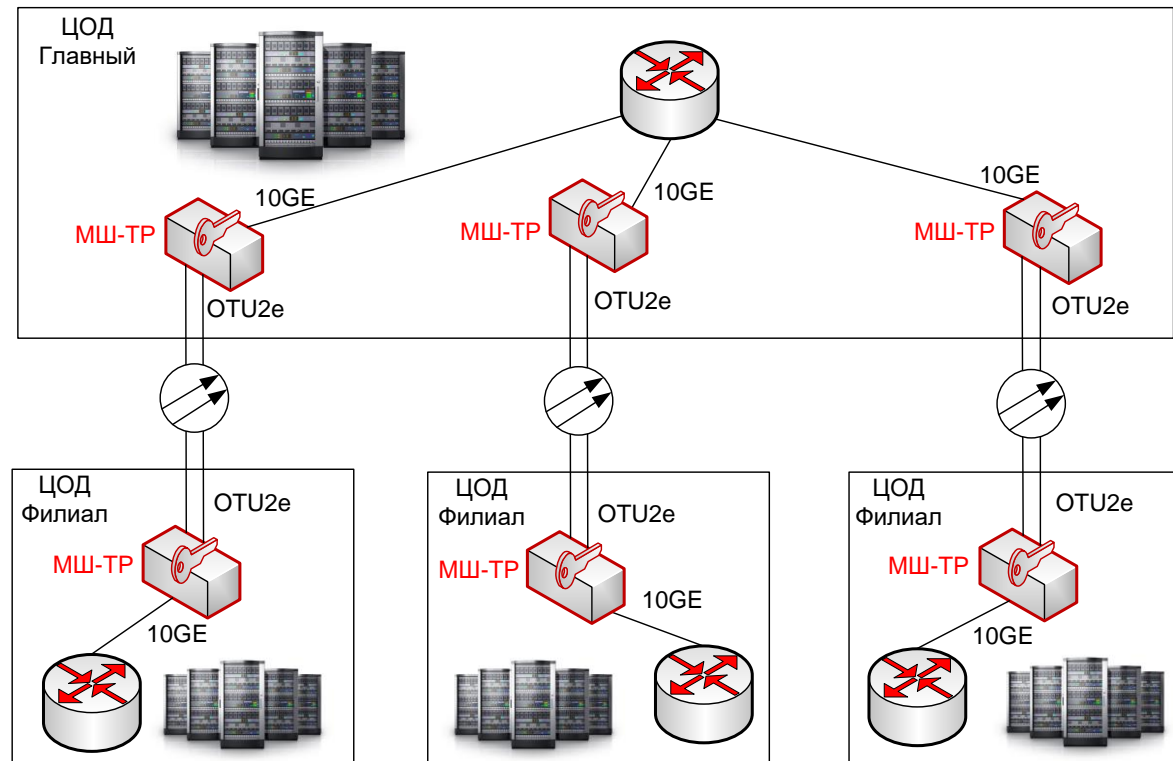
ЦОД - РЦОД



Высокоскоростные каналы передачи данных

ЦОД – площадка (site)

Площадка – площадка (site-to-site)



Проблемы защиты высокоскоростных каналов

- Снижение пропускной способности канала связи. Высокие накладные расходы на шифрование.
- Низкая скорость шифрования. Не поддерживается работа на скорости линии.
- Влияние на характеристики и качество сети — вносимая задержка и ее изменение (вариация), потери пакетов или кадров.
- Отсутствие приоритизации шифрования трафика между сервисами.
- Внесение изменений в служебную информацию. Влияние на QoS, trunk.
- Влияние на архитектуру сети. Необходимы встраивание в IP-сети или коммутация пакетов.

