ViPNet Coordinator IG - промышленные криптошлюзы с межсетевым экраном

Андрей Иванов

ViPNet Coordinator IG

- промышленный шлюз безопасности

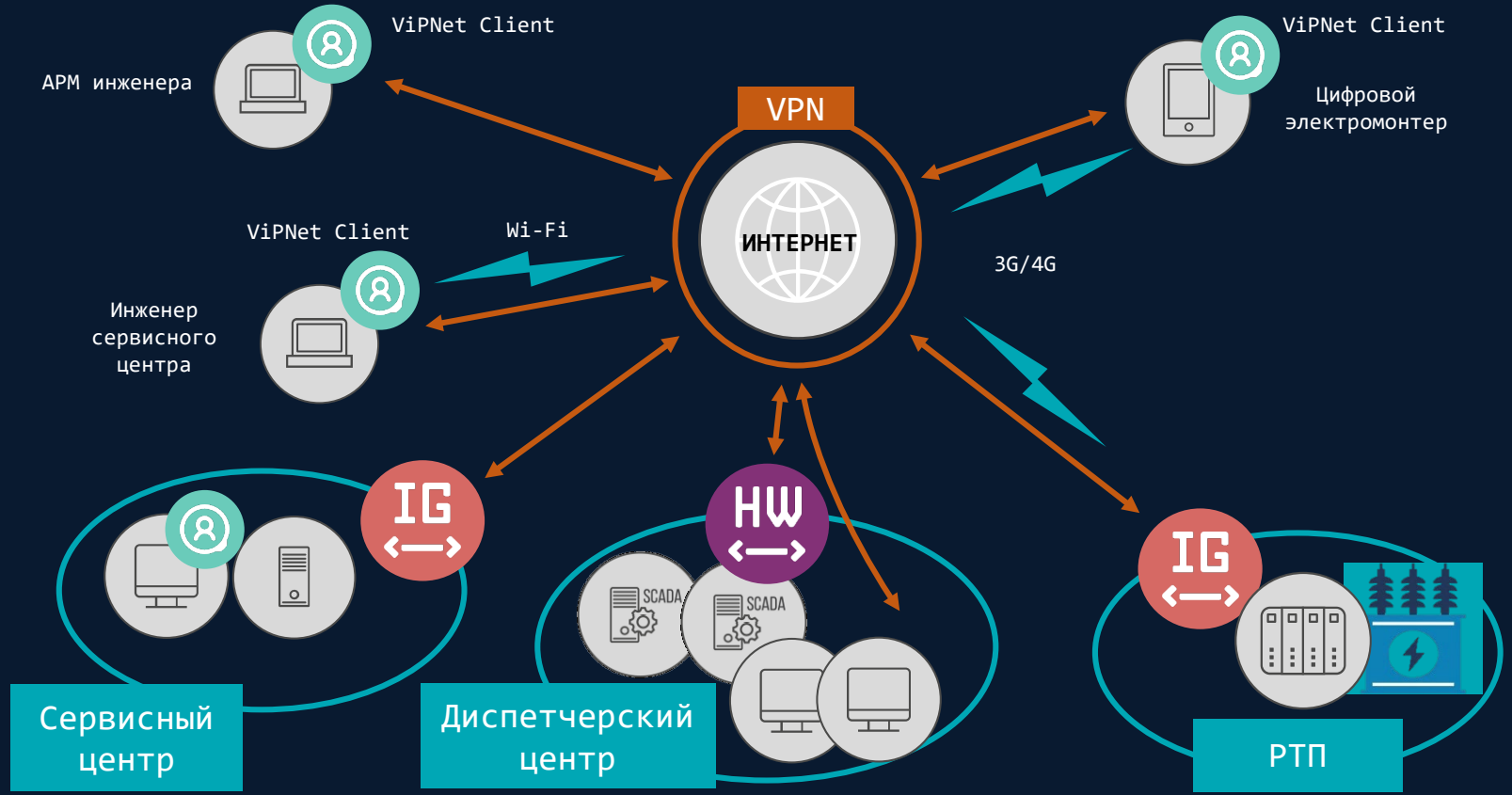
Функционал

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

Защищенная сеть ViPNet

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

Каналы передачи данных

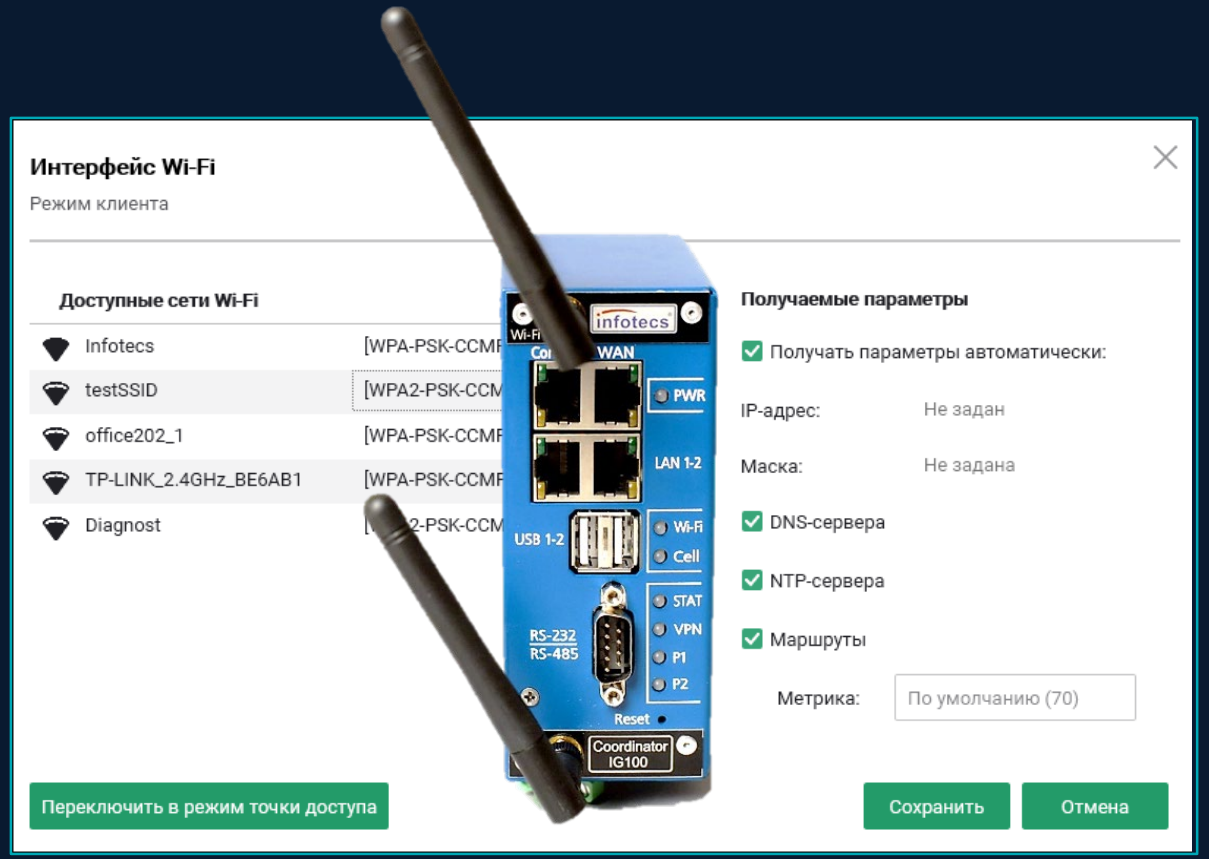


Wi-Fi

- Клиент
- Точка доступа

В комплект входит внешняя антенна.

Внимание! Wi-Fi модуль устанавливается только на производстве!

