Первый российский криптошлюз и межсетевой экран с PoE

Андрей Иванов
Иван Герасименко

infotecs

infotecs

ViPNet Coordinator IG

Индустриальный шлюз безопасности

Предназначен для:

- защиты периметра информационной и промышленной сети
- организации демилитаризованной зоны
- сегментирования сети и разграничения доступа
- организации управления сетевыми потоками
- сокрытия реальных адресов и архитектуры сети
- организации защищенного канала связи для распределенных систем
- организации защищенного удаленного доступа, в том числе с мобильных устройств

Функционал

- Защищенная сеть ViPNet
- Wi-Fi-модуль
- GSM-модуль
- Межсетевой экран + DPI протоколов Modbus и IEC 104
- Шлюз Modbus
- Коммутатор и маршрутизатор
- Отказоустойчивость
- Мониторинг состояния

Криптографическая защита
с использованием алгоритмов ГОСТ

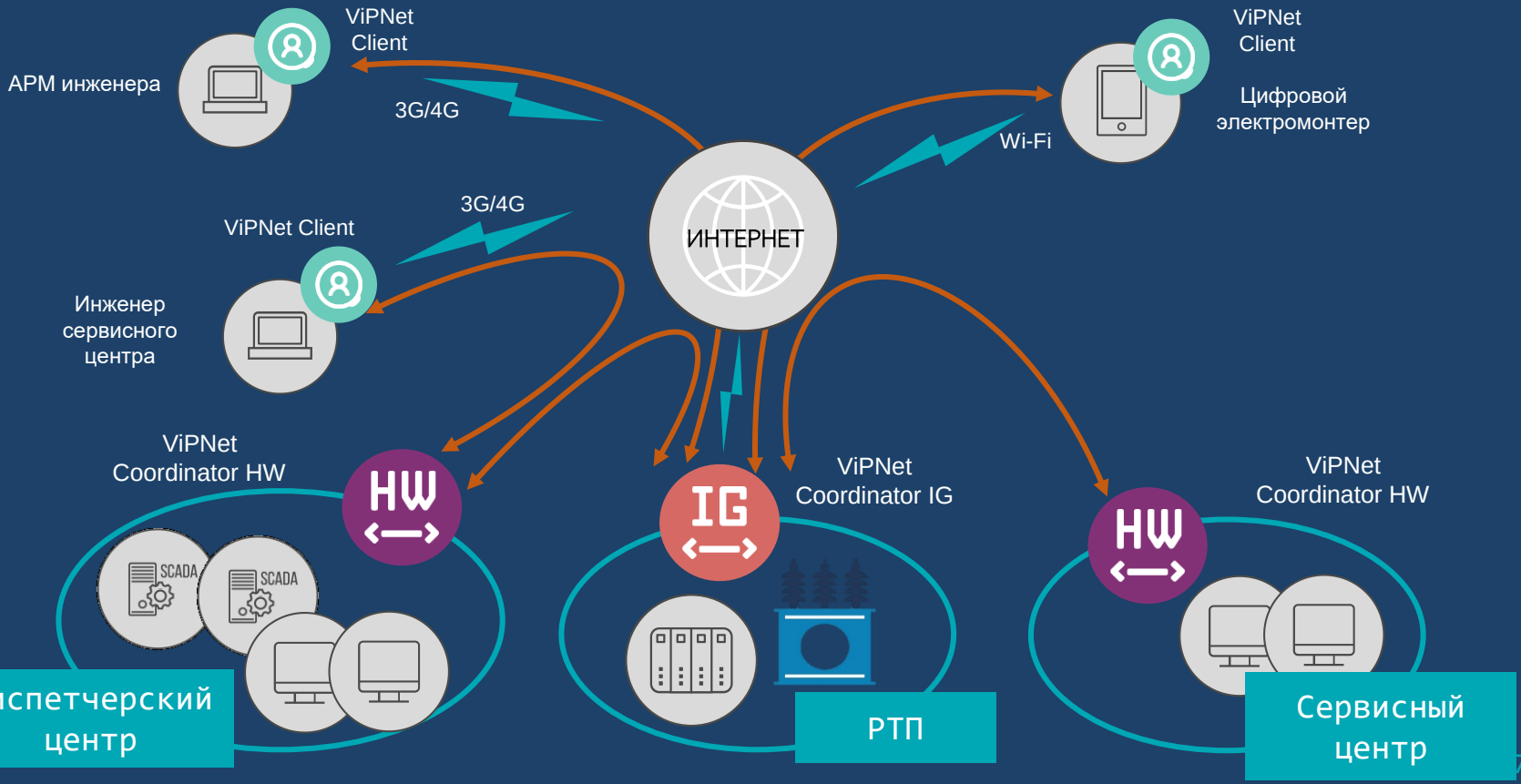
- каналов передачи данных:
  - между АСУ, в т.ч. их сегментами
  - при подключении к сетям связи общего пользования
- доступа удаленных и мобильных пользователей
- удаленного мониторинга
- подключения для сервисного обслуживания

Соответствие требованиям ФСБ России
к СКЗИ класса КС3

Защищенная сеть ViPNet

- Защита каналов передачи данных между АСУ и/или сегментами
- Передача информации по каналам связи общего пользования
- Централизованная настройка сети и политик

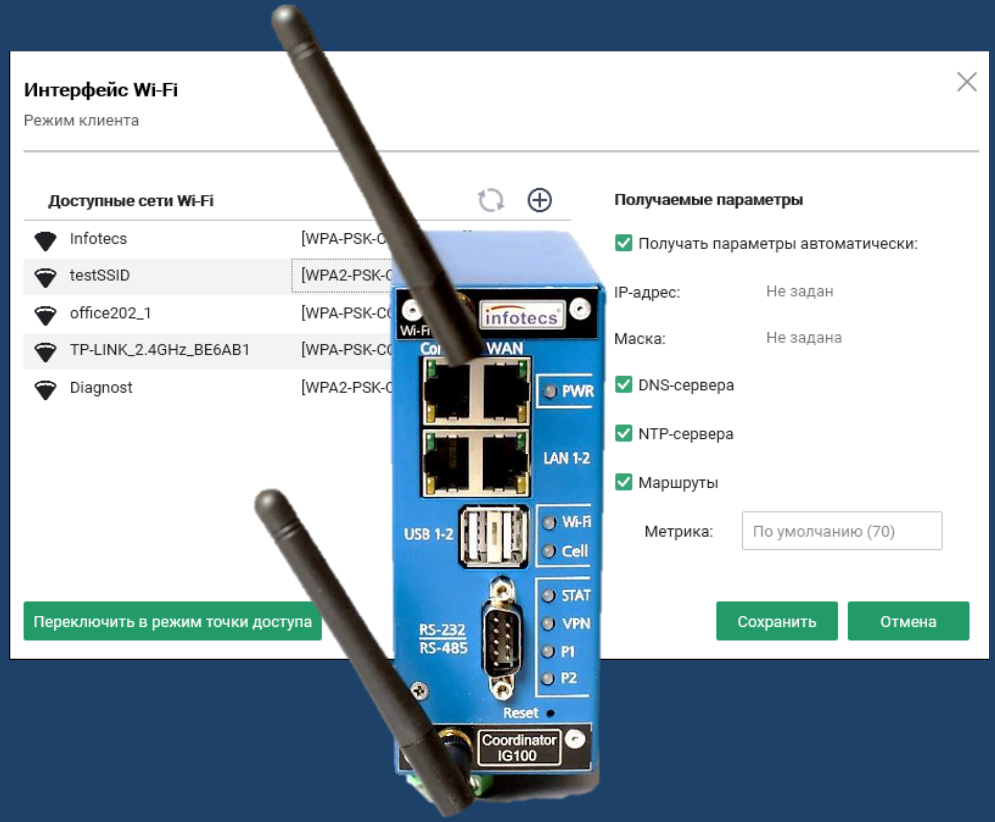
Защищенный удаленный доступ



Wi-Fi

- Клиент
- Точка доступа

Внимание! Wi-Fi модуль устанавливается только на производстве!

