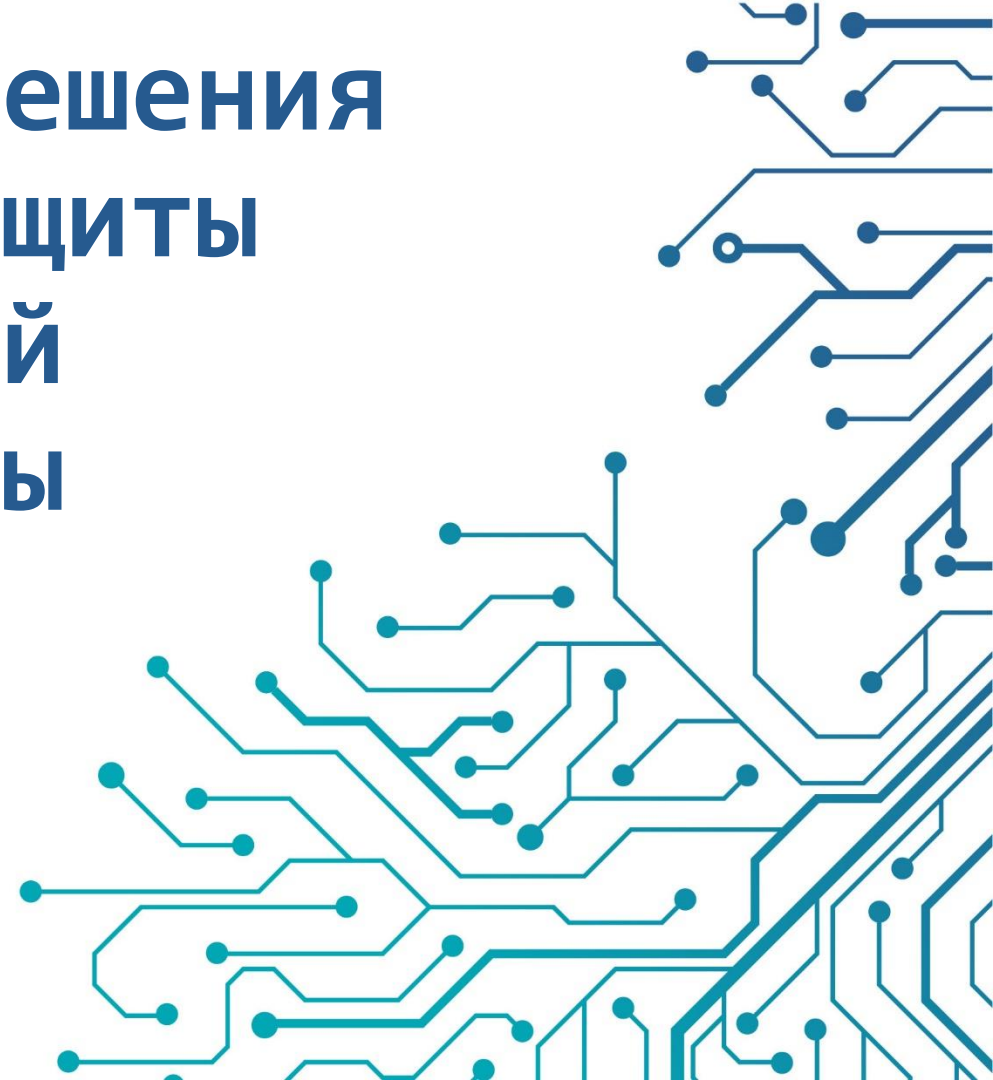
Комплексные решения ViPNet для защиты информационной инфраструктуры организации

Лихацких Иван

infotecs



Нулевое доверие. Иностранные компании?

1. **Межсетевые экраны (NGFW)**
   Fortinet, Cisco, Check Point, Palo Alto…
2. **Защищенный удаленный доступ и защита каналов связи (VPN)**
   Cisco, Check Point, Palo Alto…
3. **Защита порталов/PKI/УЦ**
   SSL/Microsoft CA…
4. **Мессенджеры**
   Slack, WhatsApp…

Что замещаем

- Fortinet
- Cisco
- Check Point
- Palo Alto
- …

Чем замещаем

- NGFW ViPNet xFirewall 5.x
- UTM ViPNet Coordinator HW5

Что такое ViPNet xFirewall

Сетевая платформа в составе:

- Межсетевой экран
- Сетевой экран приложений - DPI
- Система предотвращения вторжений
- Шлюзовой антивирус
- Интеграция с Active Directory

Производительность

Кто, как и что считает?

Устройство №1

Пропускная способность МЭ, UDP: **до 18 Гб/с**

МЭ, трафик EMIX: **до 18 Гб/с**

МЭ с DPI: **до 15 ГБит/с**

Устройство №2

Пропускная способность МЭ, UDP: **до 20 Гб/с**

МЭ, трафик EMIX: **до 22 Гб/с**

МЭ с DPI, EMIX: **до 18,7 Гбит/с**

Устройство №3

Пропускная способность МЭ, UDP: **до 60 Гб/с**

МЭ, трафик EMIX: **до 40 Гб/с**

МЭ с DPI, EMIX: **до 40 Гбит/с**

Реальность

Реальный трафик Заказчика включенный МЭ, DPI, IPS ViPNet, UserGate, Континент

около 2,3 .. 2,4 Гбит/с

Доверие к заявленному функционалу

SSL инспекция

Алгоритм работы:

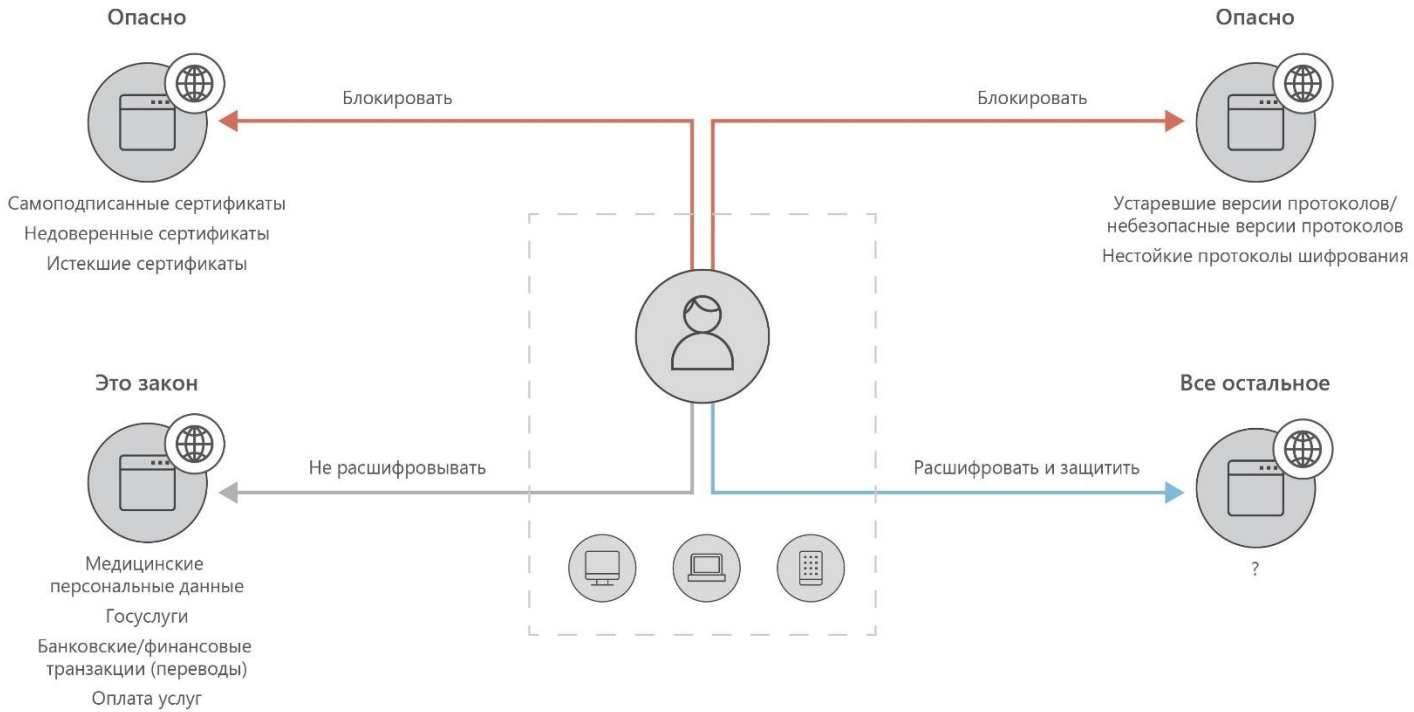
1. Расшифровка SSL трафика
2. Определение угрозы
3. Блокировка угрозы

Реальность

Алгоритм работы:

1. Расшифровка SSL трафика
2. А надо было?
3. А надо было?

Лучшие практики SSL Inspection



Доверие к базам решающих правил (БРП)

infotecs

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

Февраль 2022 – отключение иностранных сервисов обновления БРП

Snort / Suricata / антивирус

- Движок IDS/IPS?
- Используемые сигнатуры для IDS/IPS?
- Кол-во сигнатур IDS/IPS?
- Используемый антивирус?
- Кол-во антивирусных баз?

Реальность

АО «Перспективный мониторинг» (ГК ИнфоТеКС):

Advanced Monitoring - AM

Более **17 000** собственных AM-сигнатур

ViPNet Coordinator HW 5 – сертифицирован ФСБ и ФСТЭК

infotecs

Firewall
- МЭ с контролем состояния сессий (SPI)
- Контроль приложений (DPI)
- Прокси-сервер
- Идентификация пользователей (AD/LDAP)

VPN
- L3 VPN
- L2OverIP VPN
- Remote Access VPN
- Новые алгоритмы ГОСТ 34.12-2018 ГОСТ 34.13-2018