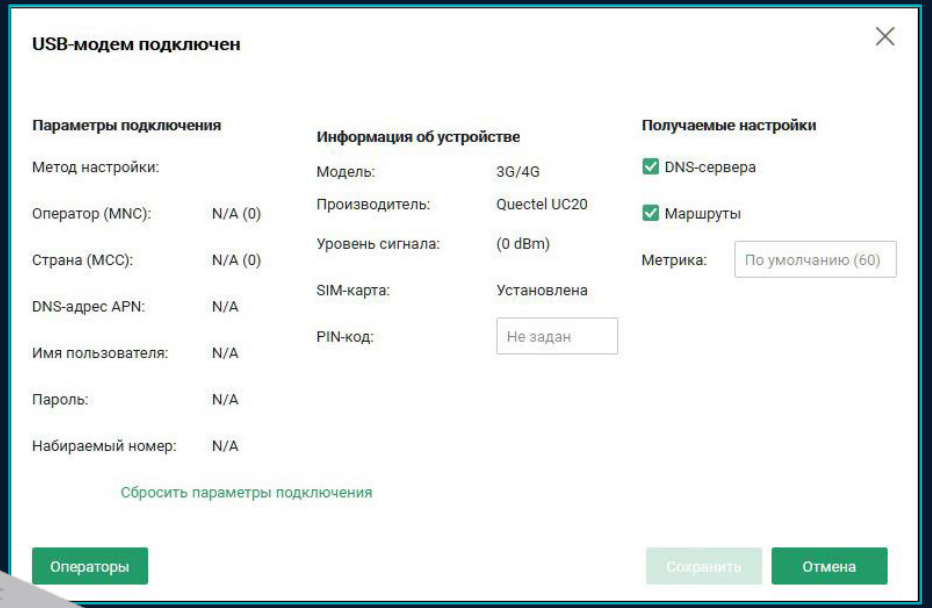


GSM-модуль

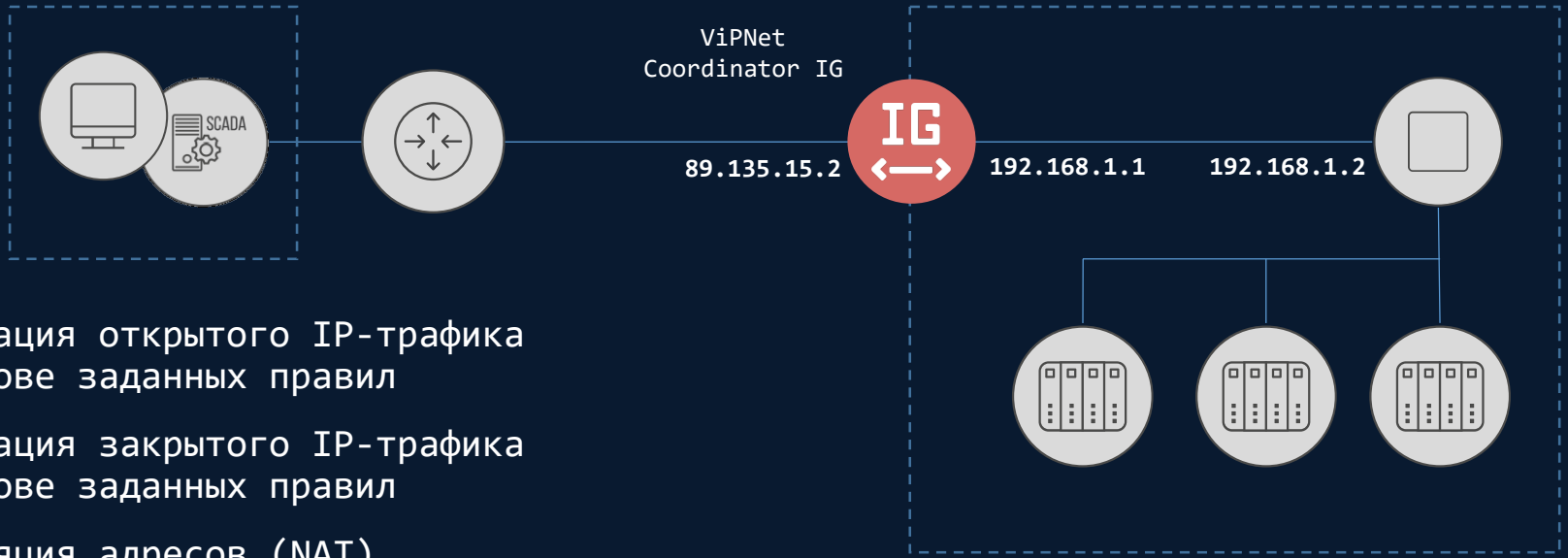
- LTE-модуль

В комплект входит внешняя GSM-антенна.

Внимание! GSM-модуль устанавливается только на производстве!



Межсетевой экран



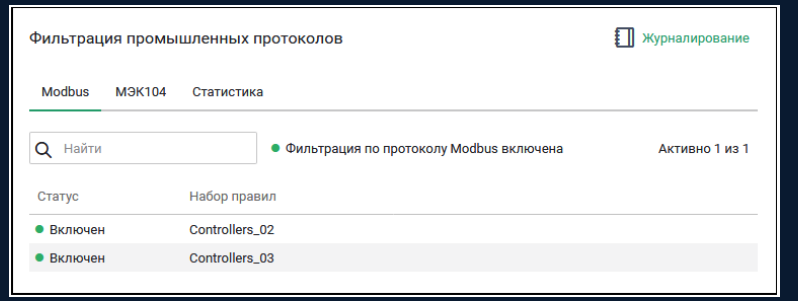
- Фильтрация открытого IP-трафика на основе заданных правил
- Фильтрация закрытого IP-трафика на основе заданных правил
- Трансляция адресов (NAT) для открытого IP-трафика