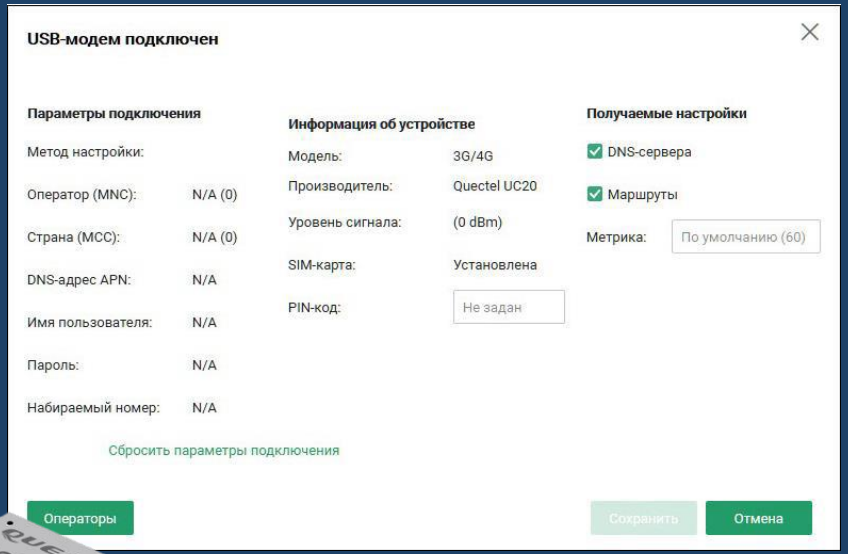


GSM-модуль

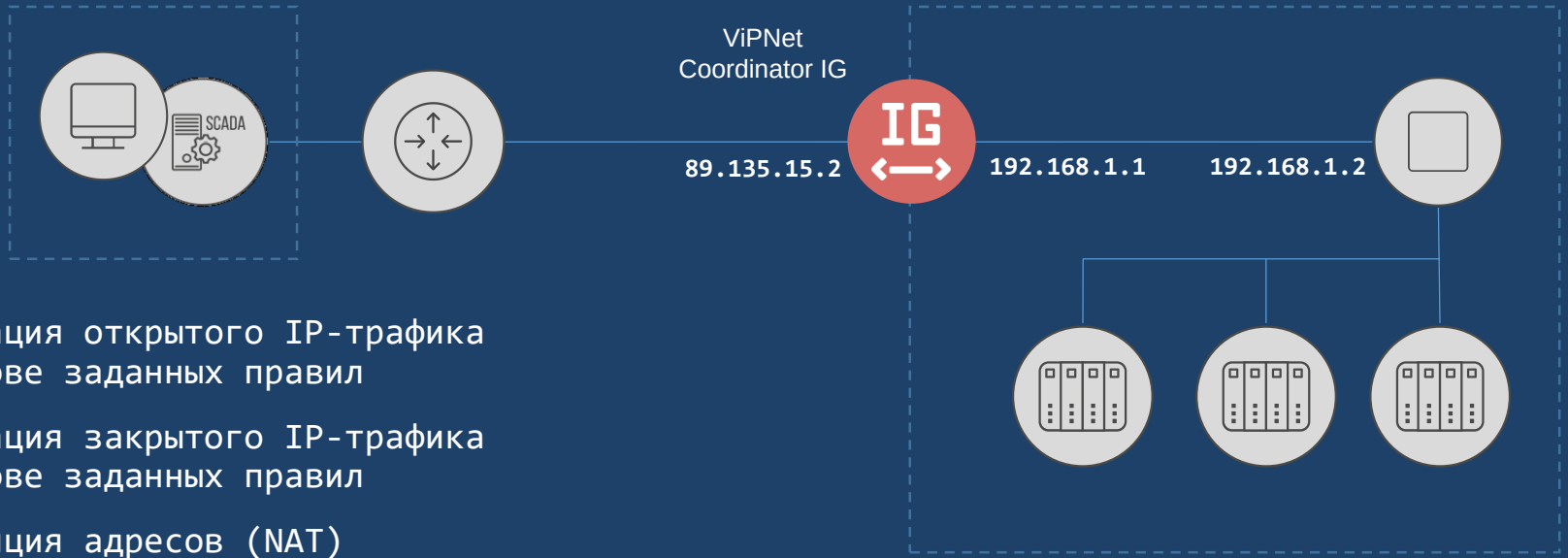
- LTE-модуль

В комплект GSM-модуля входит внешняя GSM-антенна.

Внимание! GSM-модуль устанавливается только на производстве!



Межсетевой экран

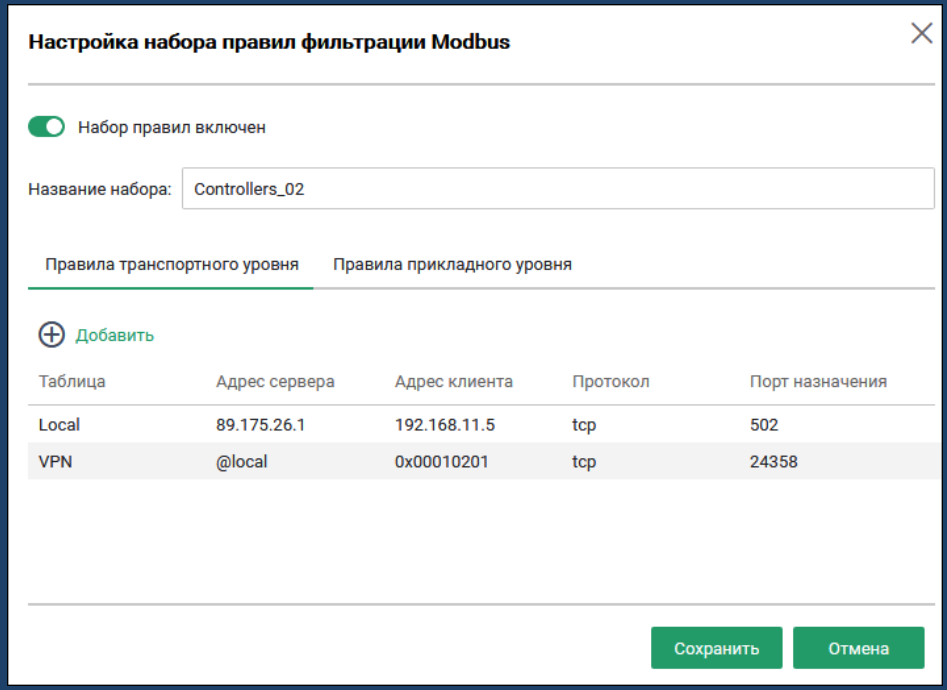


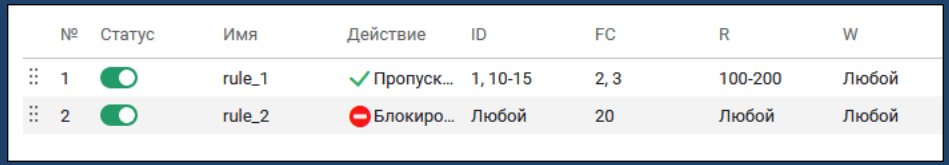
- Фильтрация открытого IP-трафика на основе заданных правил
- Фильтрация закрытого IP-трафика на основе заданных правил
- Трансляция адресов (NAT) для открытого IP-трафика
- Фильтрация на прикладном уровне трафика протоколов Modbus и МЭК 60870-5-104

МЭ тип Д: режимы работы

Фильтрация протокола Modbus TCP

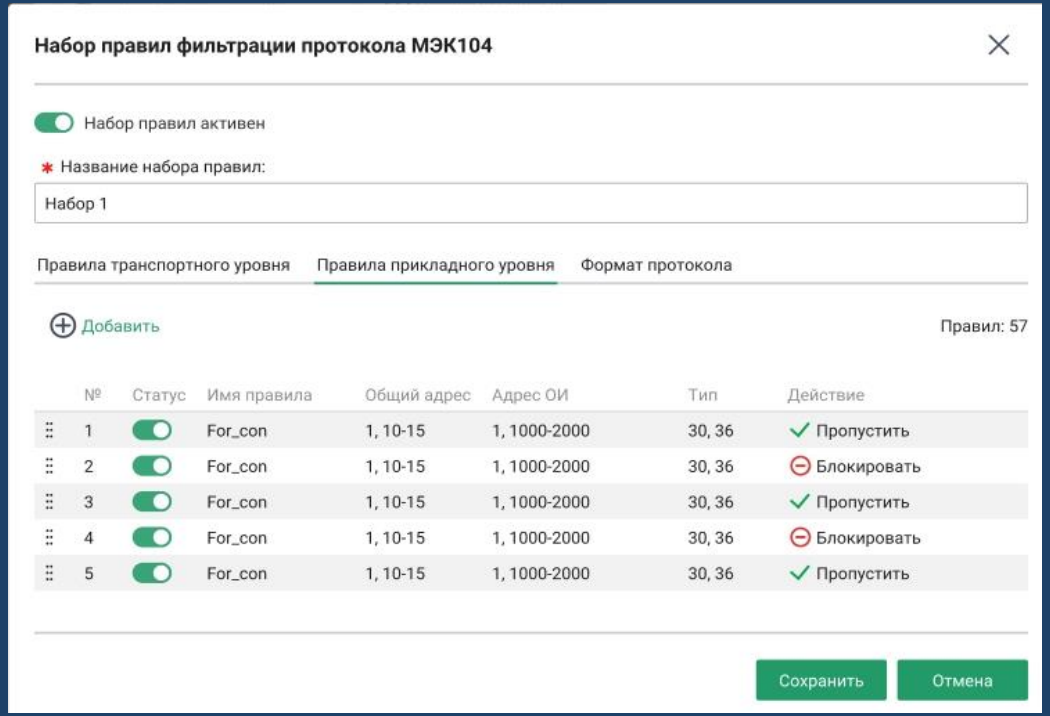
- Номер порта
- Адреса устройств
- Коды функций
- Регистры чтения и записи
- Отдельный журнал регистрации пакетов





