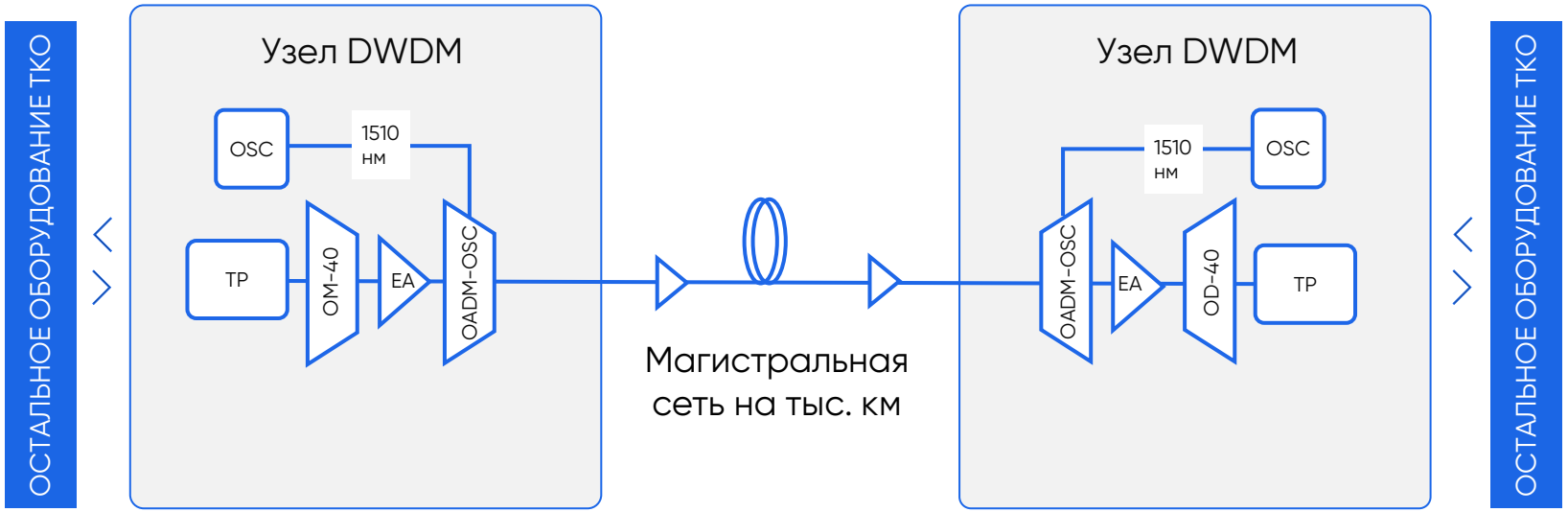
КОМПАНИЯ Т8

Развитие отечественного ТКО

DWDM-ОБОРУДОВАНИЕ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

ООО «Т8», info@t8.ru, t8.ru

DWDM-оборудование жизненно важно для информационной инфраструктуры страны



Передача десятков Терабит в секунду на тысячи километров

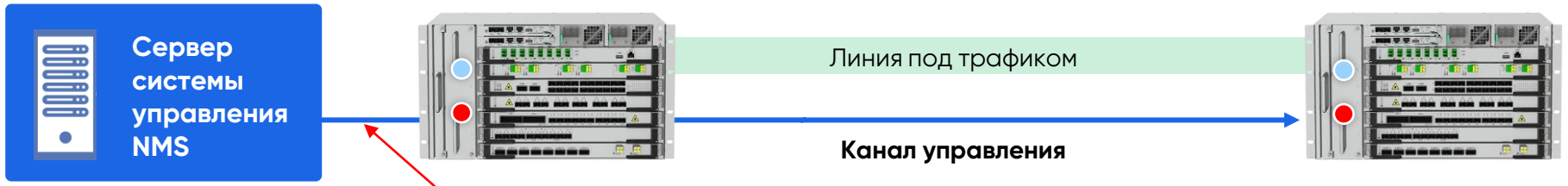
Отказ DWDM-оборудования ведет к отказам сервисов у тысяч клиентов

Операторы связи
Беспроводные сети (LTE/ 5G)
Дата-центры
Спец. потребители

Магистральные оптоволоконные сети являются основой **информационной инфраструктуры**.

По DWDM передаётся более **99% трафика данных =** критически важный вопрос информационной безопасности страны.

Проблемы информационной безопасности и предложения по усилению защиты магистральных DWDM-сетей



Обратите внимание

При шифровании канала управления сертификация оборудования по ПКЗ-2005 (как СКЗИ) не требуется.

На объекты и помещения, в которых установлено оборудование с использованием СЗИ, доп. требования (как для СКЗИ) распространяться не будут.

Угрозы

1 Атака на NMS, нецелевое подключение к серверу

NMS – самый уязвимый элемент DWDM для атаки

2 Атака на внешний канал управления, перехват и подмена команд

2.1 Атака на внутренний канал управления, перехват и подмена команд

3 Атака на блок управления, заливка ВПО с НДВ

Предложения

1 Обязательность категорирования систем управления **DWDM-оборудования** как объектов КИИ

2 Шифрование канала управления по ГОСТ, отказ от зарубежной криптографии AES256 и др.