- Фильтрация на прикладном уровне трафика протоколов Modbus и МЭК 60870-5-104

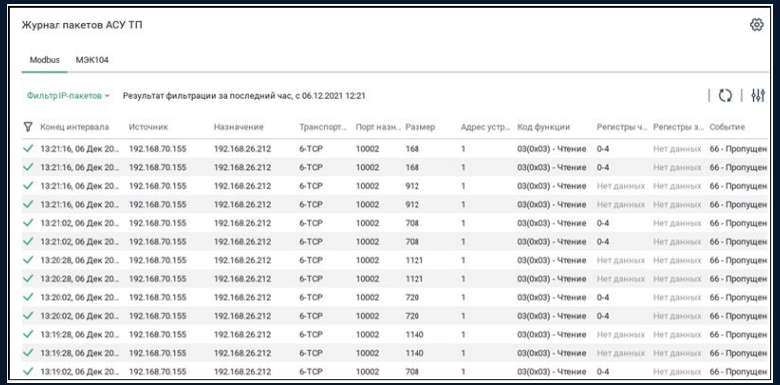
МЭ типа «Д»: режимы работы

Фильтрация промышленных протоколов

Версия 4.5.1:

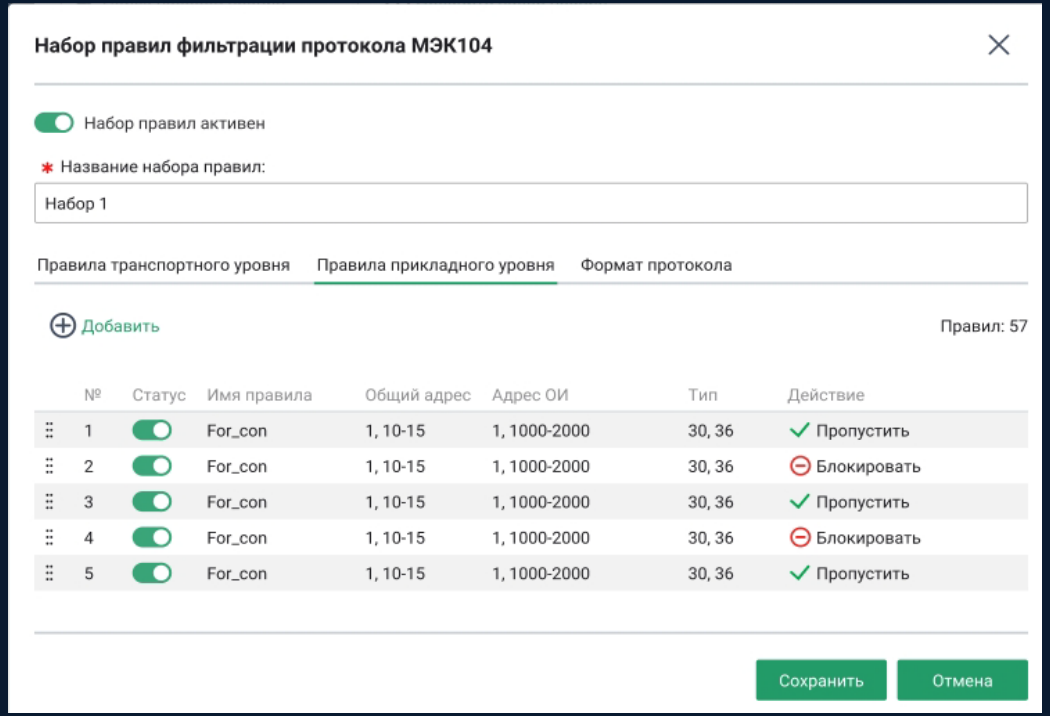
- Фильтрация промышленных протоколов настраивается отдельно от сетевых фильтров
- Отдельный журнал пакетов промышленных протоколов
- Фильтрация на прикладном уровне протоколов Modbus и МЭК 60870-5-104
  - Правила транспортного уровня
  - Правила прикладного уровня