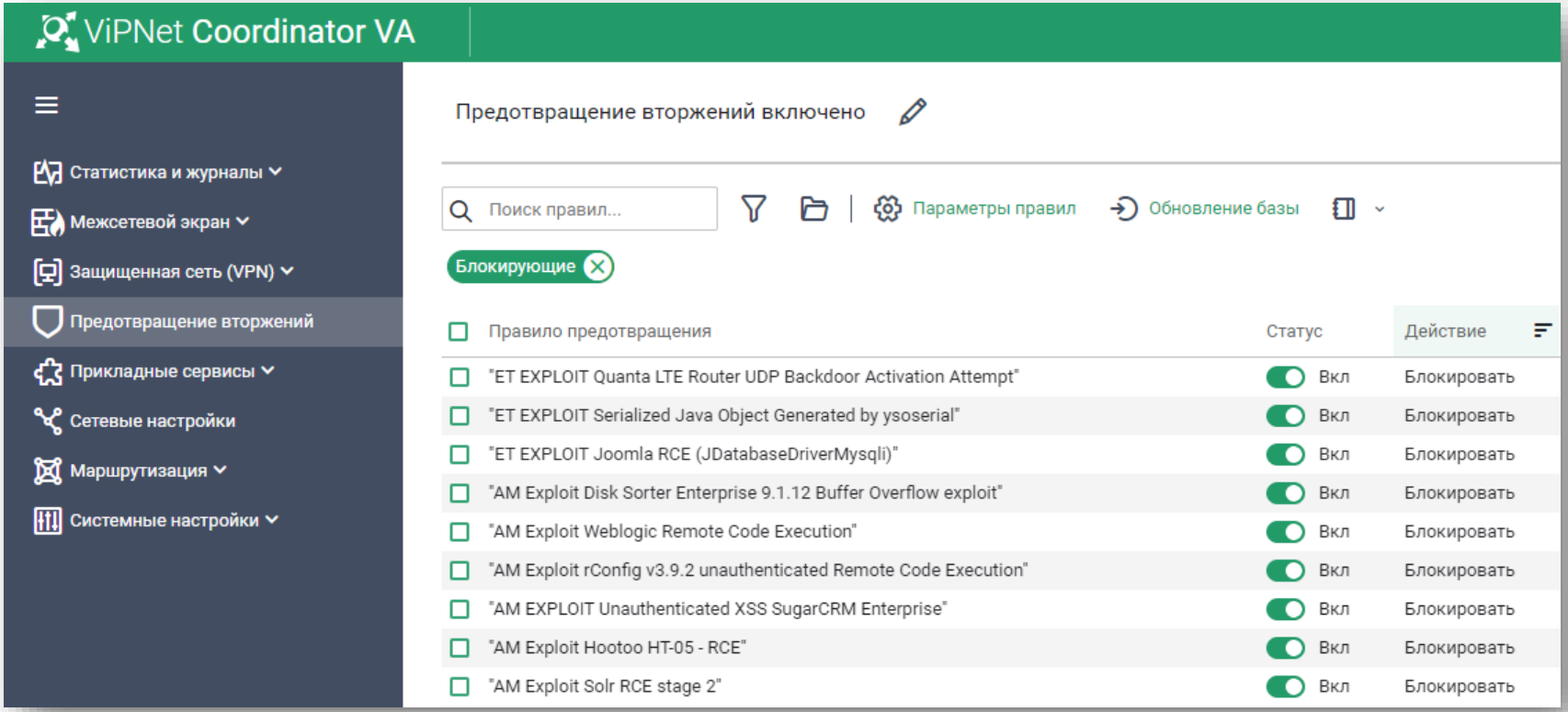
IPS
- IPS/IDS

Failover
- HA Cluster (active/passive)

Антивирус
- Любой внешний ICAP

Прочее
- Ролевая модель доступа
- Централизованное резервное копирование
- Captive Portal
- Лицензирование отдельных сервисов

Предотвращение вторжений



Требования по сертификации

ФСБ России

- ✓ СКЗИ класса КС1-КС3
- ○ Межсетевой экран 4 класса – в процессе получения

ФСТЭК России

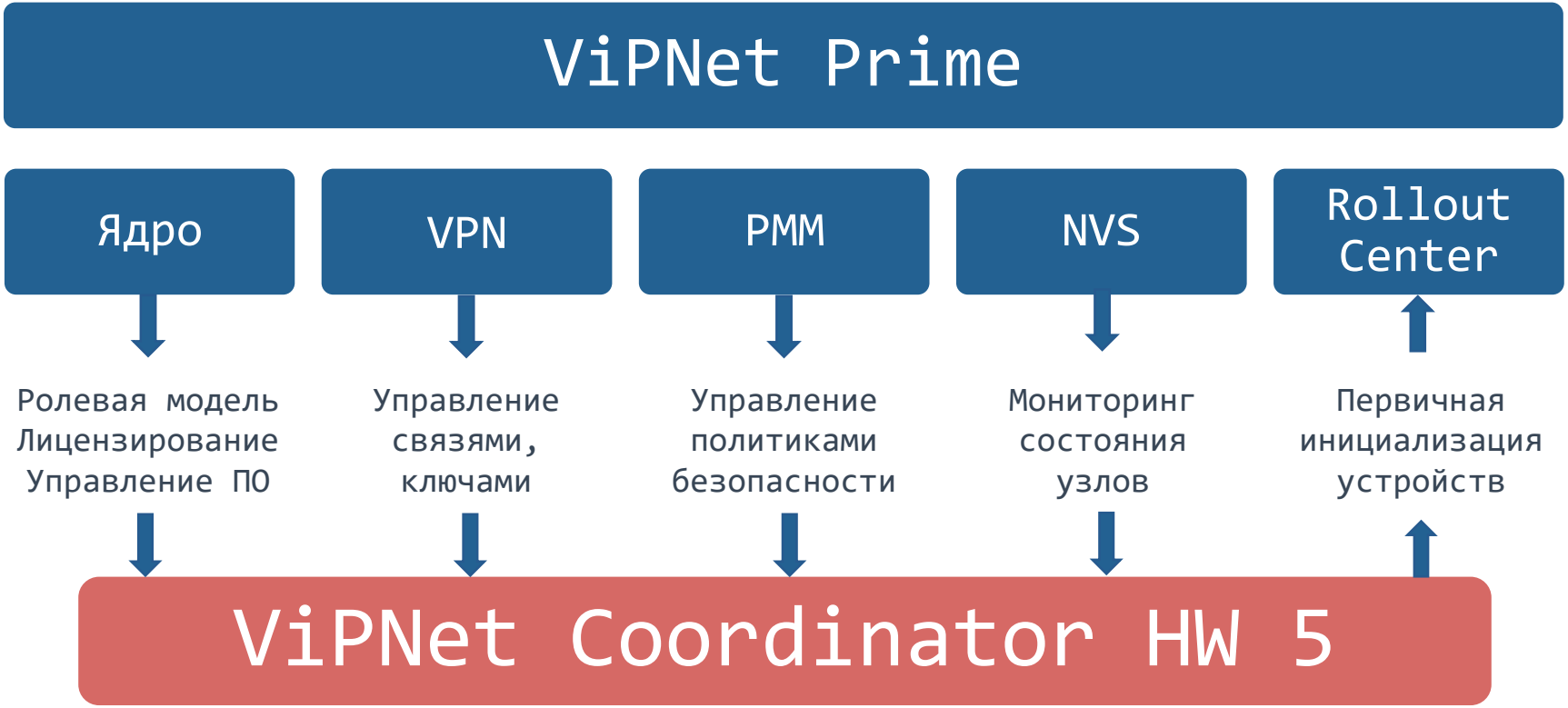
- ✓ Межсетевой экран тип «А» и тип «Б» 4 класса
- ✓ СОВ уровня сети 4 класса
- ✓ 4-й уровень доверия средств защиты информации
- ○ Многофункциональный межсетевой экран уровня сети NEW

