ViPNet L2-10G. Канальный шифратор

Алексей Данилов

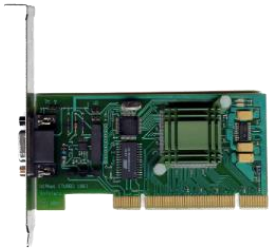
ТЕХНО 2023 infotecs ФЕСТ

Развитие шифрования

Эволюция криптографии

1991 — Программное шифрование

1999 — ViPNet Turbo100 VPN Acceleration Card



2011 — ViPNet Solo – portable encryptor

2012 — VAC 1G

2016 — L2-10G

2016

ViPNet Turbo100 – криптоускоритель

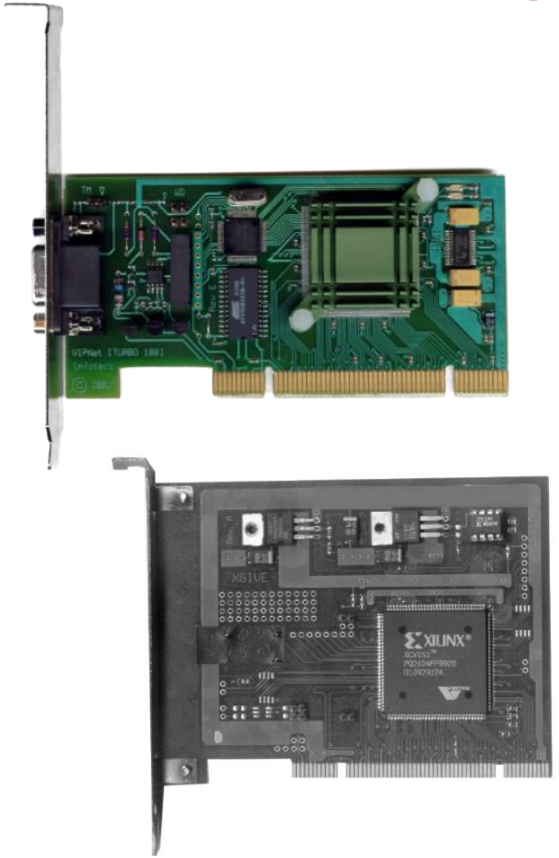
Turbo100 разработан для ускорения операций шифрования.

Функции:

- Основан на ПЛИС (FPGA) Xilinx XCV150.
- Поддержка алгоритма ГОСТ 28147-89.
- Все операции по шифрованию трафика выполняются ускорителем, обработка открытого трафика выполняется CPU системы.
- Встроенный watchdog обеспечивает автоматическую перезагрузку системы в случае программного сбоя.
- Поддержка смарт карт с целью хранения ключей.

Производительность – около 120 Мбит/с

ViPNet TURBO 100 – криптоускоритель, который может использоваться ViPNet Coordinator, ViPNet Client.