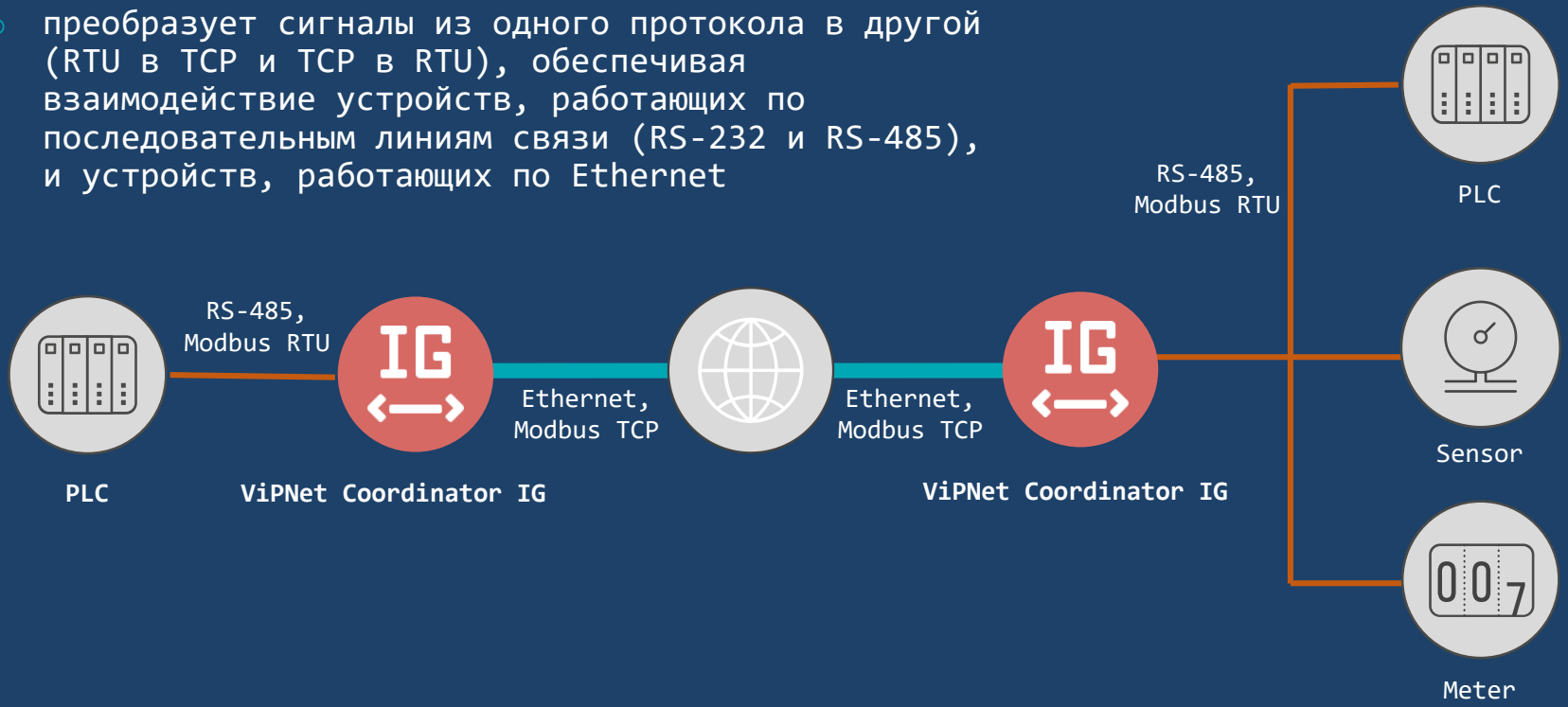
Фильтрация протокола МЭК 60870-5-104 (4.5.1)

- Номер порта
- Общий адрес (ASDU)
- Адрес объекта информации (Information Object Address)
- Идентификатор типа (Type Identifier)



Шлюз Modbus TCP-RTU и RTU-TCP

- преобразует сигналы из одного протокола в другой (RTU в TCP и TCP в RTU), обеспечивая взаимодействие устройств, работающих по последовательным линиям связи (RS-232 и RS-485), и устройств, работающих по Ethernet



Шлюз Modbus TCP-RTU и RTU-TCP

Служба Modbus остановлена

Настройки службы | Маршруты RTU to TCP

Общие настройки

Интерфейс соединения: ○ RS-232 ◉ RS-485

Режим работы: ◉ TCP to RTU ○ RTU to TCP

Адрес шлюза: Шлюз доступен по IP адресам, которые настроены на интерфейсах.

Порт шлюза: 502

Время по умолчанию на ожидание запроса: 1500 мс

Время по умолчанию на ожидание ответа: 1500 мс

Настройки интерфейса RS-232

Скорость TTY устройства: 115200 бод

Контроль бита четности: even

Настройки интерфейса RS-485

Скорость TTY устройства: 115200 бод

Контроль бита четности: even

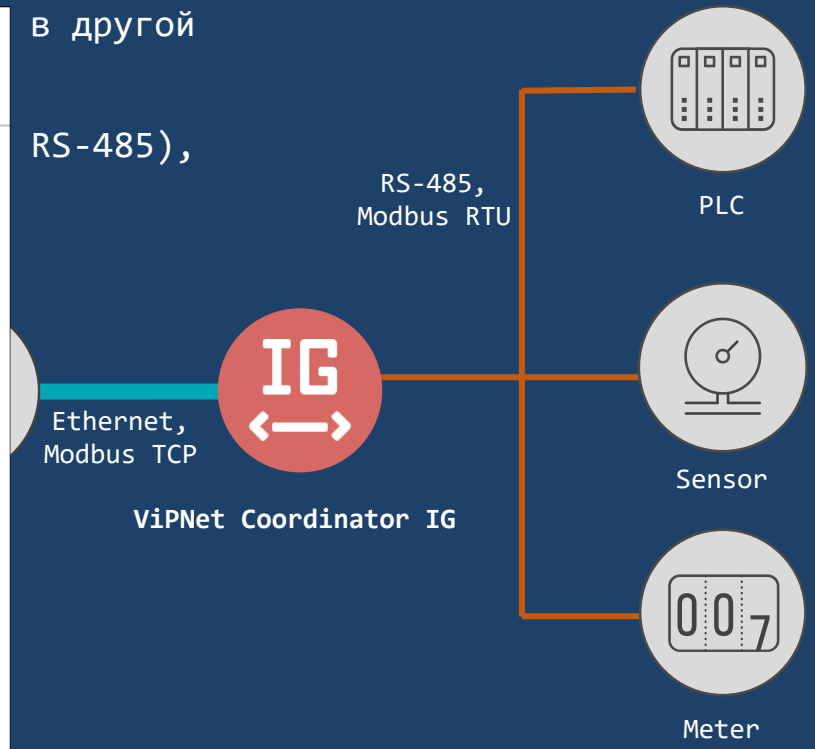
Задержка до отправки: 100 мс

Задержка после отправки: 100 мс

Сохранить | Отмена

в другой

RS-485),



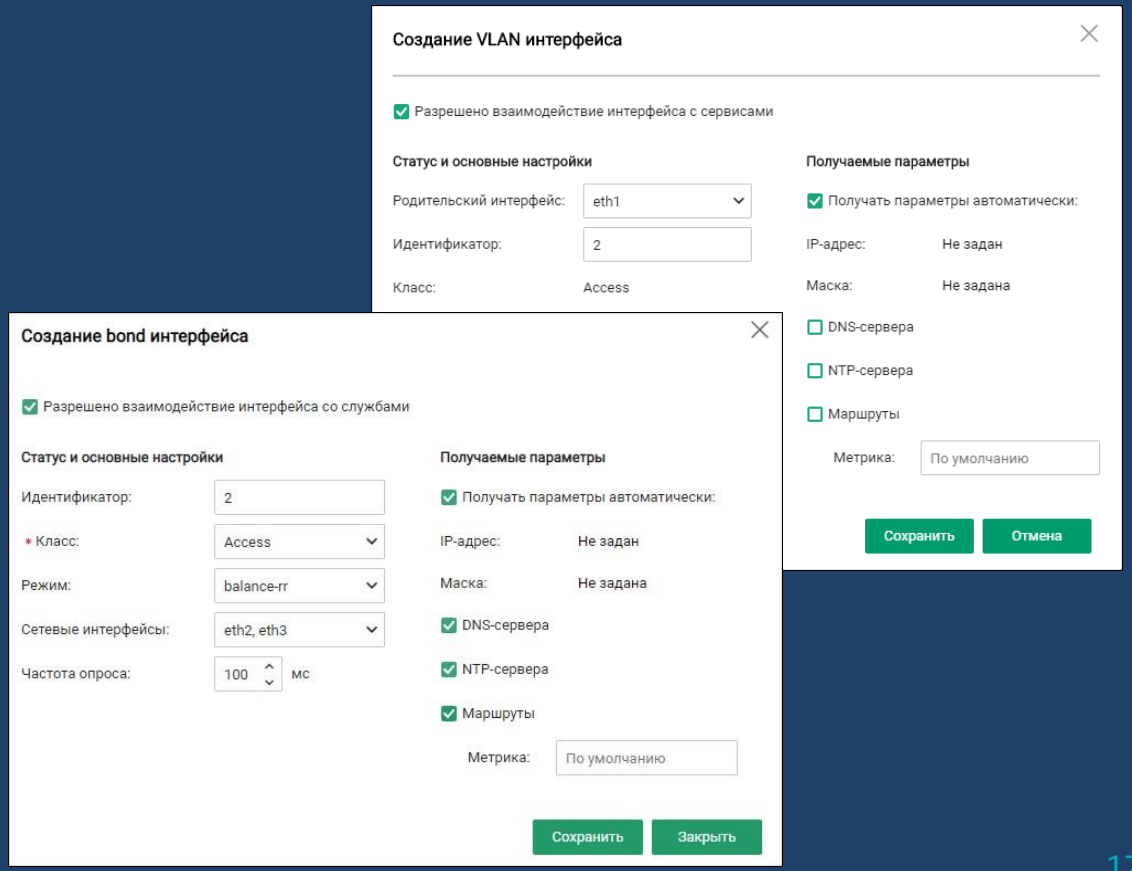
Сетевые сервисы

infotecs

DNS (client/server)	DHCP (server/relay)	NTP (client/server)	VLAN
QoS	EtherChannel	OSPF	Failover

Сетевые сервисы L2

- VLAN
- Агрегирование интерфейсов



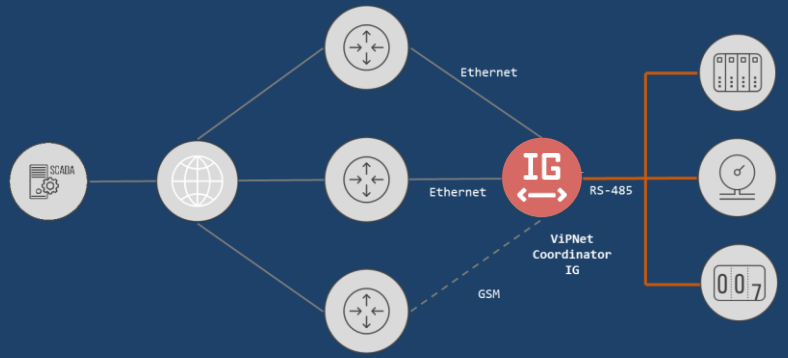
Сетевые сервисы L3

- Статическая и динамическая маршрутизация по протоколам DHCP/PPP и OSPF
- Резервирование каналов
- Балансировка трафика
- Обработка трафика в соответствии с приоритетом (поддержка протокола DiffServ)