О продукте

- Модули шифрования «Квазар» — это устройства для криптографической защиты и организации высокоскоростных каналов связи.
- Архитектура модулей шифрования «Квазар» спроектирована таким образом, чтобы обеспечить эффективную работу с оптической средой передачи данных без влияния на характеристики сети.
- Модули шифрования «Квазар» самостоятельно работают на оптических линиях без применения дополнительного оборудования, а также встраиваются в существующие системы спектрального уплотнения (WDM).
- Модули шифрования «Квазар» поддерживают протоколы 10G и Fiber Channel 8G, Ethernet 1G и STM (4-8-16) и выполняют функции криптозащиты с производительностью 10 Гбит/с.
- **Сертификат ФСБ России класс КС-3.**

Преимущества

Минимальное влияние на ИТ-сервисы благодаря уникальным сетевым характеристикам:

отсутствие потерь пакетов при любых нагрузках;

рекордно малая задержка (latency) – 44 мкс;

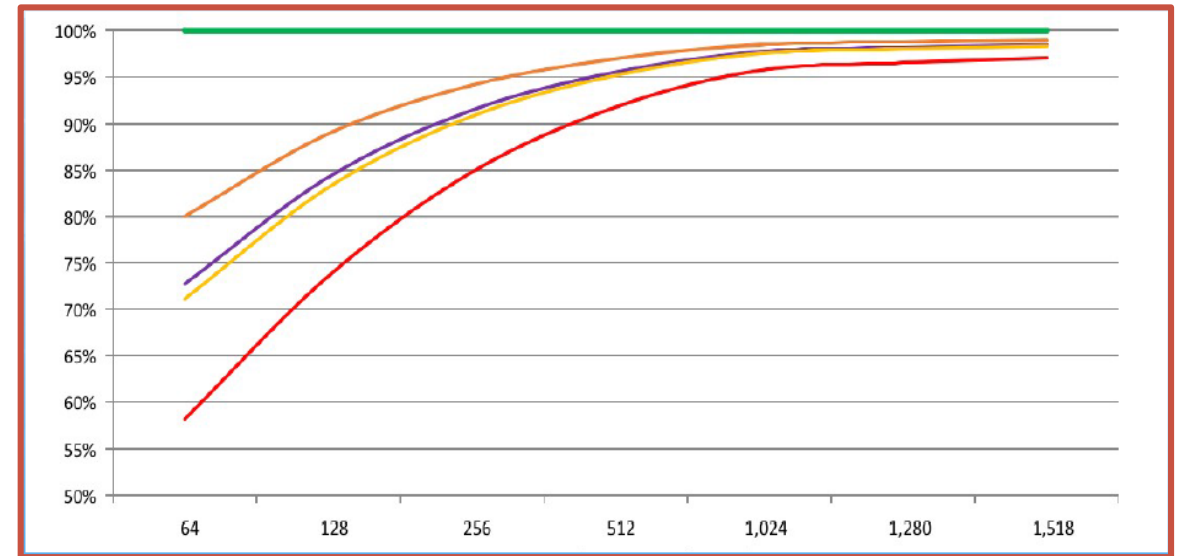
отсутствие вариации задержки (jitter) – 0;

работа скорости линии – 10 Гбит/с.

- Защита мультисервисных сетей (потокное видео, ВКС, телефония, передача данных) без необходимости разделения потоков данных.
- Поддержка основных протоколов передачи (Eth 1G и 10G, 8G FC, STM 1-4-16).
- Простая интеграция и внедрение без перерыва сервисов.
- Совместимость с любым DWDM или работа по «темному» волокну.
- Легкость в управлении. «Квазар» не требует постоянного обслуживания.
- Интегрируется с системами мониторинга.
- Низкая стоимость в пересчете на гигабит защищенной информации.

Сравнение с шифраторами других уровней

Характеристика	IPSec(L3)	MACSec(L2)	OTN (L1)
Сложность и стоимость	Высокая	Низкая	Низкая
Задержка	Высокая	Низкая	Низкая
Мультисервис	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)



Размер клиентского пакета

- Только защита передачи данных
Не IPS, не Firewall, не DLP и т.д.
- Только точка–точка.
Не full mesh, не «звезда».
- Нулевая интероперабельность.
Нет совместимости с другими СКЗИ.
- Отсутствует удаленная смена ключей.