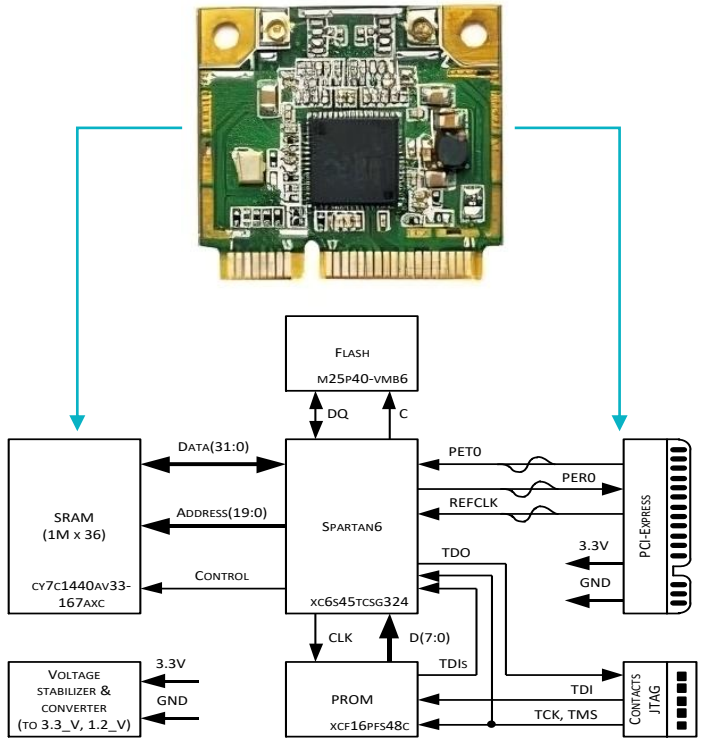
ViPNet Solo

Portable FW/VPN appliance

1. VPN
2. Firewall
3. Crypto storage
4. Apps

Криптоускоритель 1G

- Аппаратный модуль предназначенный для шифрования ip-трафика на скорости до 1 Гбит/с.
- Основная цель – снизить нагрузку на CPU
  - Ver. 1.0:
    Скорость шифрования до 1G.
  - Ver. 2.0.
    Скорость шифрования до 10G.
    Ver. 3.0.
  - Скорость шифрования до 10-40G.
- Алгоритм ГОСТ 28147-89
- Совместим с HW



VPN L2 vs L3

VPN L2 vs L3

L2

- Пропускная способность порядка 90% от ширины канала для минимального размера кадра
- Размер заголовка VPN не превышает 20 байт
- Задержка составляет микросекунды
- Подходит для любых типов L3 протоколов

L3

- Пропускная способность порядка 5-10% от ширины канала для минимального размера пакета
- Размер заголовка VPN может составлять до 40% от общего размера пакета
- Задержка составляет порядка 100 миллисекунд
- Важен тип L3 протокола (Ipv4, IPv6,TCP/IP, IPX/SPX…)

ViPNet L2-10G

ViPNet L2-10G

- Класс СКЗИ– **КВ**
- Точка-Точка
- Прием и передачу данных по протоколу Ethernet 10GBASE (в соответствии со стандартом IEEE 802.3ae) с поддержкой Jumbo Frame.
- Обработку Ethernet-кадров размером от 64 до 8988 байт.
- Шифрование и имитозащиту данных с использованием криптографических алгоритмов, регламентированных ГОСТ Р 34.12–2015 и ГОСТ Р 34.13-2015.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер **СФ/124-4266** от "**20**" **мая** 2022 г.

Действителен до "**01**" **июня** 2024 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы», Обществу с ограниченной ответственностью «Линия защиты».

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс **ViPNet L2-10G** в комплектации согласно формуляру ФРКЕ.466288.001 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КВ и может использоваться для криптографической защиты (шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»
сертификационных испытаний образцов продукции №№ 981-000501, 981-000502.

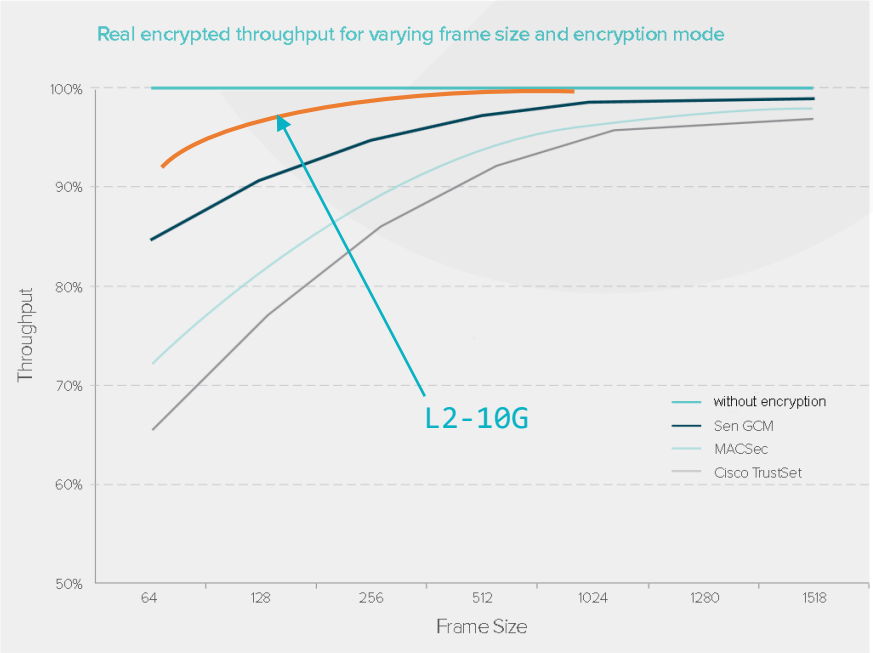
Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.466288.001 ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.466288.001 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России

СКЗИ класса КВ

Ведутся работы по сертификации 2 поколения. О нем информация позже.