Маршрутизация

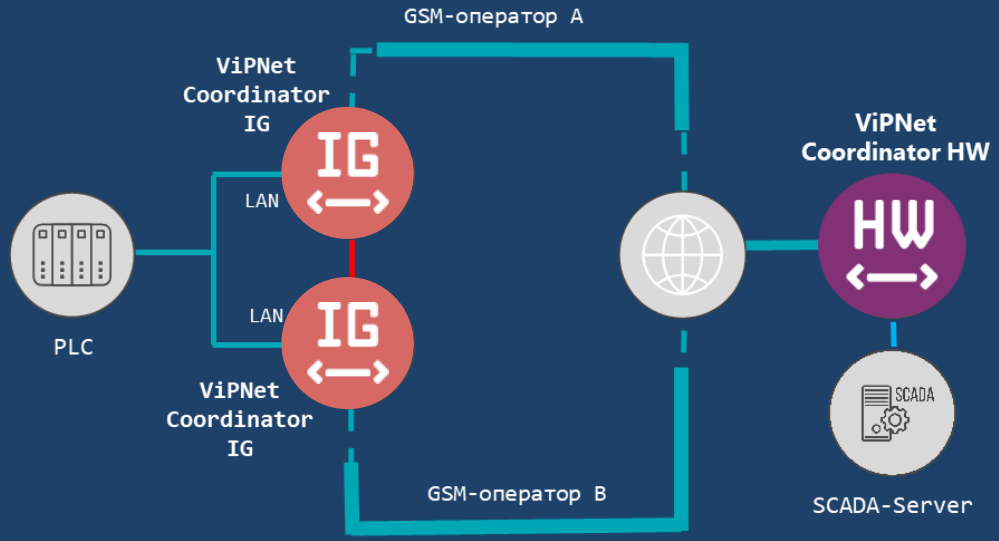
Сводная таблица | Статическая | Политики маршрутизации | DHCP | OSPF

Статус и тип	Адрес назначения и маска	Диста...	Метри...	Вес	Шлюз	Сетевой интерфе...	Активность
DHCP/PPP	0.0.0.0/0	70	70		192.168.179.2	eth0	
Connected	10.0.40.0/24				directly	eth3	
Connected	10.0.40.0/24				directly	eth1	
Connected	10.0.40.0/24				directly	eth2	
Connected	127.0.0.0/8				directly	lo	
Connected	192.168.179.0/24				directly	eth0	



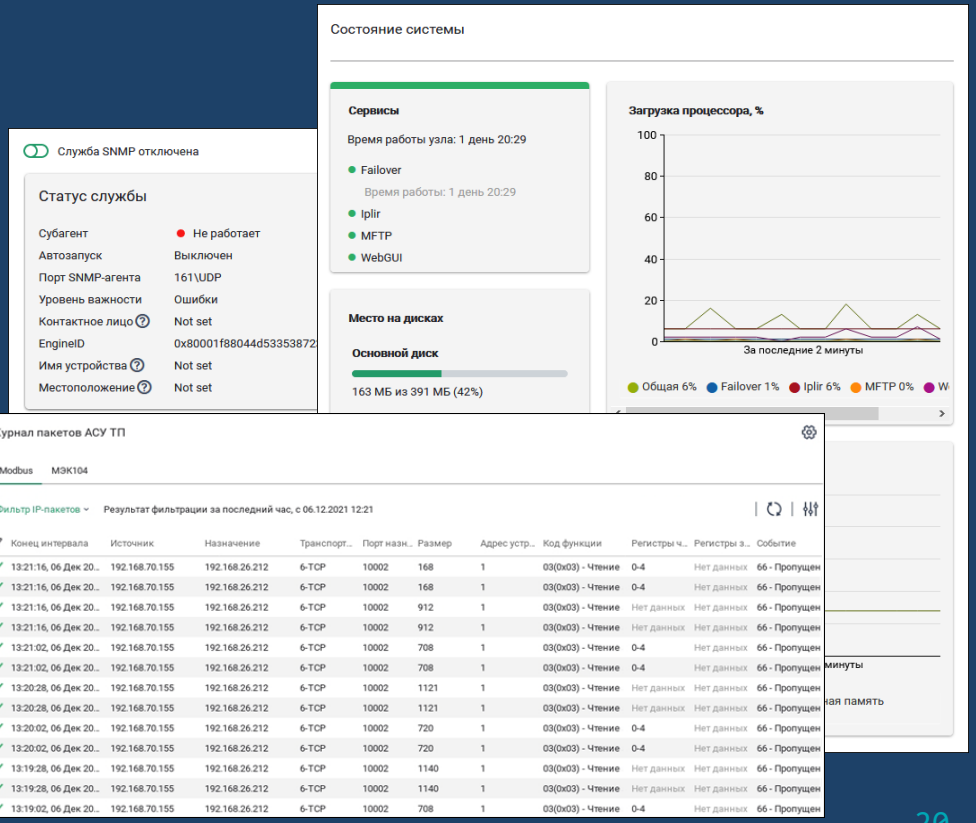
Отказоустойчивость

- Защита от программных сбоев
- Резервирование каналов связи
- Агрегирование каналов связи
- Кластер горячего резервирования:
  - с беспроводными интерфейсами
    - GSM-модем и модули Wi-Fi могут иметь разные настройки на нодах
  - с использованием шлюза Modbus
  - с использованием DHCP



Мониторинг состояния

- Удаленный мониторинг по протоколу SNMPv3
- Просмотр статистики IP-пакетов
- Просмотр журналов:
  - регистрации IP-пакетов
  - пакетов промышленных протоколов
  - транспортных конвертов (MFTP)
  - системного
- Экспорт журналов по протоколу syslog



GPIO

General-Purpose Input/Output – интерфейс ввода/вывода общего назначения

Входной сигнал

- Датчик вскрытия шкафа
- Переключение в специальный режим работы (для типа Д)
- Сигнал с пользовательского устройства

Выходной сигнал

- Кластер с шлюзом Modbus TCP-RTU
- Индикатор событий:
  - работа в режиме обслуживания
  - работа в штатном режиме
  - работа в специальном режиме
  - вскрыт шкаф
  - сигнал на пользовательское устройство

Сценарии работы

ViPNet Coordinator IG 4

Сценарии работы

Версия продукта: 4.5.1

ViPNet Coordinator IG10
ViPNet Coordinator IG100

Содержание

Сертификаты соответствия по требованиям ФСБ России

ViPNet Coordinator IG 4.3.3:

- Сертификат № СФ/124-4247 по требованиям к СКЗИ класса КС3
- Анализ изменений МЭ 4 класса защищенности

ViPNet Coordinator IG 4.5.1:

- Передан на анализ изменений

Сертификат соответствия по требованиям ФСТЭК России

ViPNet Coordinator IG 4.5.1:

Сертификат № 4379

- Требования к МЭ
- Профиль защиты МЭ типа Д 4 класса защиты (ИТ.МЭ.Д4.ПЗ)
- Профиль защиты МЭ типа А 4 класса защиты (ИТ.МЭ.А4.ПЗ)
- Профиль защиты МЭ типа Б 4 класса защиты (ИТ.МЭ.Б4.ПЗ)
- 4 уровень доверия по ТДБ (2020 г)

Реестры РПО, РЭП

- ПО ViPNet Coordinator IG включено в реестр российского ПО – рег.номер 5102 (19.01.2019)
- Единый реестр российской радиоэлектронной продукции (РЭП) – как ПАК ViPNet Coordinator IG, в процессе подтверждения

Линейка шлюзов безопасности ViPNet Coordinator IG

ViPNet Coordinator IG10 I1

ViPNet Coordinator IG100 I1

ViPNet Coordinator IG10 I2

ViPNet Coordinator IG100 I4

ViPNet Coordinator IG100 I5

Классические исполнения

Новые исполнения

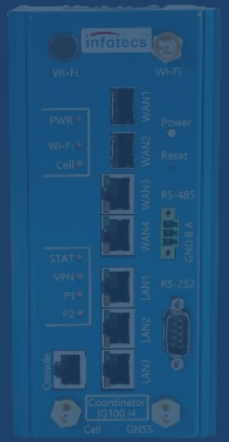
Линейка шлюзов безопасности ViPNet Coordinator IG

ViPNet Coordinator IG10 I1

ViPNet Coordinator IG100 I1

ViPNet Coordinator IG10 I2

Классические исполнения



ViPNet Coordinator IG100 I4

ViPNet Coordinator IG100 I5

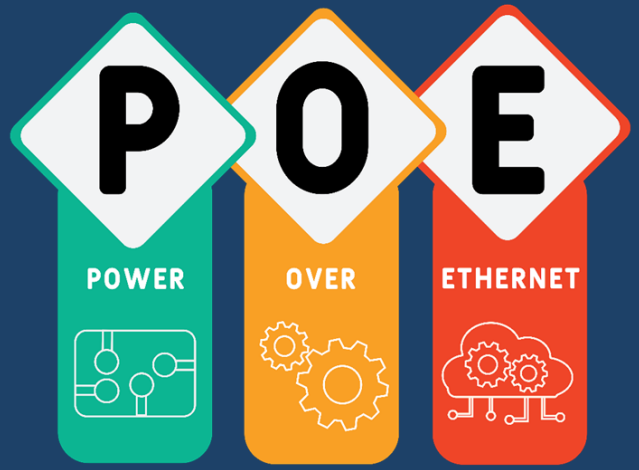
Новые исполнения

Что такое PoE?