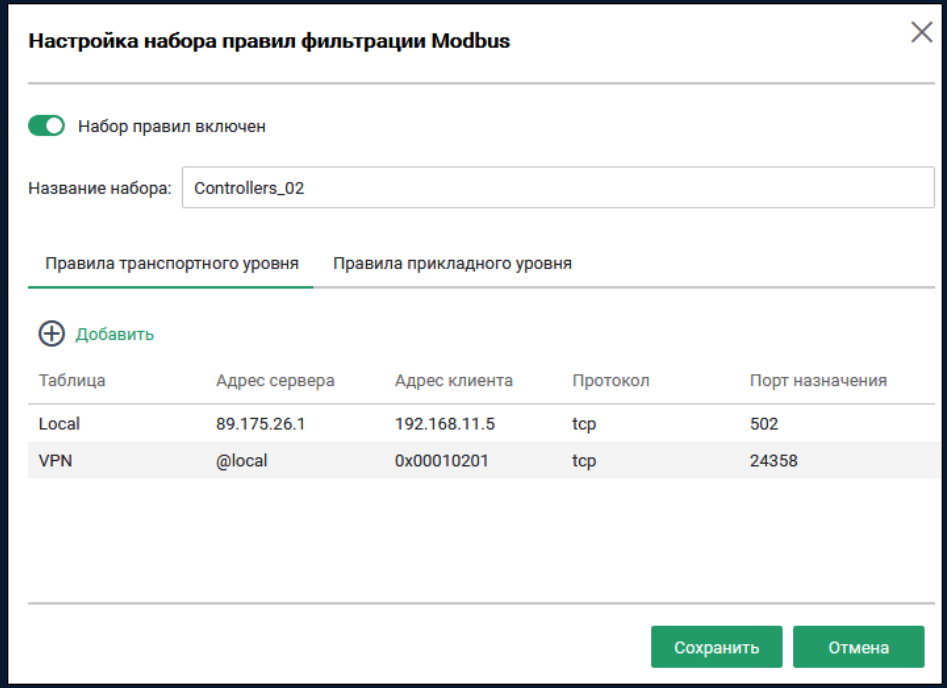
Фильтрация протокола МЭК 60870-5-104 (4.5.1)

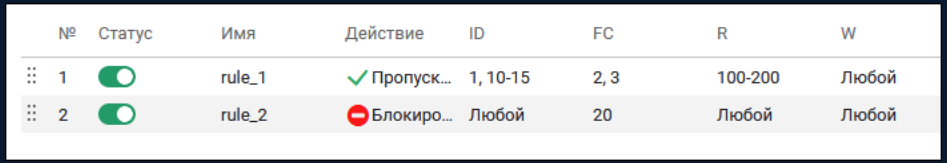
- Номер порта
- Общий адрес (ASDU)
- Адрес объекта информации (Information Object Address)
- Идентификатор типа (Type Identifier)