Минцифры России и Минпромторг России

- ✓ В реестре российского ПО и реестре российской продукции

Типовая схема применения HW 5

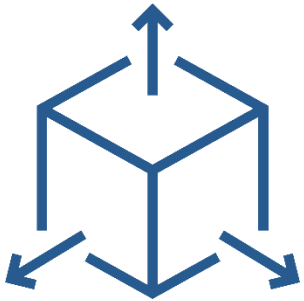
Модули ViPNet Prime



Криптография (VPN)

- «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- ГОСТ 28147-89 для обратной совместимости
- IPlir 6 – протокол безопасности сетевого уровня

ТК 26 Р 1323565.1.034-2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня»



Комплексная защита рабочих станций

ViPNet SafeBoot 3

ViPNet Client 4U

ViPNet SafePoint

ViPNet EndPoint Protection

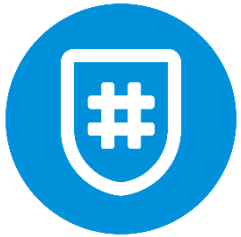
ViPNet SafeBoot 3 – два исполнения

- **Исполнение 1.** ViPNet SafeBoot 3 – обладает двумя сертификатами ФСБ России и ФСТЭК России.

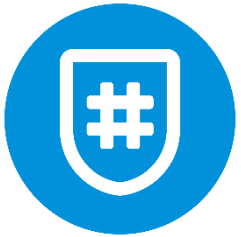
Необходим, при построении систем СКЗИ и соответствовать требованиям ГИС, ИСПДн, АСУ ТП, КИИ.

- **Исполнение 2.** ViPNet SafeBoot 3 – обладает – только сертификатом ФСТЭК России

Необходим, при построении АС только по требованиям ФСТЭК



Похожи как братья близнецы, но есть особенности



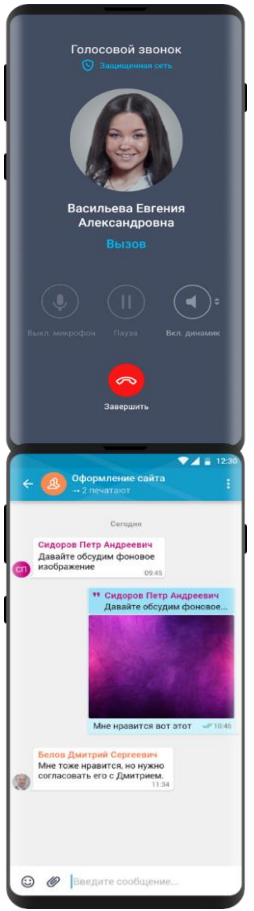
ViPNet SafePoint

ViPNet SafePoint – сертифицированный программный комплекс защиты информации от несанкционированного доступа уровня ядра операционной системы (ОС).

ViPNet SafePoint устанавливается на рабочие станции и серверы в целях обеспечения мандатного и дискреционного разграничения доступа пользователей к критически важной информации и подключаемым устройствам.

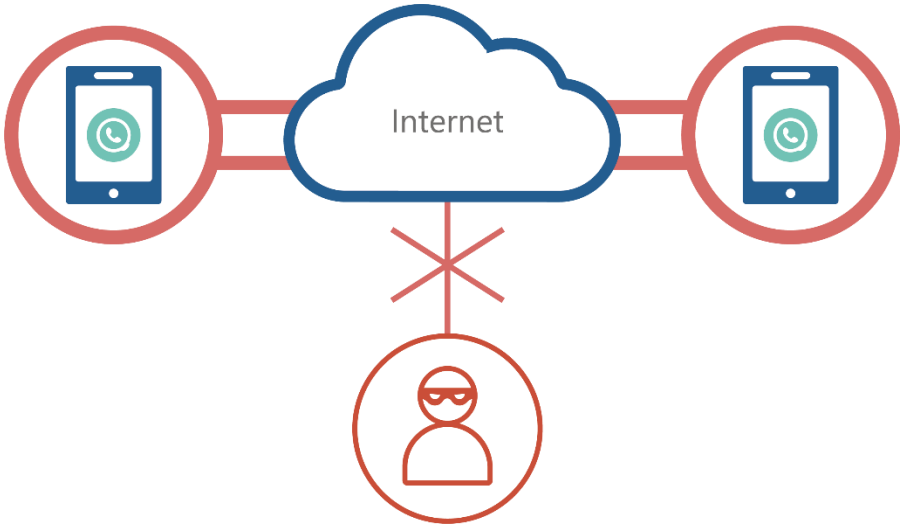
ViPNet CSS Connect. Что это?