Производительность



Производительность:

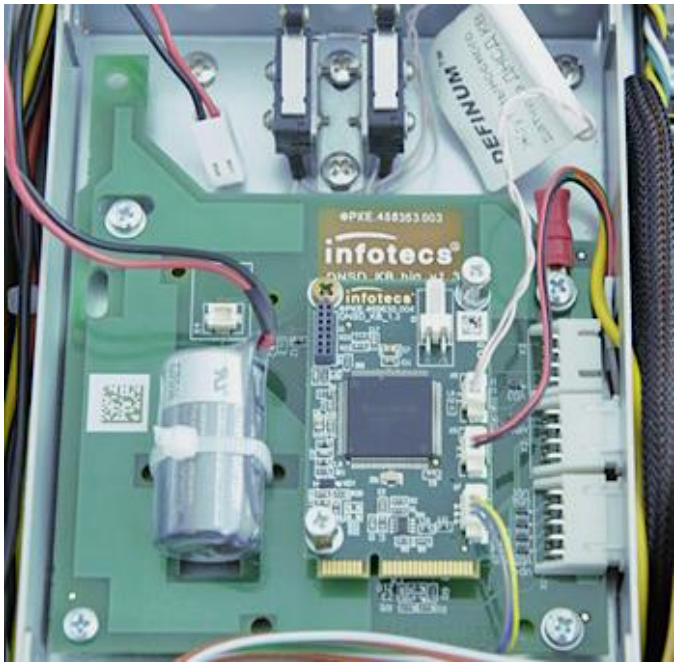
- Скорость шифрования Ethernet кадров размером 110 байт, полудуплекс – до 7,6 Гбит/с.
- Скорость шифрования Ethernet кадров размером 110 байт, полный дуплекс – до 15,2 Гбит/с.
- Скорость шифрования Ethernet кадров размером 1453 байт, полудуплекс – 9,7 Гбит/с.
- Скорость шифрования Ethernet кадров размером 1453 байт, полный дуплекс – 19,5 Гбит/с.

Сверхнизкая задержка:

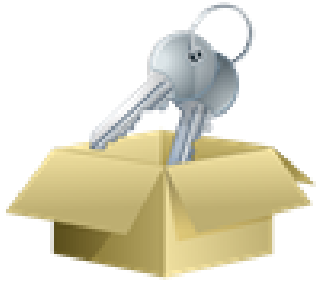
- L2-10G – менее **3 ms (микросекунд)**

ДНСД – датчик от несанкционированного доступа

- Защита от физического вскрытия
- Защита ключей: хранение и уничтожение
- Контроль целостности ПО ПАК



Генерация и ввод ключей



ключевые блокноты ДСДР-i, изготавливаемые в/ч *****

Роль «L2-10G»