- Шифрование «Квазар»
- IEEE MACSec (8 байт SecTag, 16 байт ICV)
- IPSec Туннельный режим
- IEEE MACSec (8 байт SecTag, 8 байт ICV)
- IPSec Транспортный режим

Криптографические характеристики изделий

- Все изделия имеют сертификат соответствия требованиям ФСБ к СКЗИ по классу КС-3.
- 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 определенное количество кадров.
- Защита от «чтения назад» — периодическая нереверсивная модификация ключей (период менее 1 часа).

Требования регуляторов



Федеральный закон
«О безопасности критической
информационной
инфраструктуры Российской
Федерации»
№187-ФЗ от 26.07.2017



Федеральный закон
«О персональных
данных» **№152-ФЗ**
от 27.07.2006



Положение Банка России
№ 719-П «О требованиях к
обеспечению защиты
информации...» от 23.09.2020
(замена 382-П)



«Пакет Яровой»
Федеральный закон «О внесении
изменений в Федеральный закон
«О противодействии
терроризму»...» от 06.07.2016
№ 374-ФЗ и другие
законодательные акты

Заказчики

Промышленность		Государственные организации
<ul style="list-style-type: none">○ Атомная○ Ракетно-космическая○ Горнодобывающая○ Metallургия○ Химическая○ Оборонная	<ul style="list-style-type: none">○ ТЭК○ Энергетика○ Здравоохранение<ul style="list-style-type: none">○ Наука○ Транспорт○ Телекоммуникации<ul style="list-style-type: none">○ Финансы	<ul style="list-style-type: none">○ Министерства○ Фонды○ Центры○ Комитеты○ Службы

Условия для применения СКЗИ «Квазар»

- Требования по защите передаваемой информации с применением алгоритма шифрования ГОСТ.
- Потребность в высокоскоростных каналах передачи данных.
- Наличие информационных систем и сервисов с высокими показателями SLA.

Внедрения

- **Банки**

 - 4 поставки.

Общий объем изделий в эксплуатации
- более 120 шт.

- **Промышленность**

 - 2 поставки.

Мощность производства
- более 500 изделий в год.

- **Государственные учреждения**

 - 2 поставки.

В разработке
- более 10 проектов.

- **Телеком**

 - 1 поставка.

СКЗИ «Квазар» — модули для шасси

Транспондер — МШ-TRfc



Агрегирующий транспондер — МШ-MUXs



СКЗИ «Квазар» — модули 1U

Транспондер — МШ-ТРfc-1U



Агрегирующий транспондер — МШ-MUXs-1U

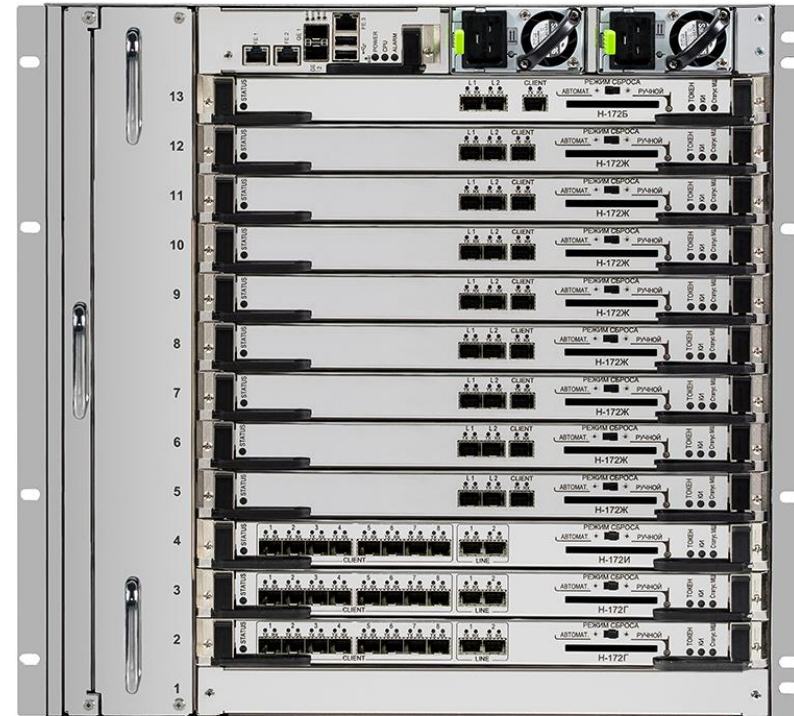


СКЗИ «Квазар» — шасси для установки

Шасси – V3



Шасси – V10



Шасси – V6



Техническая поддержка (ТП) и гарантия

Линейка продуктов ТП

Линейка продуктов гарантии

1. Базовая ТП

1. Гарантия производителя — 1 год.