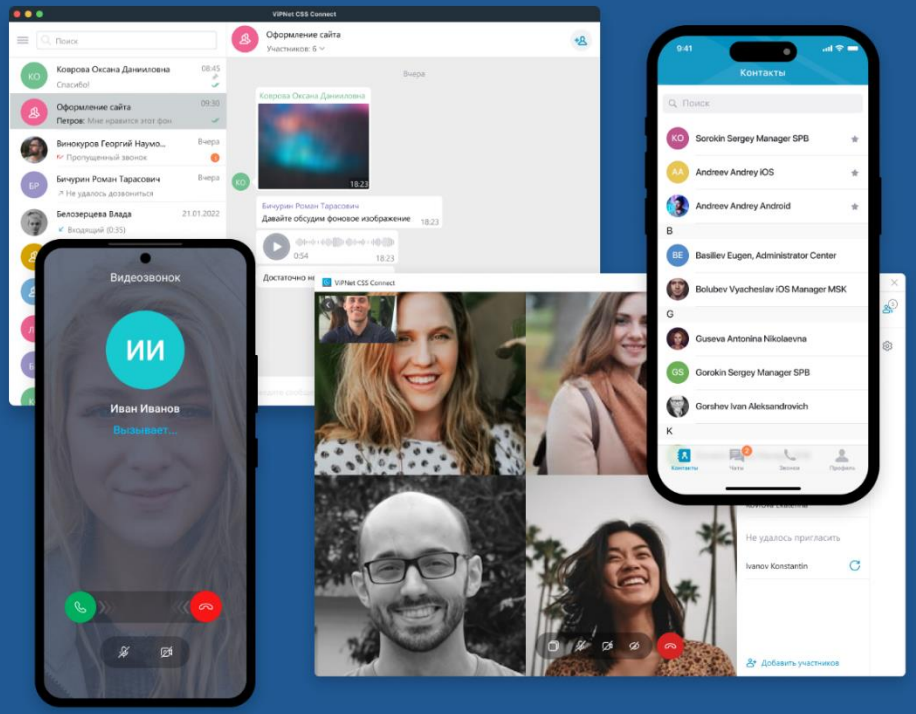
Изолированная система для организации **защищенного контура** корпоративных коммуникаций



Абонентское шифрование точка-точка

Все коммуникации осуществляются по **защищенным каналам связи**, в том числе при передаче в **локальной сети**, что **исключает** возможность **перехвата** защищаемой информации как внешними, так и внутренними нарушителями