ViPNet Administrator

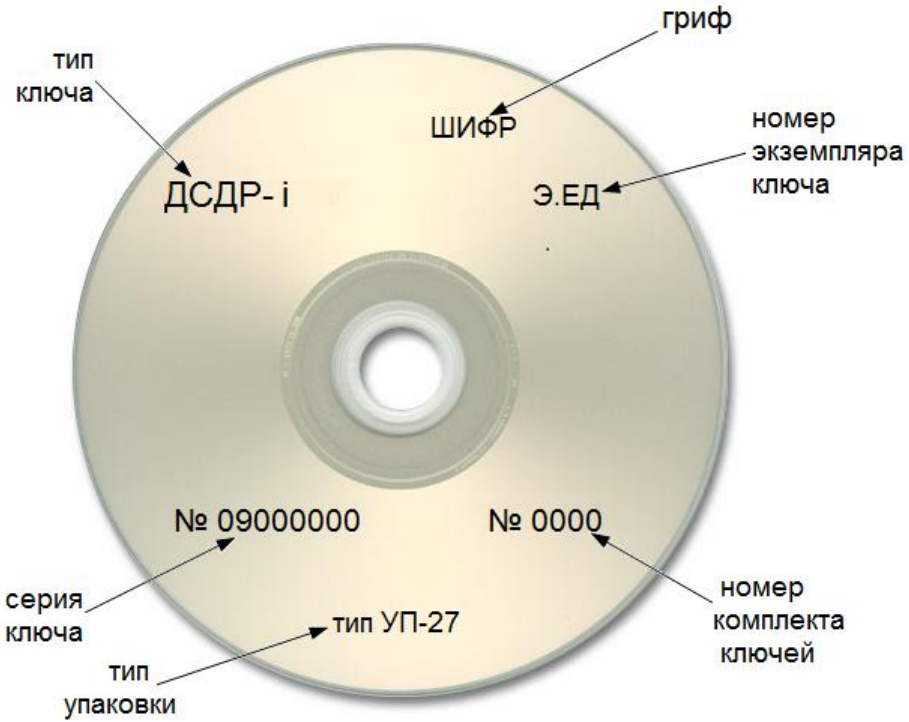
Регистрация ДСДР-I в УКЦ

Генерация ДСТ

Переносим на токен персональный ключ

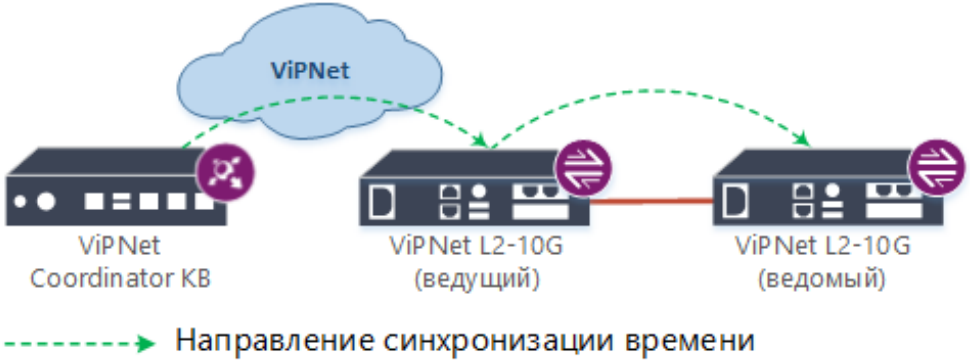
Распаковка ДСТ

Установка ключа ДСДР-i



Ключевой диск ДСДР-i

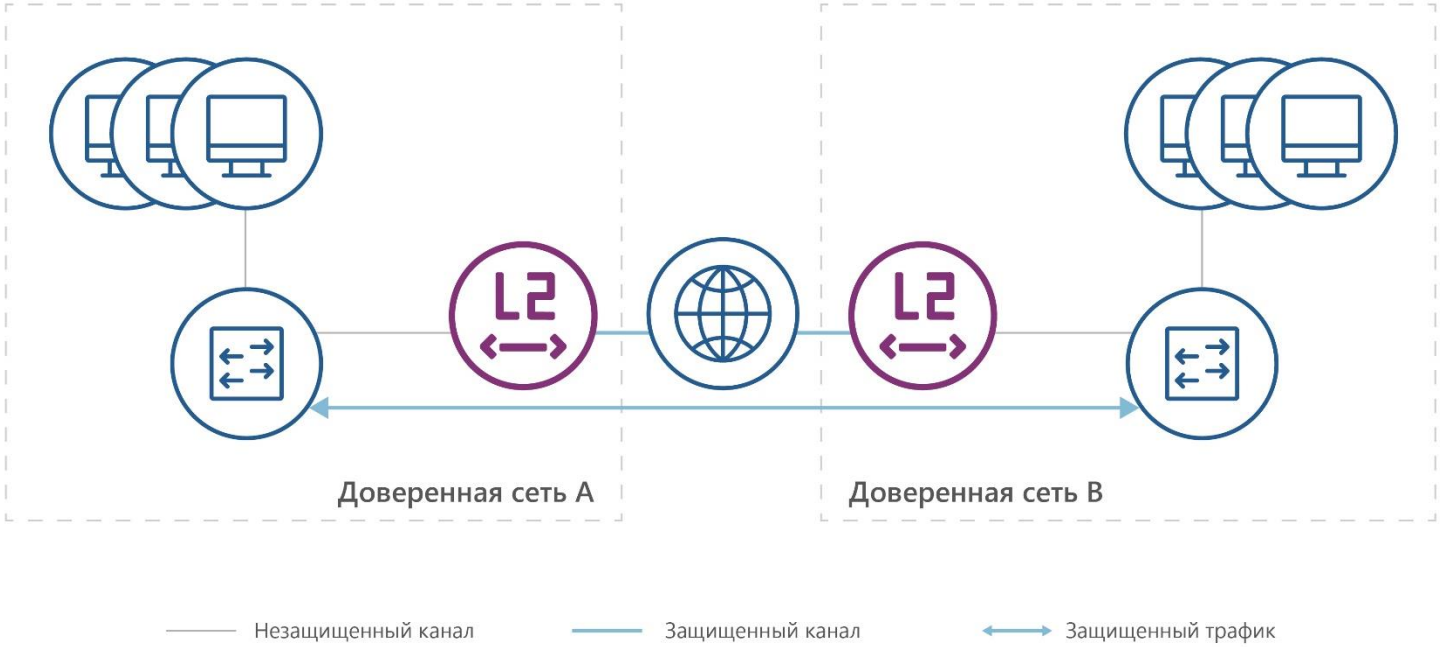
Синхронизация времени



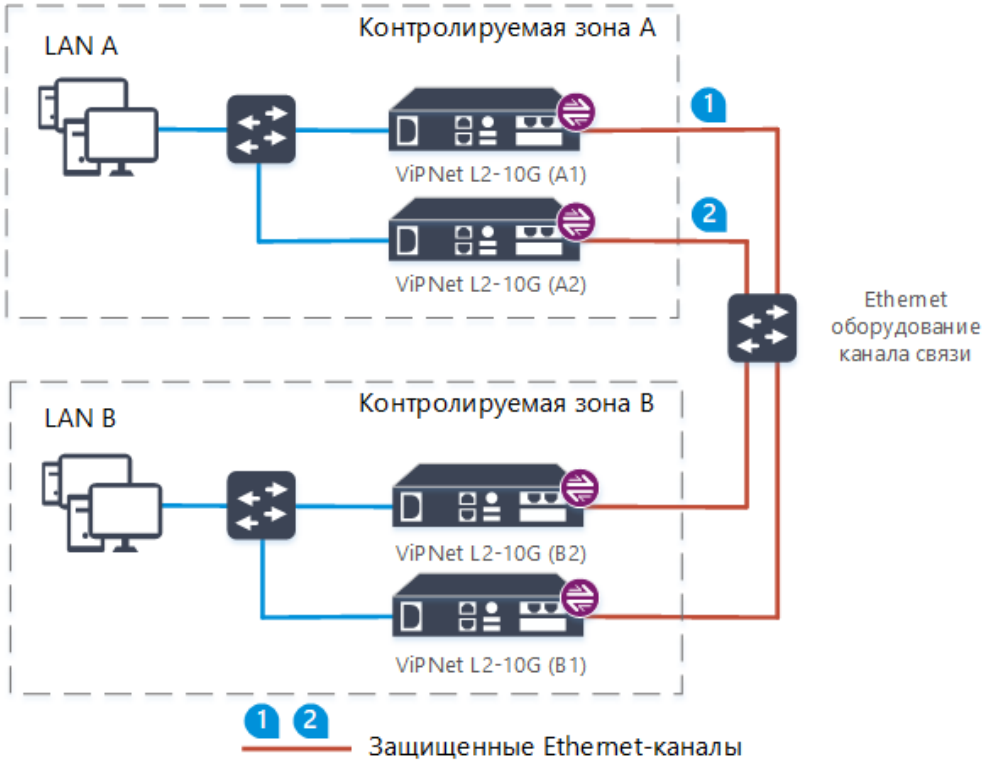
Внимание! Для синхронизации времени допустимо использовать только доверенные NTP-серверы из защищенной сети ViPNet. В качестве такого сервера может использоваться координатор ViPNet Coordinator KB либо другой узел ViPNet L2-10G.

Типовой сценарий использования службы времени NTP для синхронизации времени между сопряженными ViPNet L2-10G предусматривает их настройку в режиме ведущий-ведомый.

Сценарий использования



Резервирование каналов связи



Режим резервирования: один из защищенных каналов является основным, а второй – резервным, подключаемым при отказе основного. Реализуется с использованием протоколов резервирования, таких как STP, RSTP, MSTP и др.

Режим балансировки нагрузки: задействуются оба транспортных канала при помощи балансировщика нагрузки и технологии агрегации каналов, например LAG, LACP, bounding и пр.