2. Совместная ТП

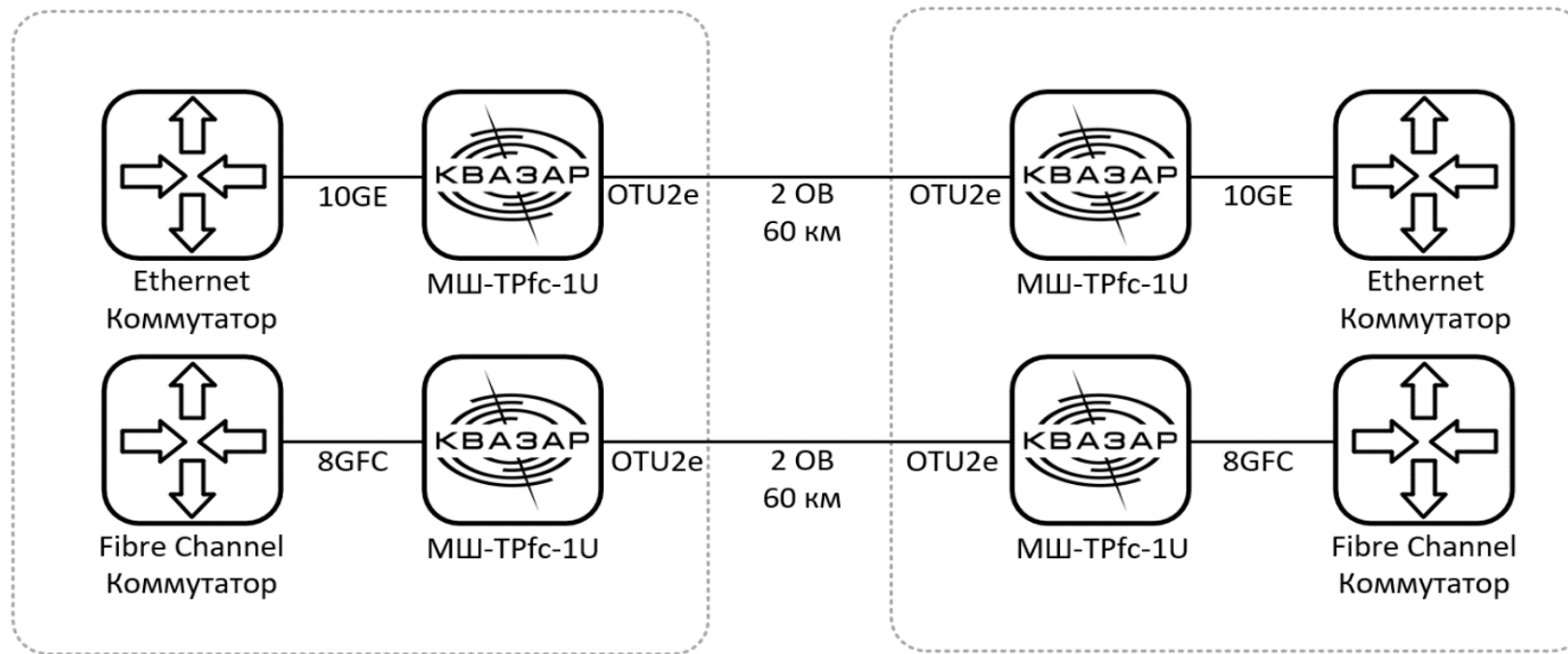
2. Продление гарантийного обслуживания на срок 1 год для 2–3-го года эксплуатации.

3. Расширенная совместная ТП

3. Продление гарантийного обслуживания на срок 1 год для 4–5-го года эксплуатации (в разработке).