PoE (Power over Ethernet) – технология использования витой пары стандарта Ethernet для передачи данных и для питания устройства.

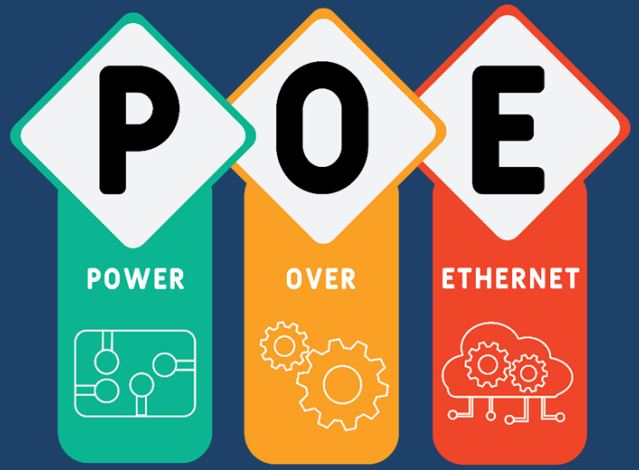
Питающие устройства - инжекторы;
Power Sourcing Equipment, PSE

Питаемые устройства
Powered Device, PD



Зачем?

- Подключение устройств в труднодоступных местах
- Управление питанием (включение/выключение/перезапуск)
- Упрощенное обслуживание (нет отдельных блоков питания)
- Электробезопасность



ViPNet Coordinator IG100 I5

- Питание: 24В DC, PoE
- Ethernet: 2 x LAN 10/100BASE-T
  с возможностью питать PoE-устройства по стандартам IEEE 802.3af и IEEE 802.3at (PoE PSE)
- 1 x WAN 10/100BASE-T
  с возможностью получать питание по стандартам IEEE 802.3af и IEEE 802.3at (PoE PD)
- Рабочая температура - -20⁰C* …+50⁰C

* Для АП с беспроводными модулями

МАСТЕР-КЛАСС: сценарии

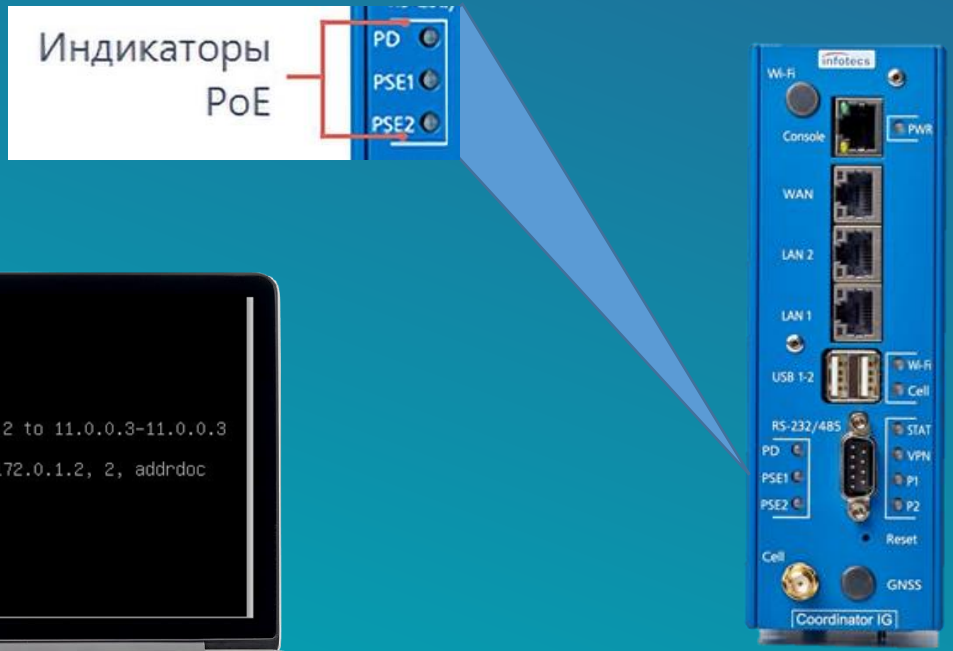
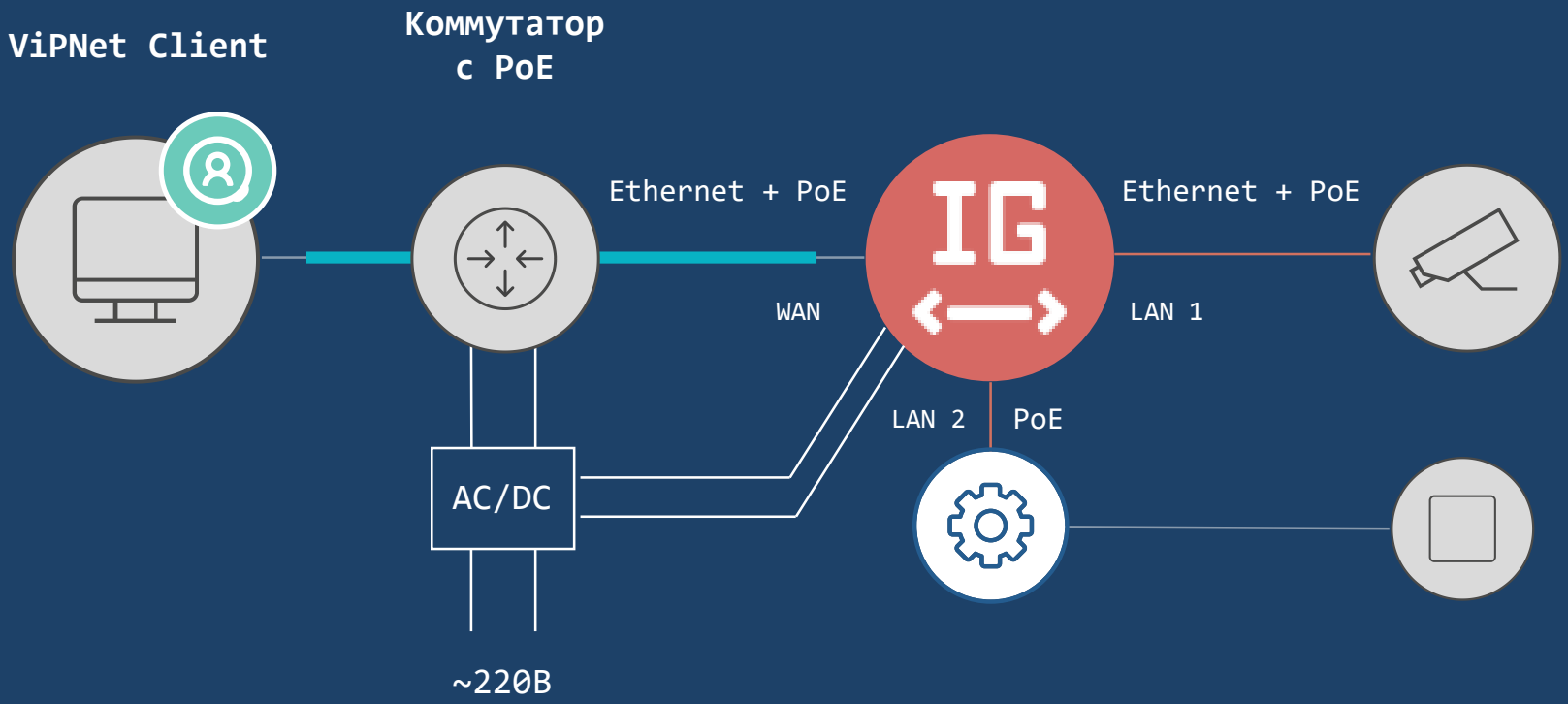
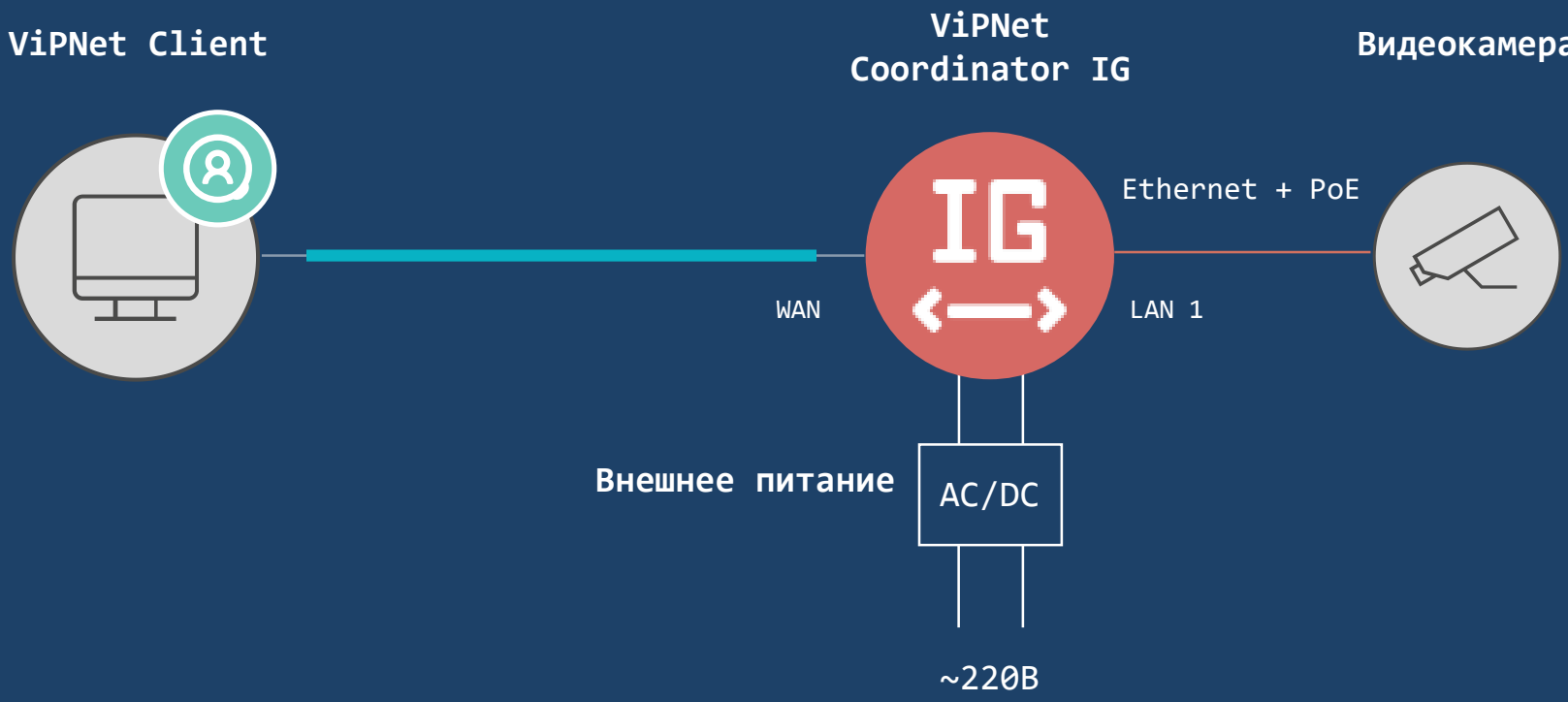