Фильтрация протокола Modbus TCP

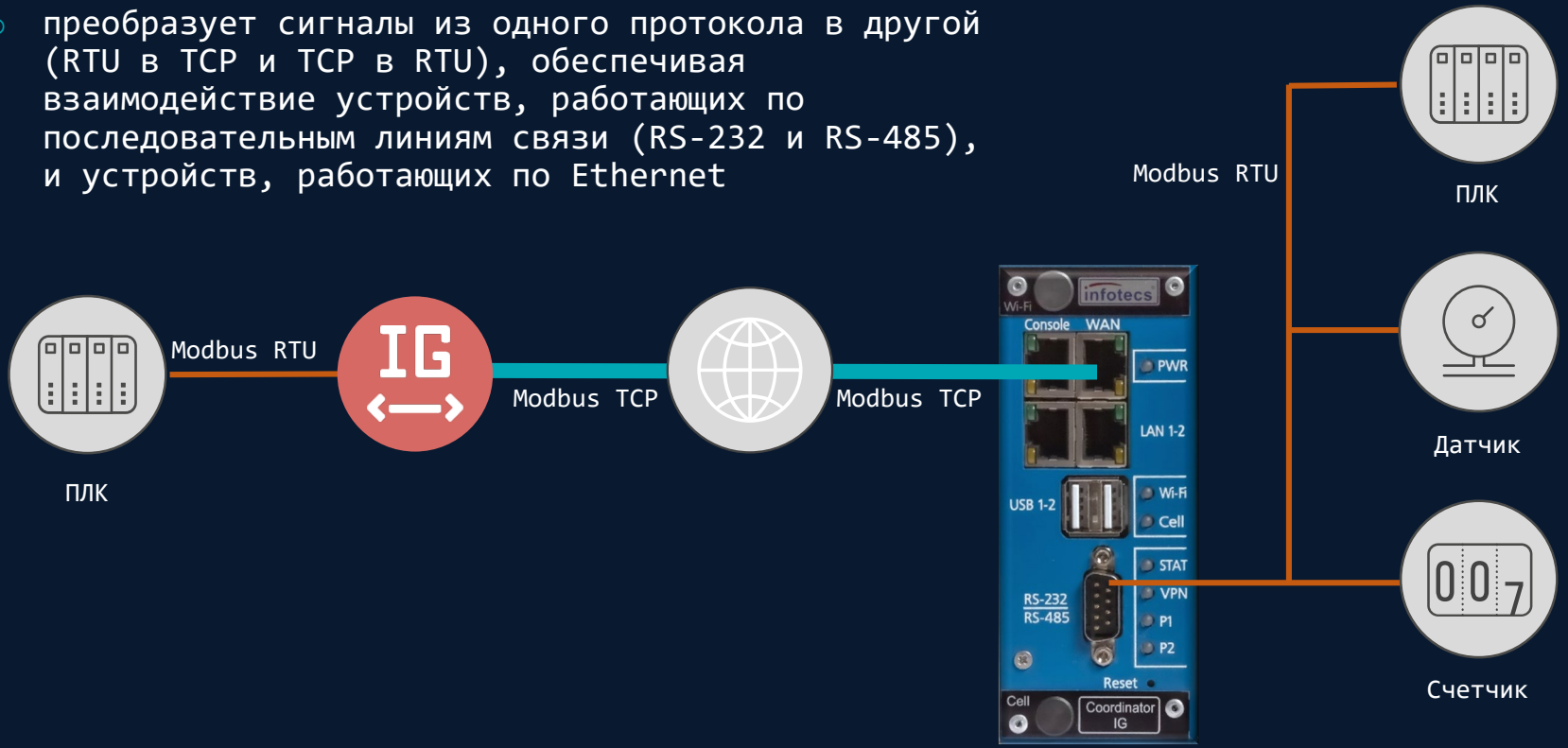
- Номер порта
- Адреса устройств
- Коды функций
- Регистры чтения и записи
- Отдельный журнал регистрации пакетов





Шлюз Modbus TCP-RTU и RTU-TCP

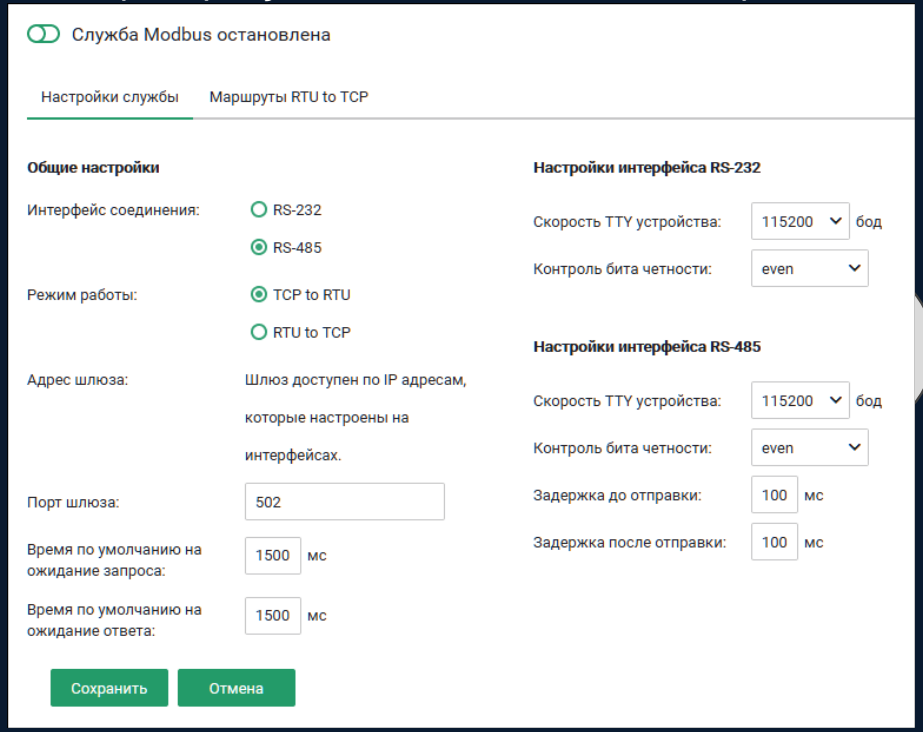
- преобразует сигналы из одного протокола в другой (RTU в TCP и TCP в RTU), обеспечивая взаимодействие устройств, работающих по последовательным линиям связи (RS-232 и RS-485), и устройств, работающих по Ethernet