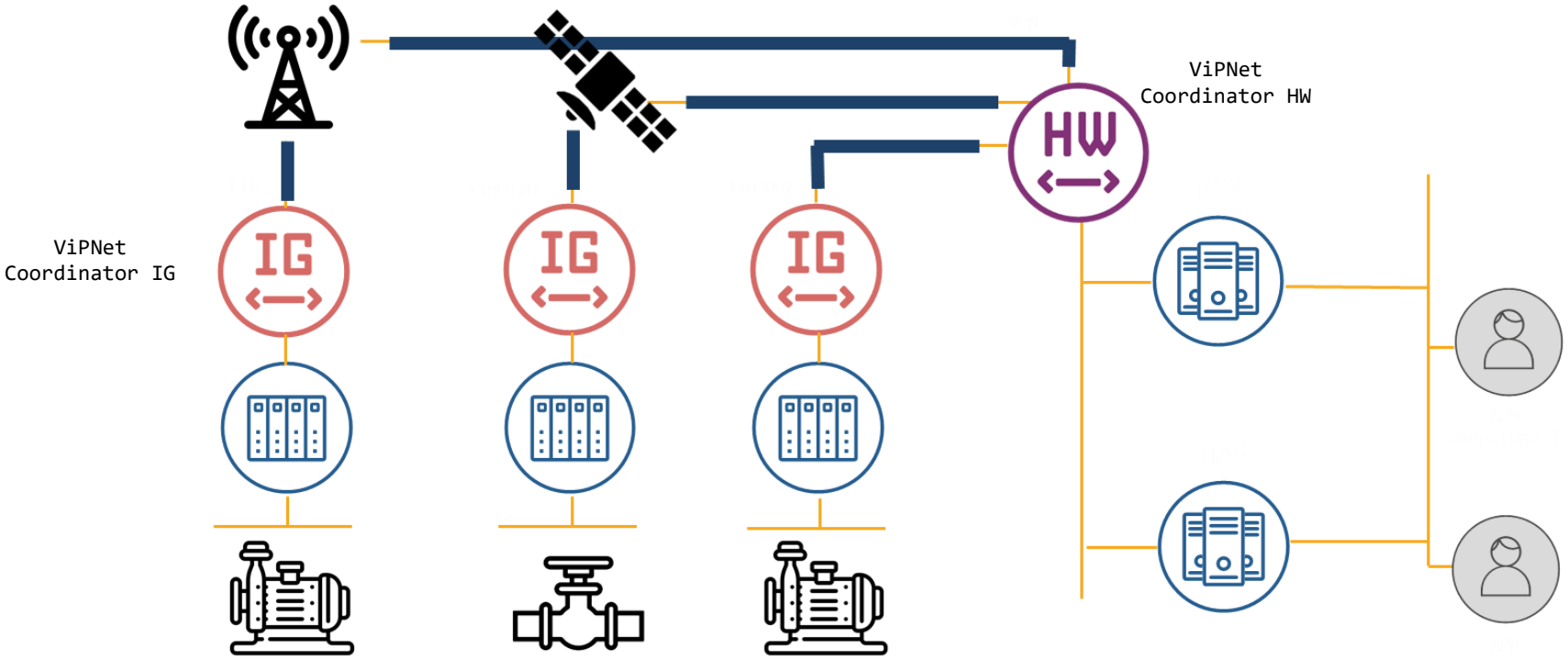




ViPNet CSS Connect возможности

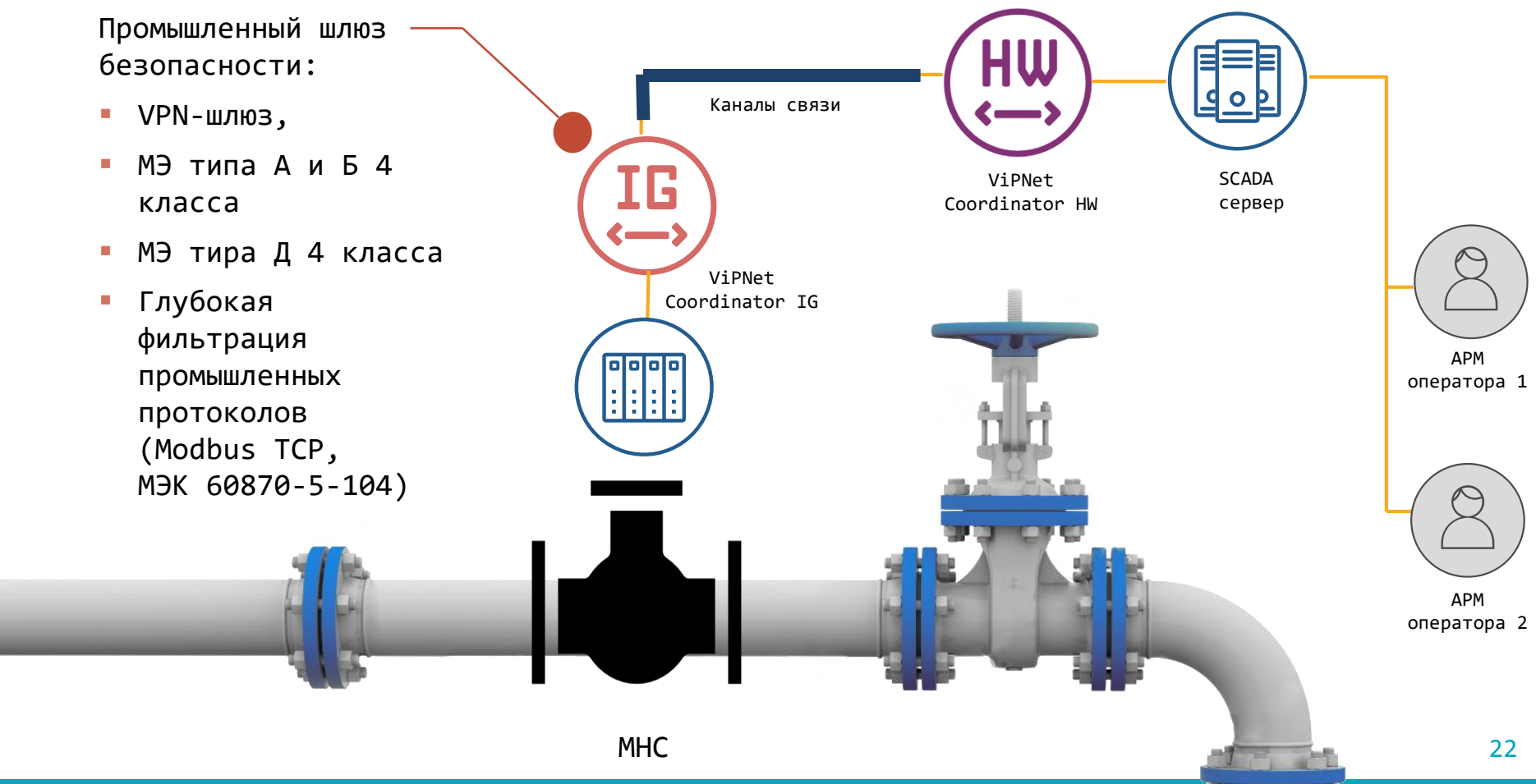
ViPNet CSS Connect обеспечивает голосовые коммуникации, видеосвязь, отправку текстовых сообщений и файлов со стационарных компьютеров, ноутбуков и мобильных устройств, а также интеграцию **с SIP телефонией и ВКС**.