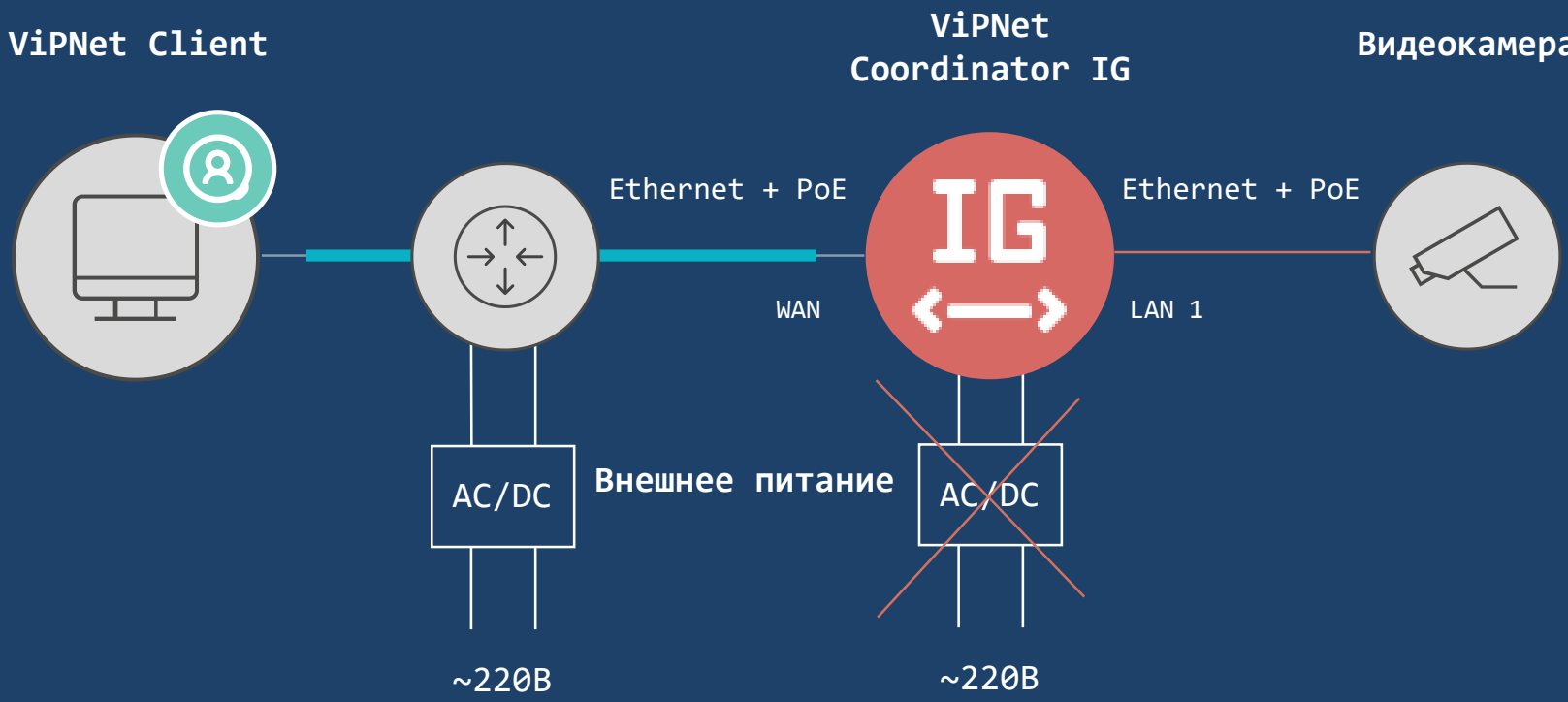
Схема стенда



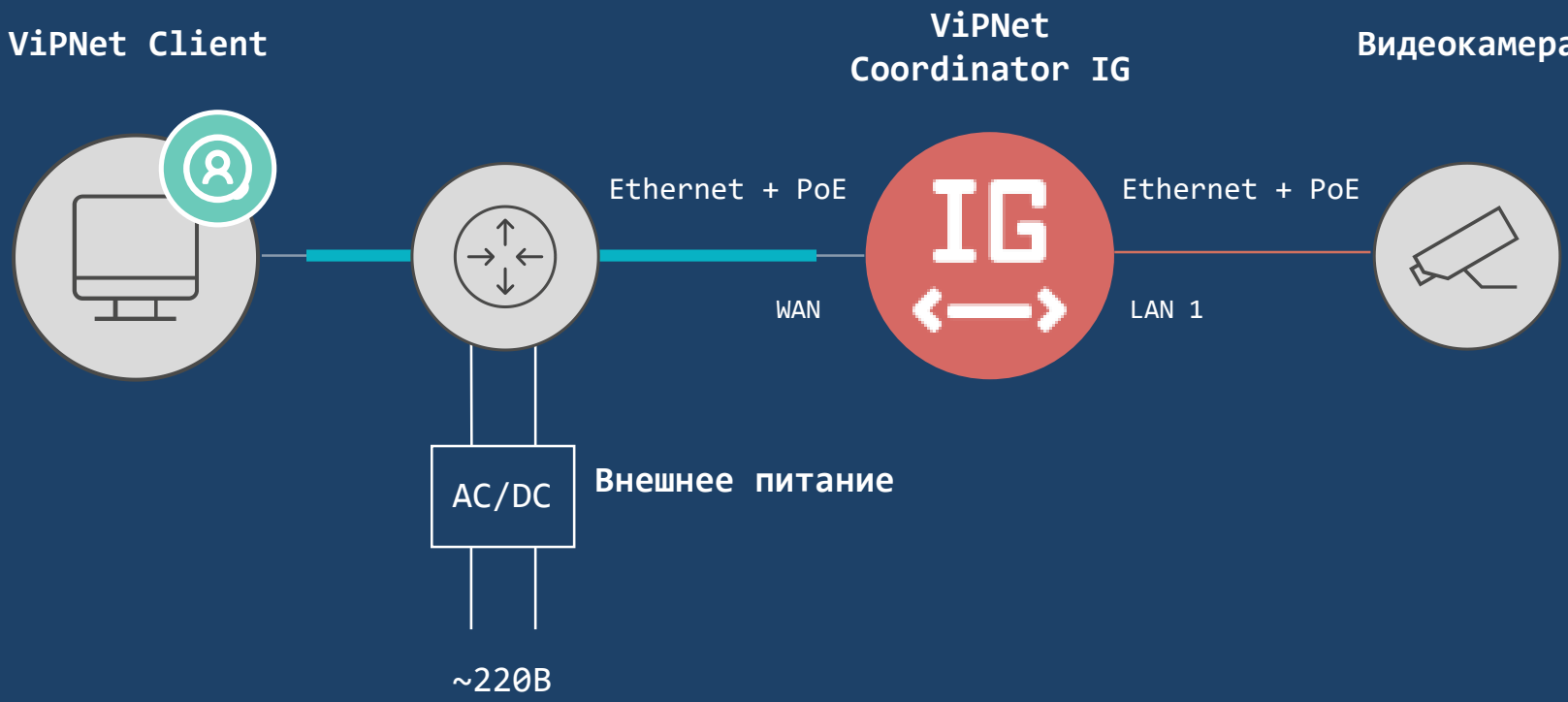
PoE-источник (PSE)