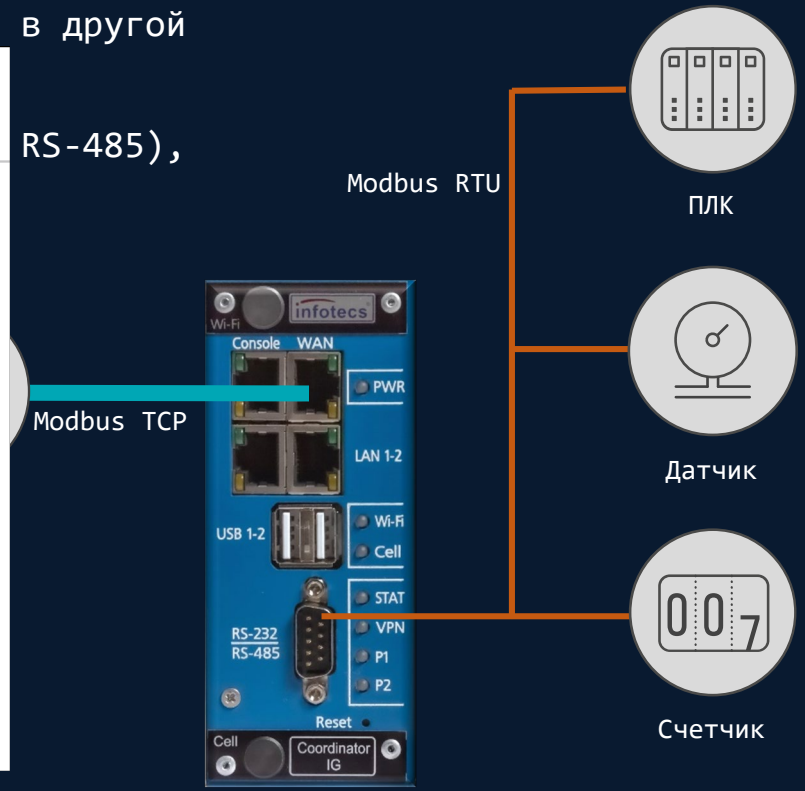


Шлюз Modbus TCP-RTU и RTU-TCP

- преобразует сигналы из одного протокола в другой

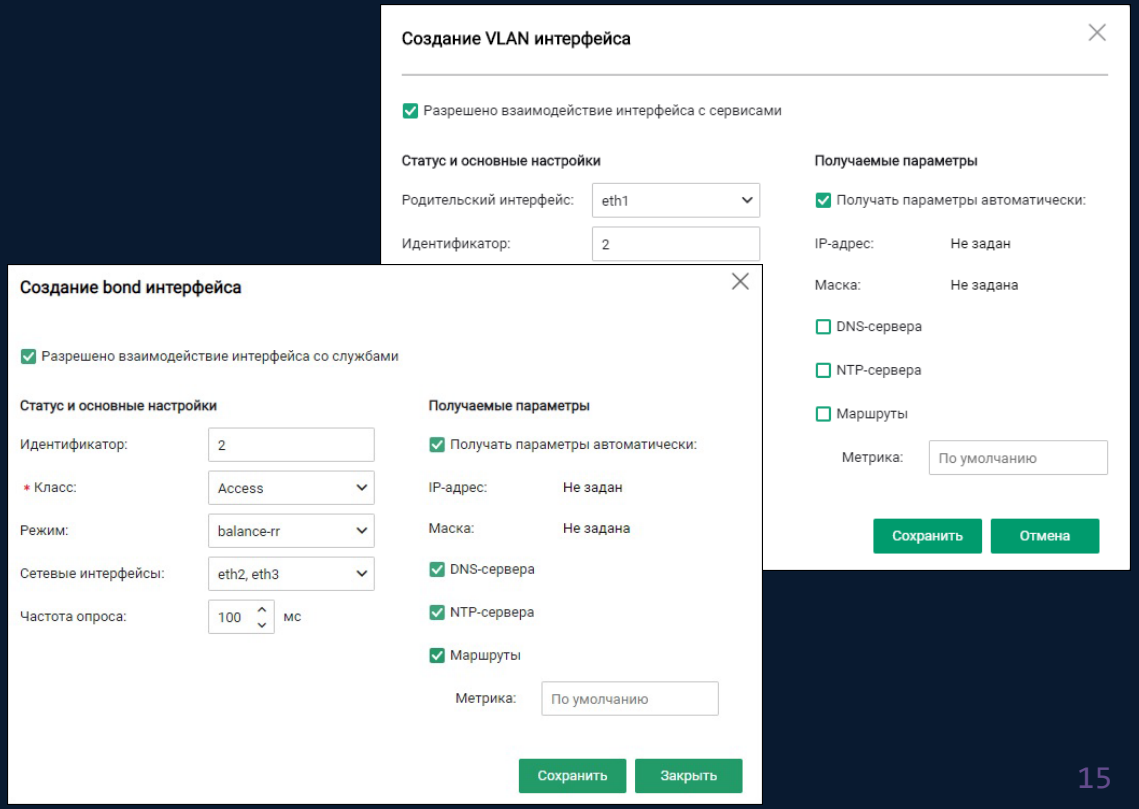
RS-485),





Сетевые сервисы L2

- VLAN
- Агрегирование интерфейсов



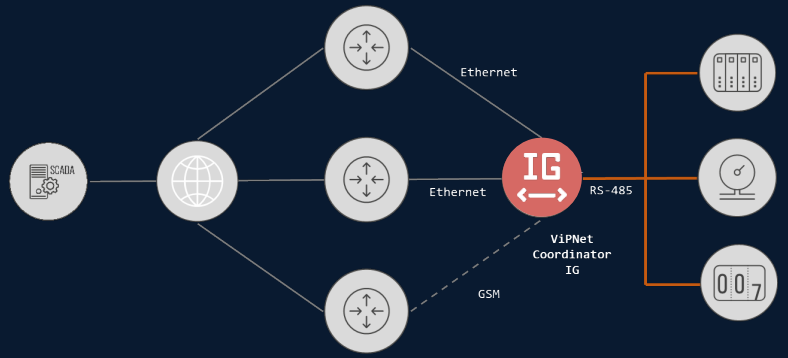
Сетевые сервисы L3

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

Маршрутизация

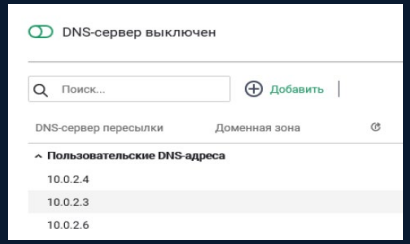
Сводная таблица | Статическая | Политики маршрутизации | DHCP | OSPF