Схемы применения СКЗИ «Квазар»

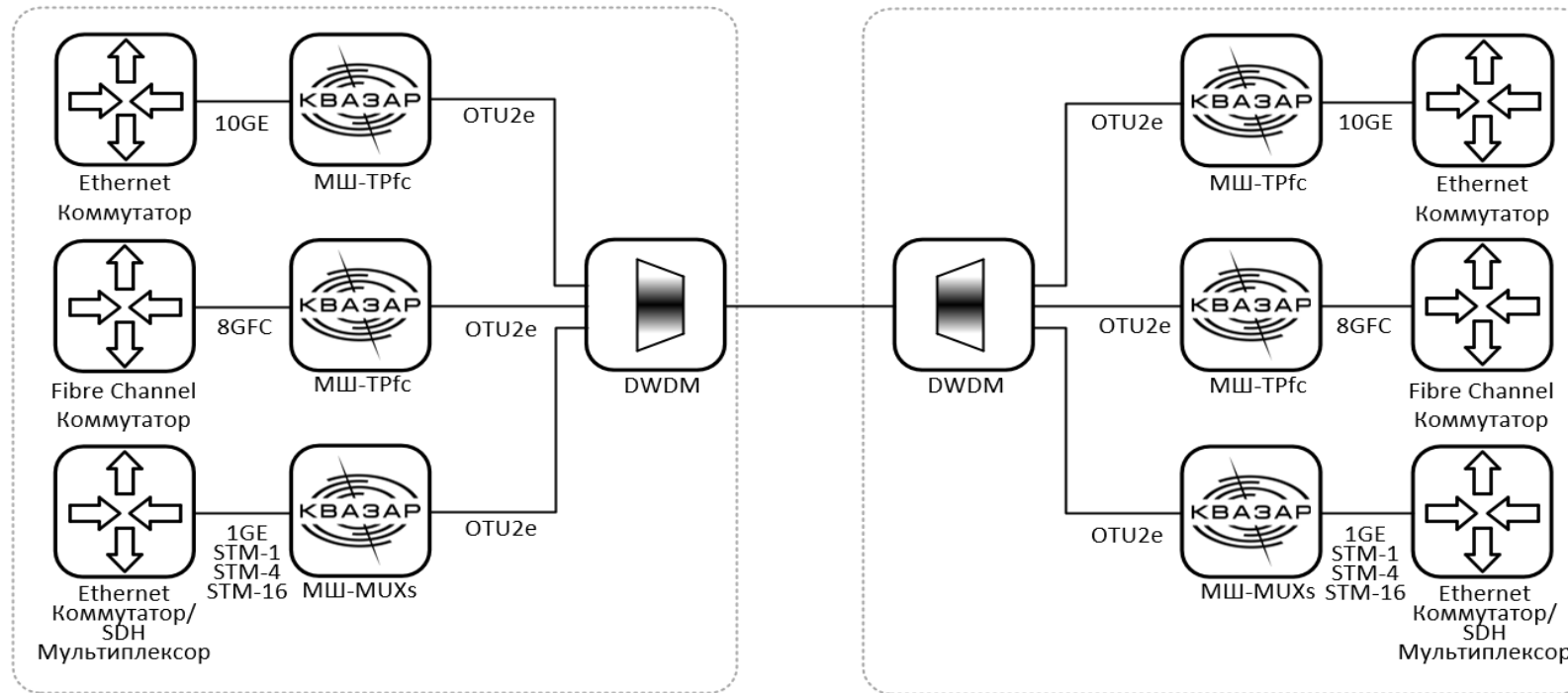
Защита каналов 10GE или 8GFC без WDM без резервирования



Данное решение позволяет защитить один оптический канал со скоростью до 10 Гбит/с с типом сервиса 10GE или 8GFC по одной паре волокон.