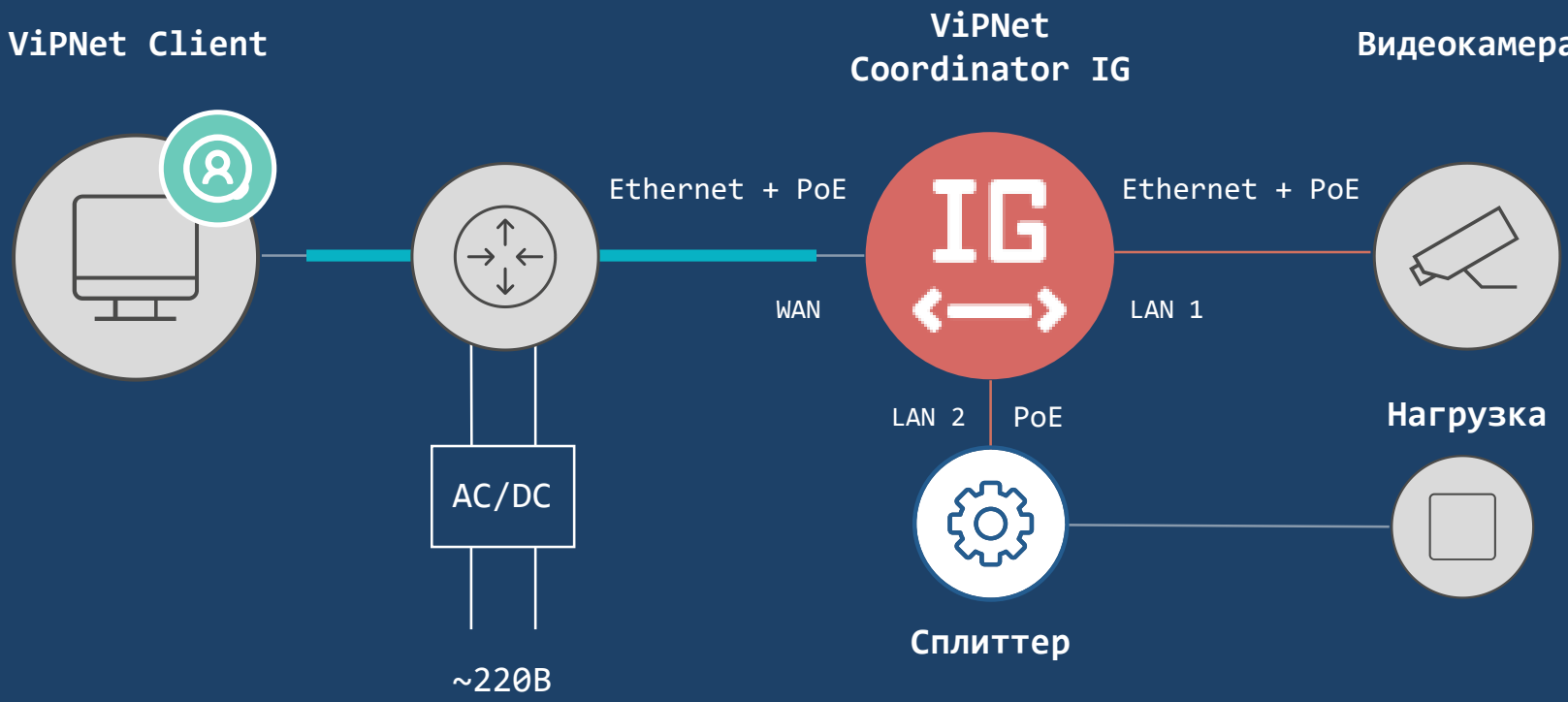
PoE-Delivery (PD + PSE)



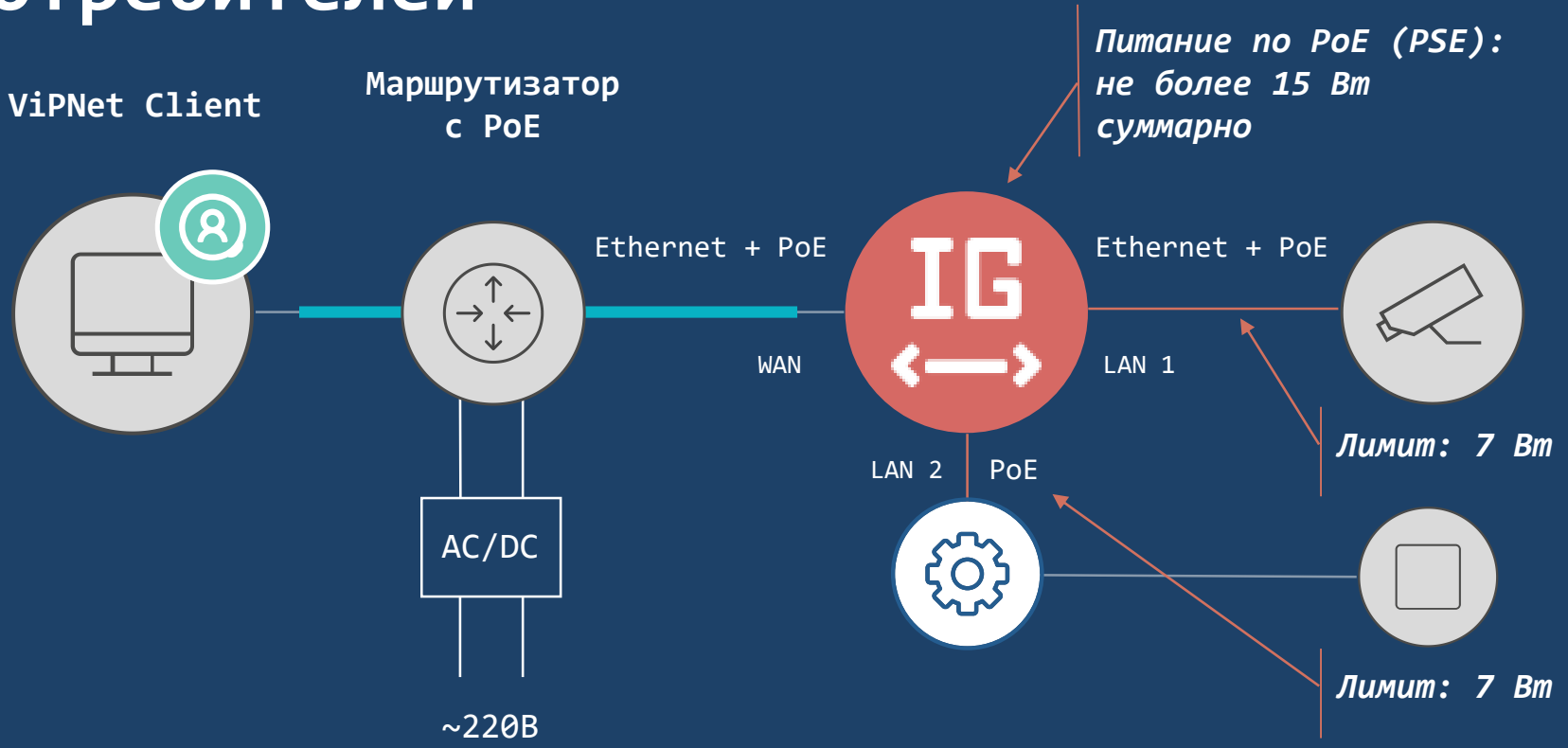
PoE-Delivery (PD + PSE)