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	

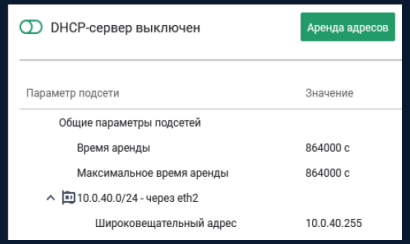


Сетевые сервисы

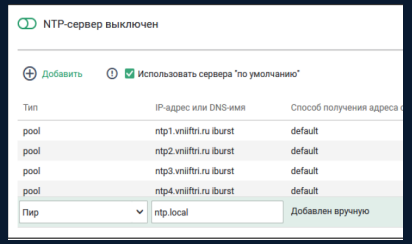
DNS (client/server)



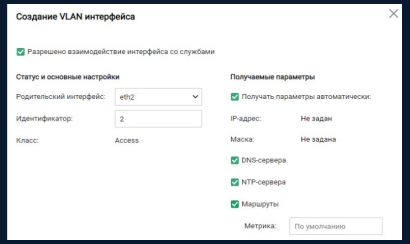
DHCP (server/relay)



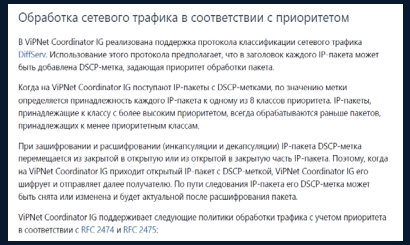
NTP (client/server)