VPN для распределенных систем

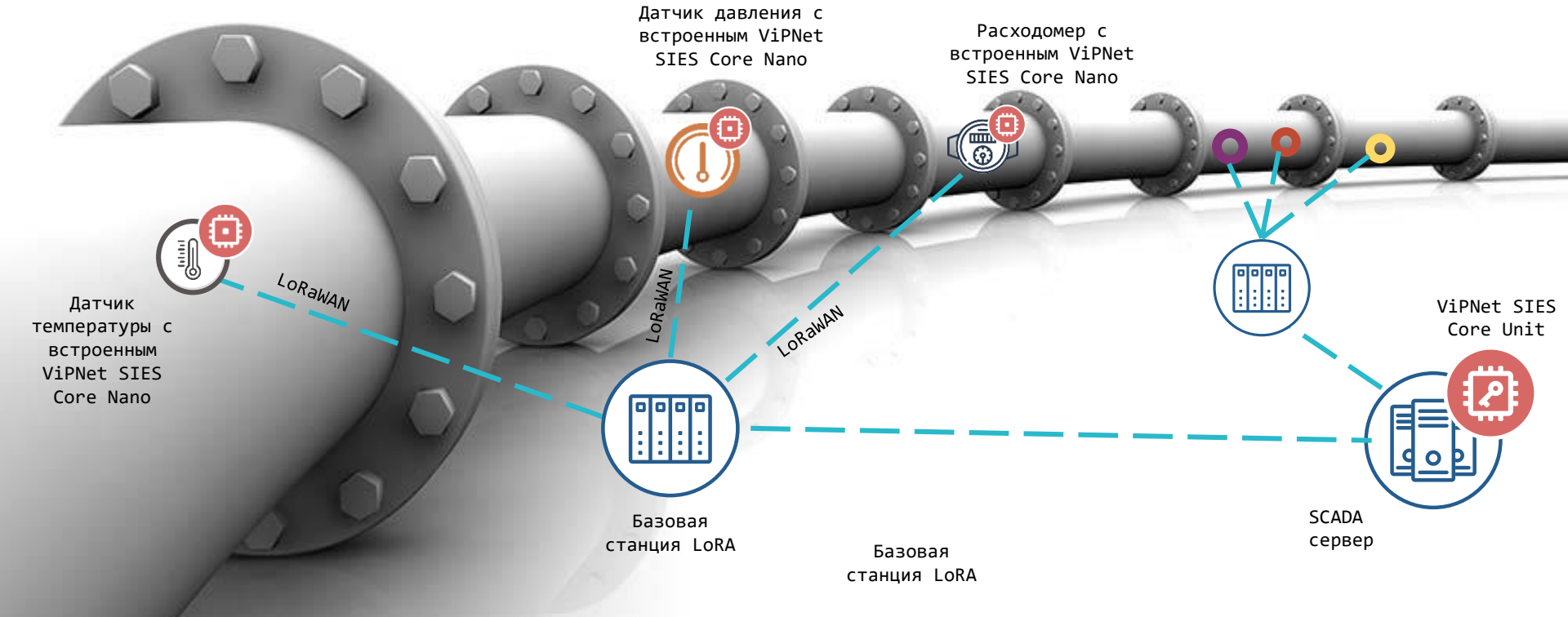


Промышленный шлюз безопасности:

- VPN-шлюз,
- МЭ типа А и Б 4 класса
- МЭ тира Д 4 класса
- Глубокая фильтрация промышленных протоколов (Modbus TCP, МЭК 60870-5-104)