Схемы применения СКЗИ «Квазар»

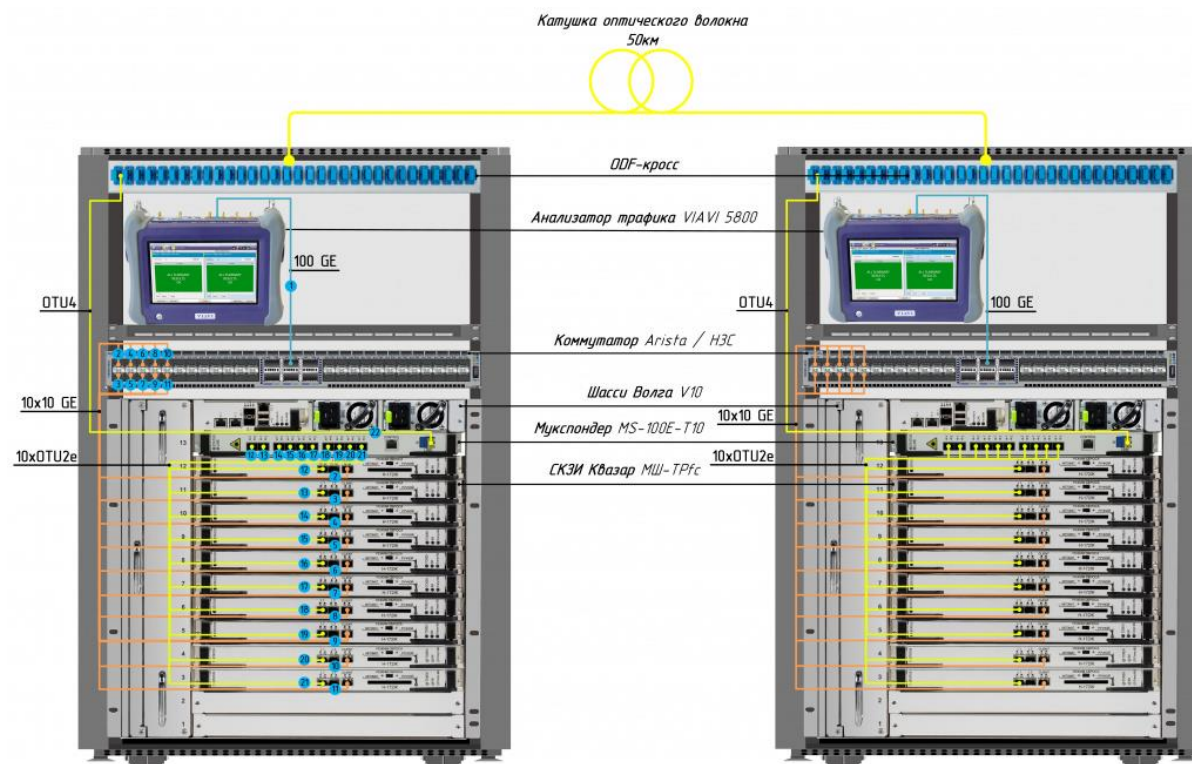
Защита каналов с включением в существующую DWDM-сеть без резервирования



Данное решение позволяет защитить оптические каналы 10GE, 8GFC, 1GE, STM-1/4/16 с включением в существующую DWDM-сеть (соответствующую стандарту ITU G.709) по OTU2e на чужой длине волны.

Перспективы развития

Комплексные решения по защите каналов связи 40G–100G на базе СКЗИ «Квазар»



[Подробное описание решения](http://systemrb.ru) на сайте systemrb.ru в разделе «Новости».

Перспективы развития

Проектирование и разработка линейки оборудования для защиты каналов:

- Ethernet 100G — агрегированные каналы между ЦОД
 - Fiber Channel 16
 - Fiber Channel 32
- } — модернизация сетей СХД

Уже имеются технические задания, работающие образцы изделий, ведутся работы по сертификации.

Ожидаемый срок выхода на рынок — конец 2021 г.

Спасибо за внимание!

Маркевич Кирилл Викторович

Руководитель направления высокопроизводительных СКЗИ,

ООО «Системы практической безопасности»

Т. +7 (812) 468-15-85, доб. 409

М.+7 (917) 570-33-62

MarkevichKV@systempb.ru

<https://systempb.ru>

<https://skzi.ru>