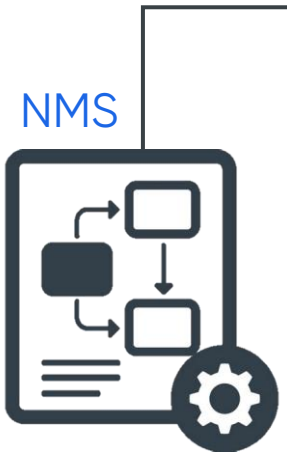
2.1 Шифрование канала управления по ГОСТ

3.1 Контроль целостности ПО и ВПО **с помощью ЭП** на российских алгоритмах, рекомендованных регулятором (подпись прошивки)

3.2 Установка модуля доверенной загрузки и удаленного обновления (корень доверия)

- Микросхема «Корень доверия»
- ЭП прошивки (подпись кода)

Предложение №1. Категорирование систем управления DWDM-оборудования как КИИ, сертификация по УД4 (ФСТЭК)



- ✓ **NMS - ВСЕГДА** КИИ
- ✓ **NMS - ВСЕГДА** объект категорирования
- ✓ **NMS - ВСЕГДА** присваивается категория 1
- ✓ **NMS - ВСЕГДА** сертифицируется по требованиям ФСТЭК России

Что это дает?

- Невозможность применения зарубежных систем управления DWDM с закрытым исходным кодом, обладающих НДВ;
- Защиту от несанкционированного доступа к информации;
- Минимизацию рисков кибератак на критически важные объекты.

Закрепление на нормативном уровне

Обязательность категорирования систем управления DWDM-оборудования как КИИ для всех отраслей

Проекты постановления Правительства РФ:

- Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры в сфере связи, транспорта, химической промышленности, металлургической промышленности, науки, ракетно-космической, атомной промышленности, здравоохранения, топливно-энергетического комплекса и энергетики (ID: 156891, 157391, 157760, 157754, 157758, 157727, 157757, 157931, 158039, 157505, 157203 и других)

Включение требования о сертификации ФСТЭК России систем управления DWDM-оборудования при получении Сертификата средств связи.

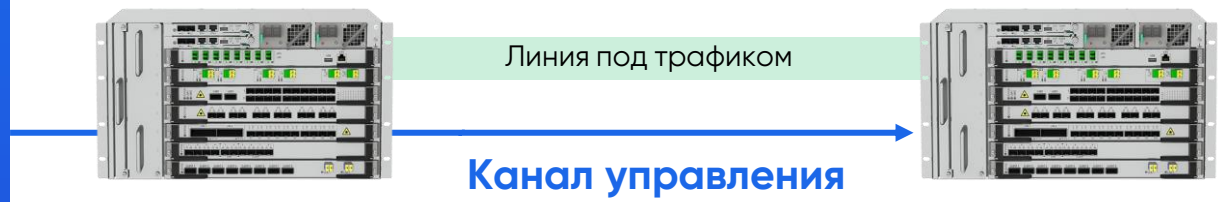
Обязательность присвоения 1-й категории значимости DWDM как объекту КИИ при категорировании для применения требований по УД4:

- Приказ ФСТЭК России от 25 декабря 2017 г. № 239
- Постановление Правительства РФ от 08.02.2018 N 127

Модернизация постановления Правительства РФ № 1912:

- Дополнение перечня субъектов КИИ сферой внутренней торговли (включая сегмент онлайн-торговли) ПП РФ от 14.11.2023 № 1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов»

Предложение №2. Переход от шифрования каналов управления оборудованием с зарубежной криптографией на российскую



Выполнение на оборудовании DWDM требования УПД.3 в части передачи управляющей информации только по защищенному каналу связи путем шифрования канала по ГОСТ

↓

Шифруется только сигнал управления, клиенту услуга шифрования данных не предоставляется;

На узлах связи не хранится секретная часть ключа, только сертификат открытого ключа;

↓

DWDM станет СЗИ, но не СКЗИ.
Для СЗИ не требуется сертификация защиты канала управления как СКЗИ по ПКЗ-2005.

Закрепление на нормативном уровне

Включение в Приказы Минцифры России требования о шифровании каналов управления DWDM-оборудования при проектировании, вводе в эксплуатацию и модернизации сетей связи. (№№ 132, 832, 984)

Предложение № 3.1 – контроль целостности ПО и ВПО с помощью ЭП на российских алгоритмах, рекомендованных регулятором

Электронная подпись (ЭП) прошивки
криптографический механизм, который обеспечивает целостность и аутентичность программного обеспечения, записанного в постоянную память (ПЗУ) устройства.

Защита от:

- ✓ Установки неавторизованного программного обеспечения;
- ✓ Изменения характеристик и функций оборудования;
- ✓ Внедрения закладок и вредоносного кода.

Риски сейчас:

Механизм ЭП разрабатывается и внедряется производителями за рубежом, что создает уязвимость, которую невозможно проверить



Закрепление на нормативном уровне

Приказ ФСТЭК России от 2 июня 2020 г. № 76

Предложение № 3.2 – установка модуля доверенной загрузки на устройства

Установка на блок управления DWDM модуля доверенной загрузки, поддерживающего удаленное обновление и шифрование канала управления (например «Корень доверия»)

Доверенная
ПЛАТФОРМА

Риски сейчас:

Зарубежные производители могут устанавливать такие микросхемы без физического включения или без контроля штатных функций ВПО