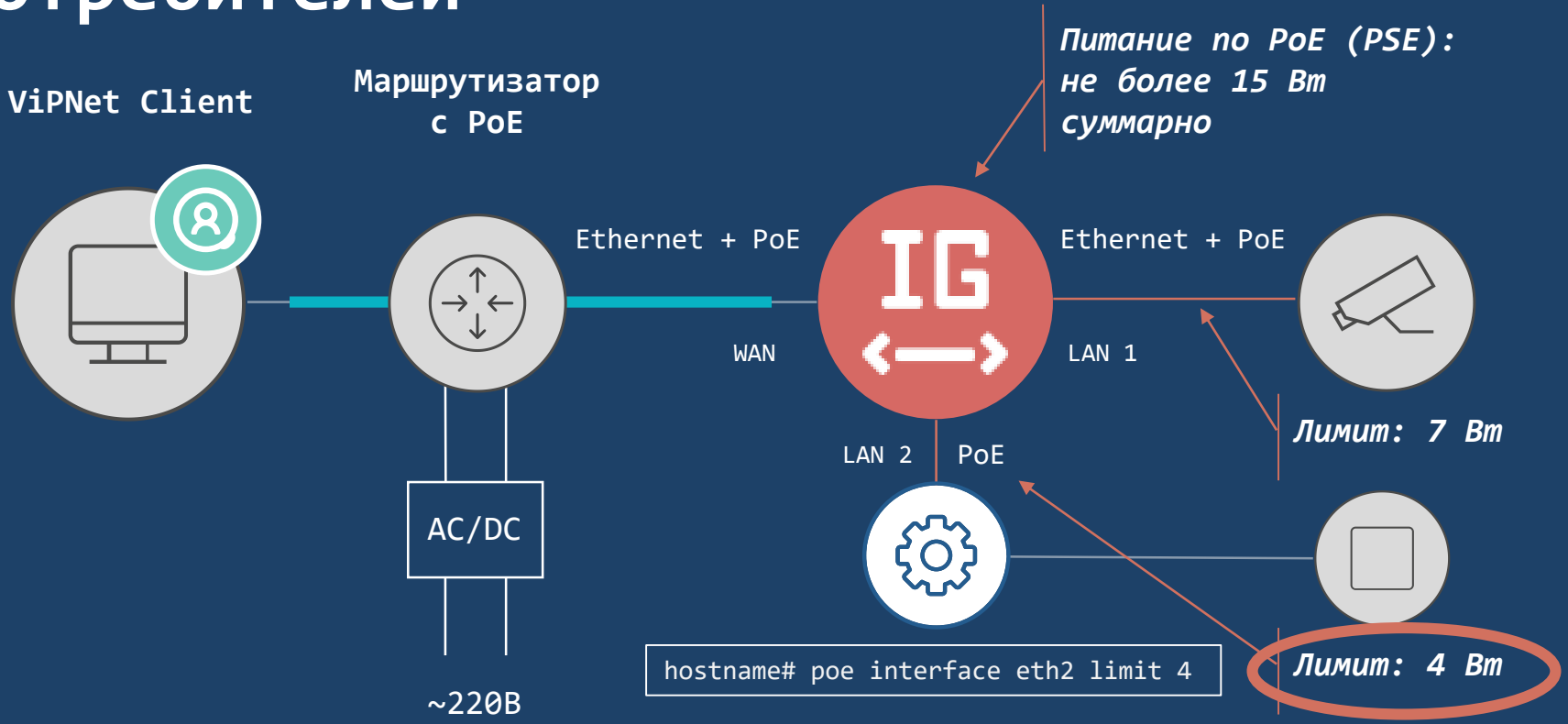
Питание потребителей по двум каналам



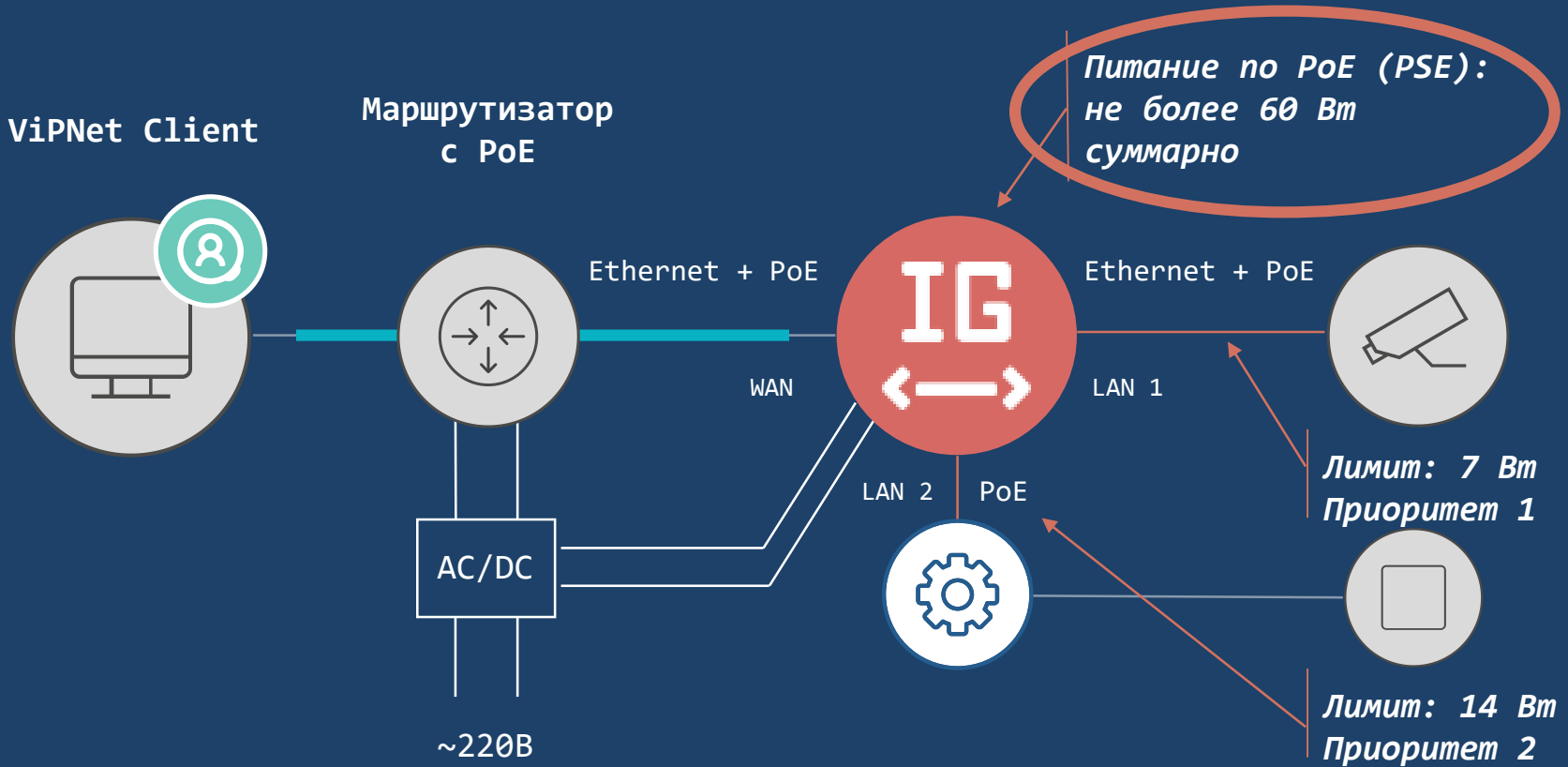
Ограничение мощности потребителей



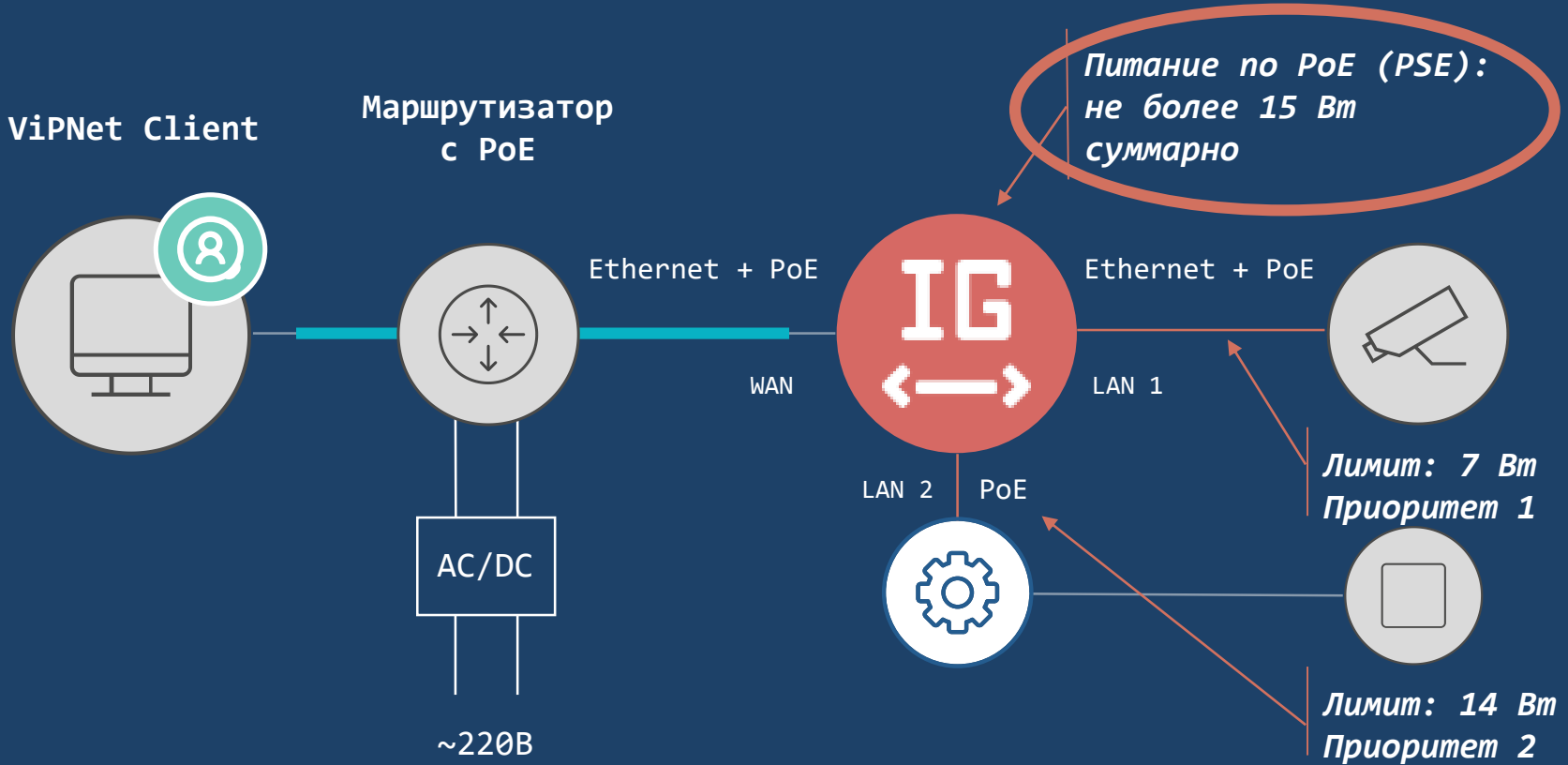
Ограничение мощности потребителей



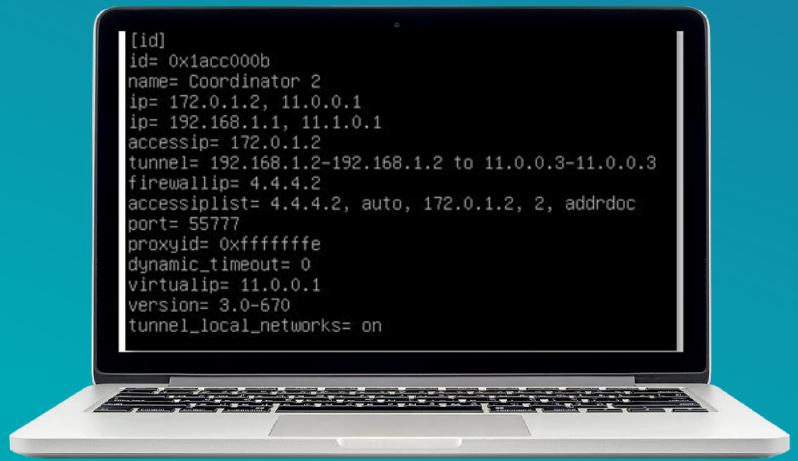
Power Delivery



Приоритеты потребителей



МАСТЕР-КЛАСС: демонстрация



Андрей Иванов Andrey.Ivanov2@infotecs.ru

Иван Герасименко Ivan.Gerasimenko@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363