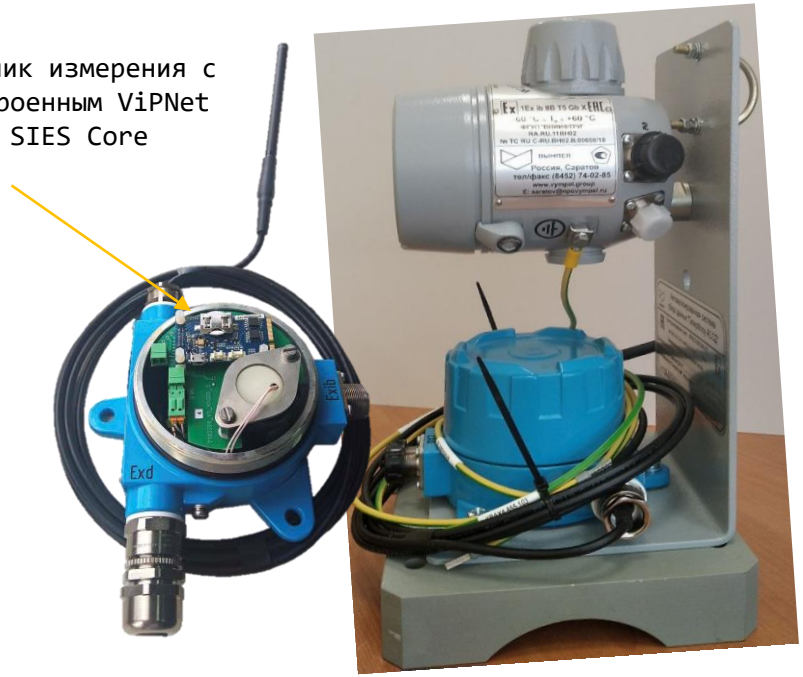


Автоматизированная система сбора данных с трубопровода



Автоматизированная система сбора данных с трубопровода

Датчик измерения с встроенным ViPNet SIES Core



Датчик измерения параметров с встроенным ViPNet SIES Core Nano

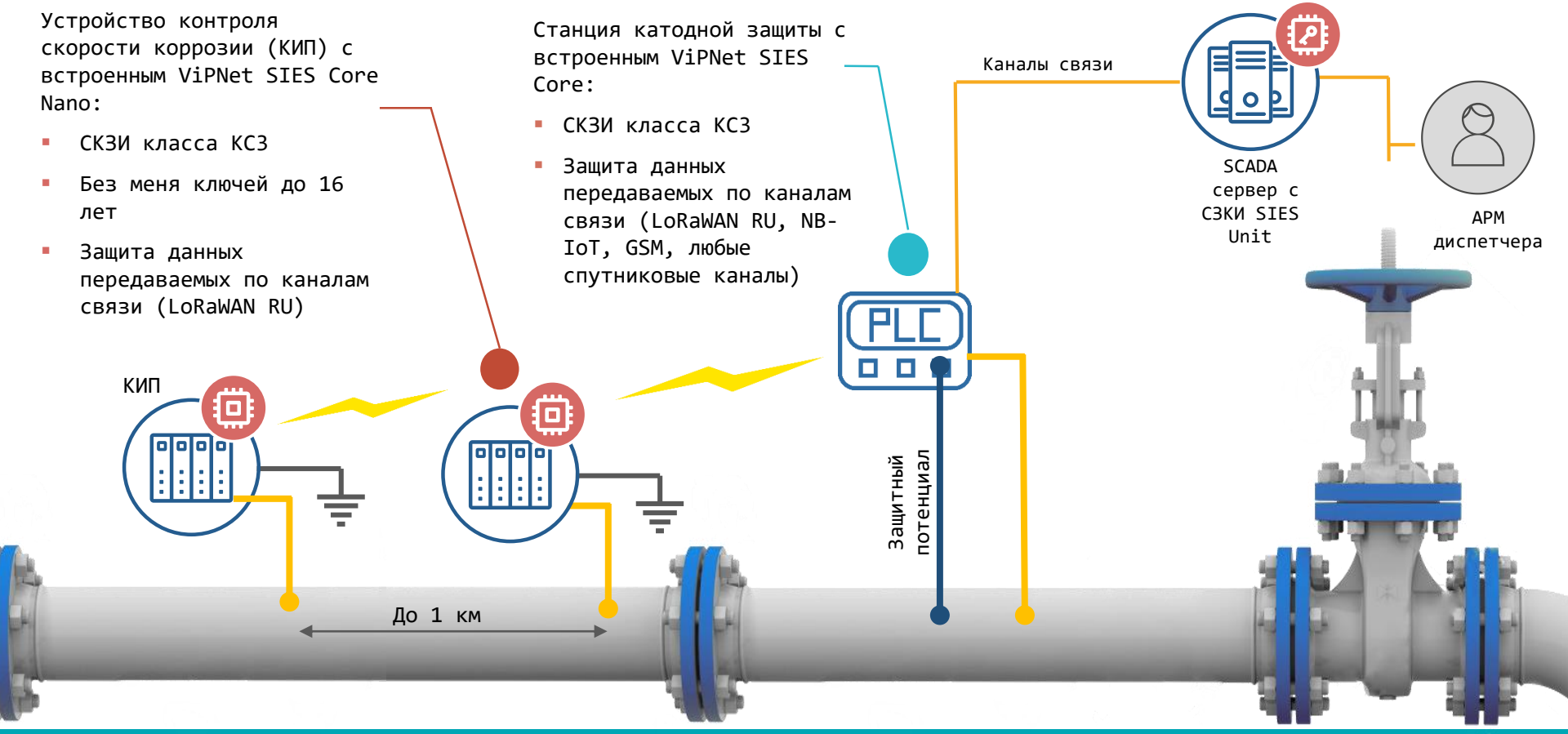
Система коррозионной защиты

Устройство контроля скорости коррозии (КИП) с встроенным ViPNet SIES Core Nano:

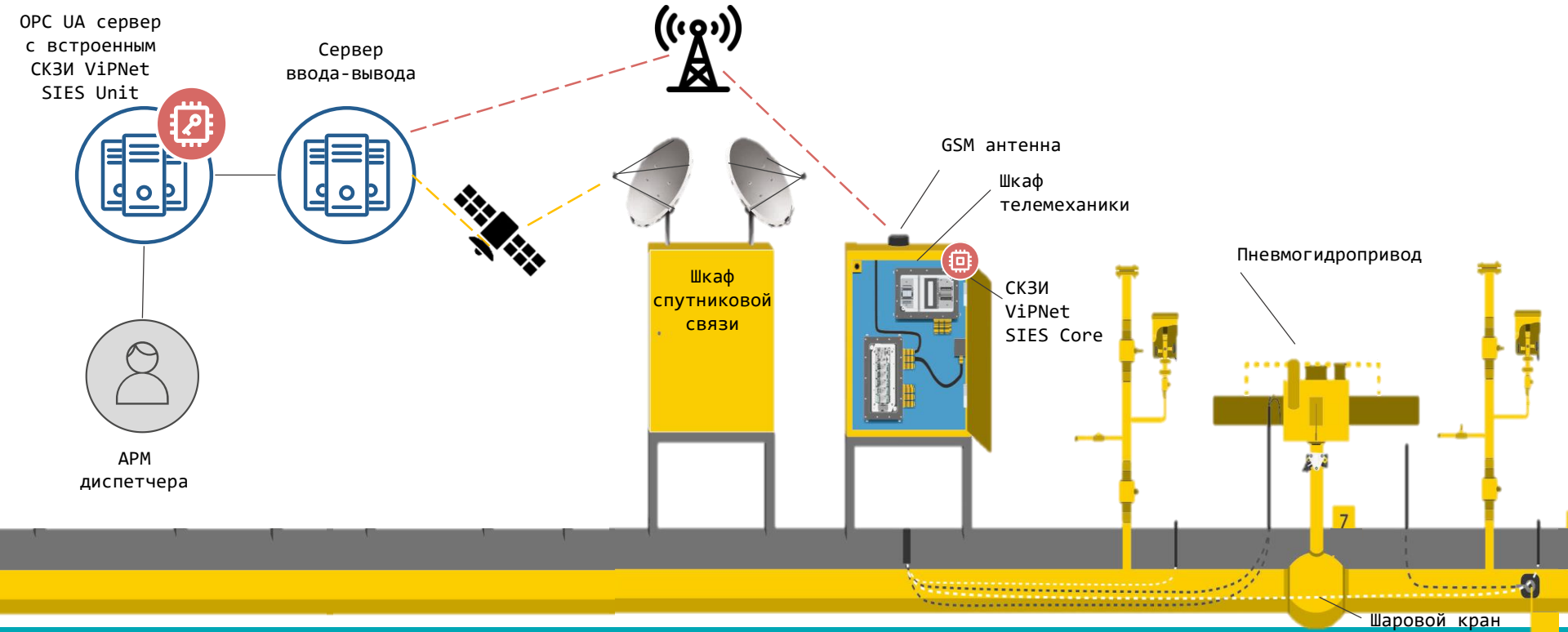
- СКЗИ класса КС3
- Без меня ключей до 16 лет
- Защита данных передаваемых по каналам связи (LoRaWAN RU)

Станция катодной защиты с встроенным ViPNet SIES Core:

- СКЗИ класса КС3
- Защита данных передаваемых по каналам связи (LoRaWAN RU, NB-IoT, GSM, любые спутниковые каналы)

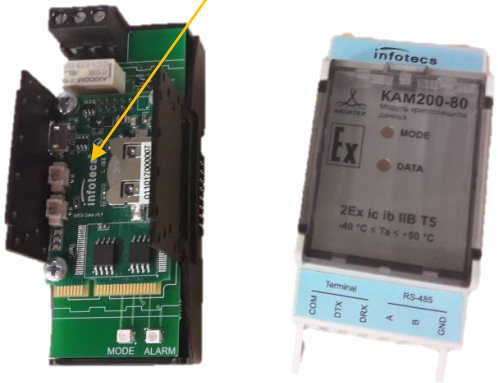


Система телеметрического контроля и телемеханизации



Система телеметрического контроля и телемеханизации

Коммуникационный модуль с встроенный СКЗИ ViPNet SIES Core



Спасибо за внимание!

Иван Лихацких
lin@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363