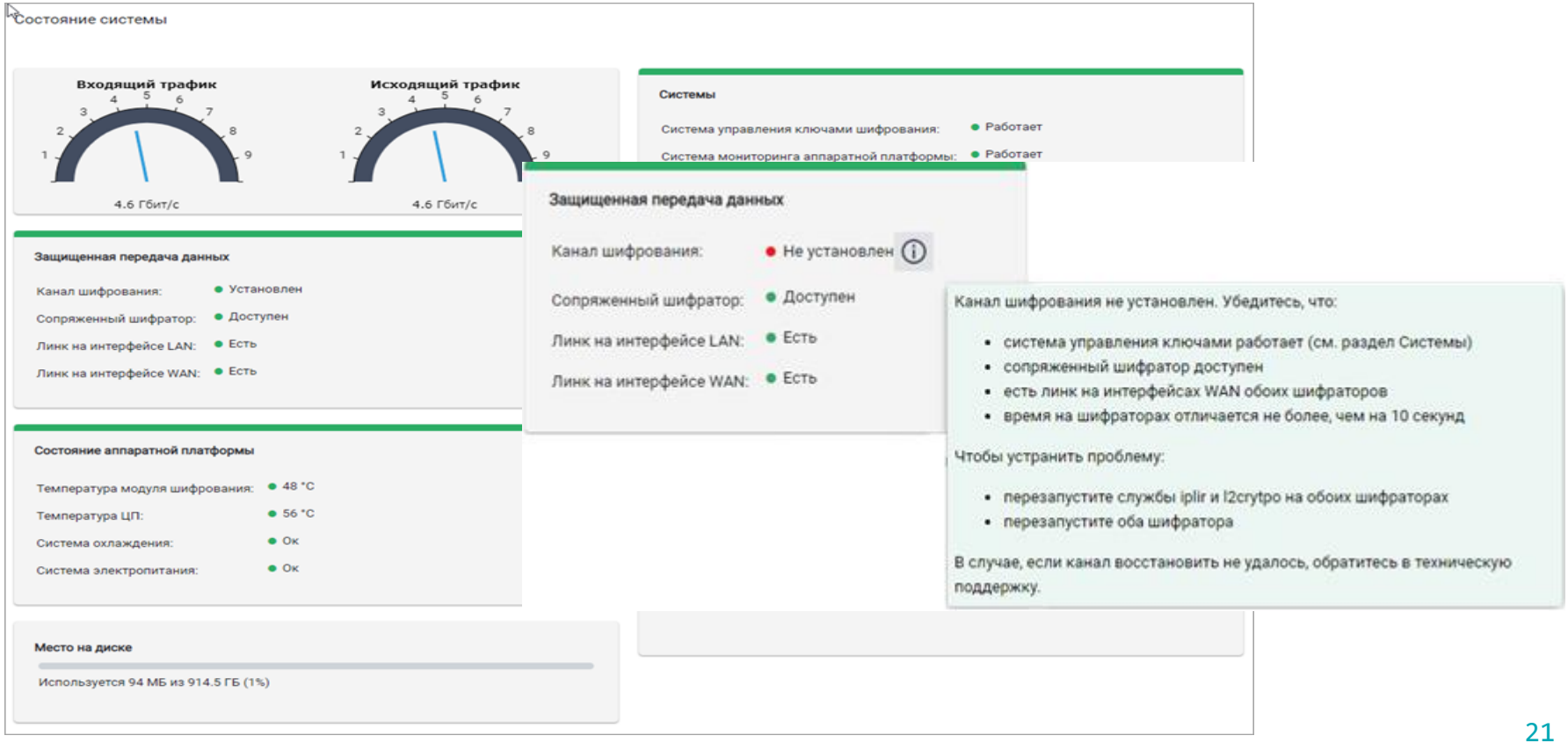
ТехноФест 2023 infotecs

L2-10G
версия 2.0.0

Что нового

- Поддержка новой аппаратной платформы
- Автоматическая смена блокнота ДСДР ViPNet L2-10G
- Веб-интерфейс для управления ViPNet L2-10G
- Реализован мониторинг состояния ViPNet L2-10G по протоколу SNMP

Информация о системе



Состояние интерфейсов и канала

```
LAN Interface Link Status:
Yes
LAN Interface SFP+ Info:
Intel Corp FTLX8571D3BCVIT1
Tx1: -2.1 dBm, Rx1: -6.4 dBm (t = 36.7 C)
WAN Interface Link Status:
Yes
WAN Interface SFP+ Info:
Intel Corp AFBR-703SDZ-IN2
Tx1: -2.4 dBm, Rx1: -2.2 dBm (t = 38.7 C)
```

```
hostname> l2crypto info
```

ТЕХНО 2023 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363