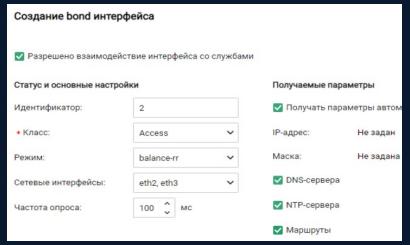
VLAN



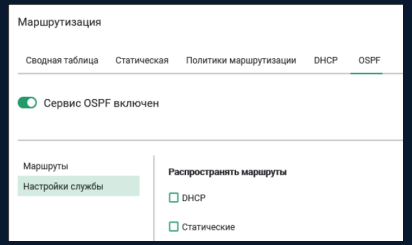
QoS



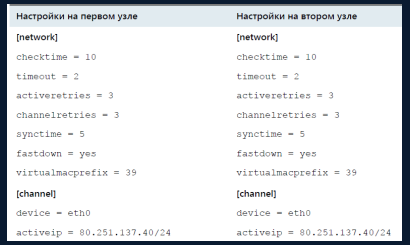
MultiWAN



OSPF

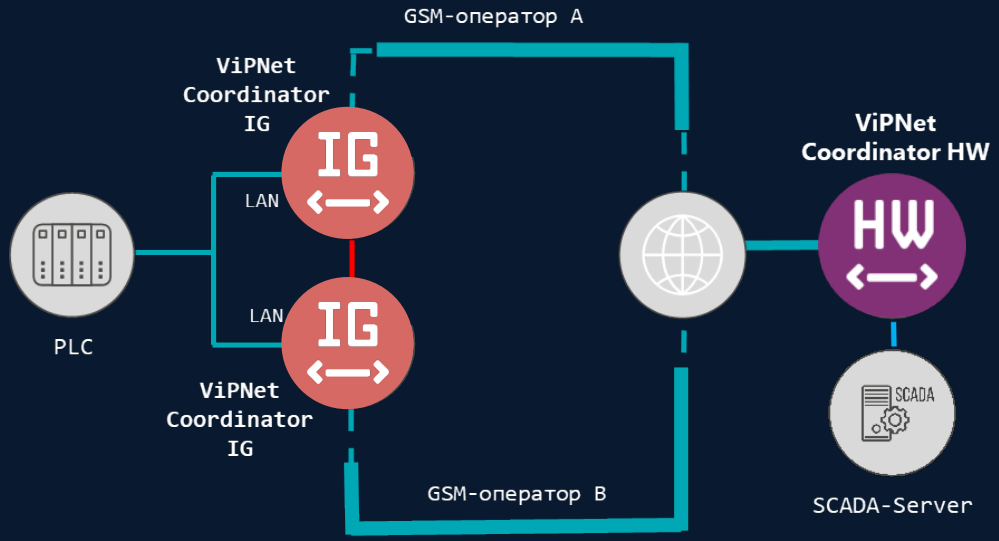


Cluster



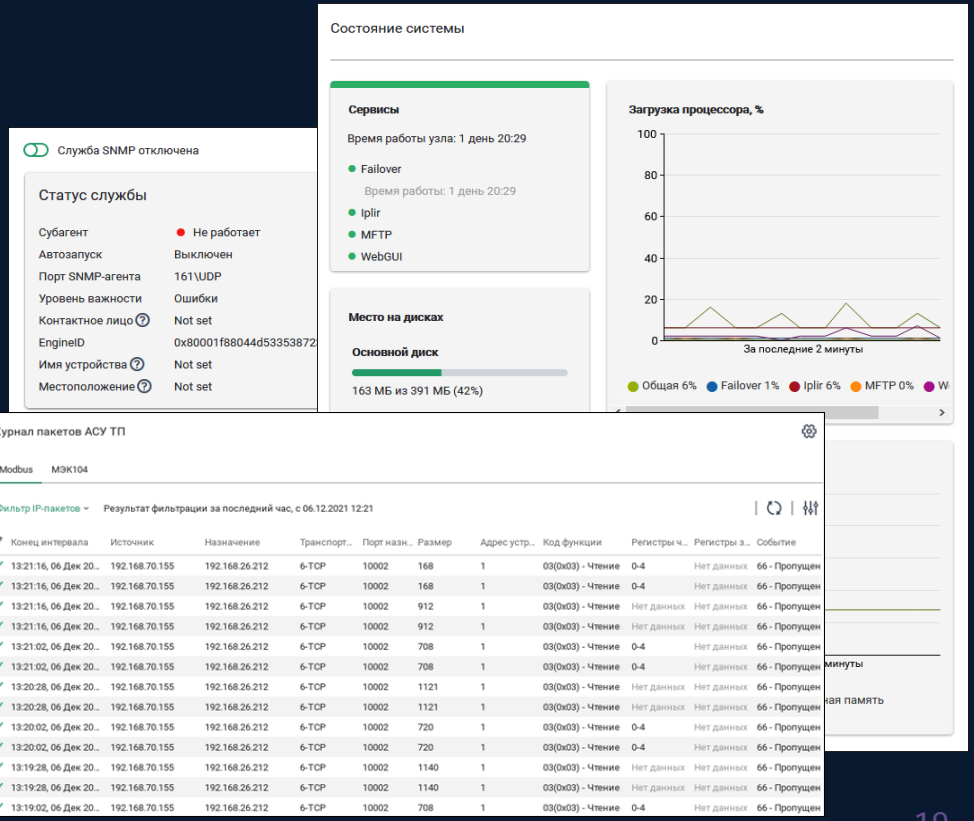
Отказоустойчивость

- 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

Линейка шлюзов безопасности ViPNet Coordinator IG 4

ViPNet Coordinator IG10 I1

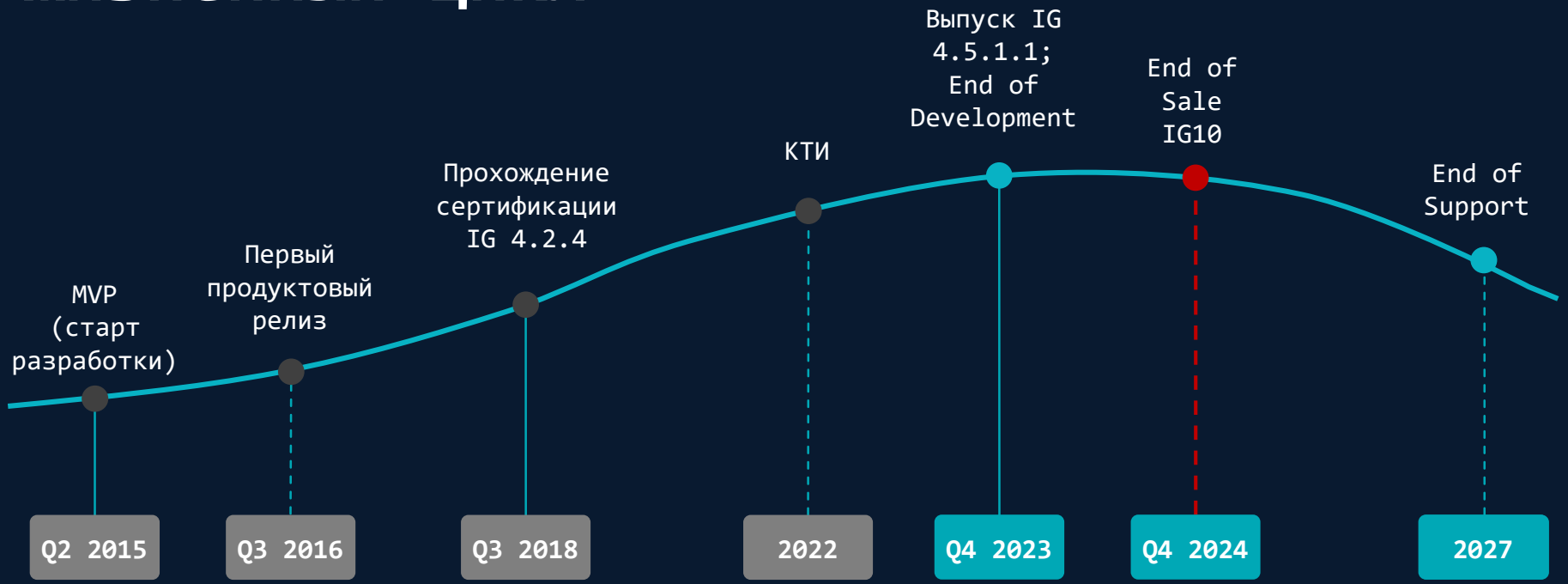
ViPNet Coordinator IG100 I1

ViPNet Coordinator IG10 I2

ViPNet Coordinator IG100 I4

ViPNet Coordinator IG100 I5

ViPNet Coordinator IG 4: жизненный цикл



ViPNet Coordinator IG 5.1

Выпущен в декабре 2023 г.

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ:

- «Кузнечик» и «Магма» (ГОСТ 34.12-2018, !ГОСТ 34.13-2018)
- ГОСТ 28147-89 для обратной совместимости

```
Root: ~$ info ГОСТ 34.12-2018
[1] ГОСТ 34.12-2018 «Информационная технология.
  Криптографическая защита информации. Блочные шифры»
[2] введен в эксплуатацию 2018 г.
>
>/////
Root: ~$ info ГОСТ 28147-89
[1] ГОСТ 28147-89 «Системы обработки информации. Защита
  криптографическая. Алгоритм криптографического
  преобразования»
                    -
```

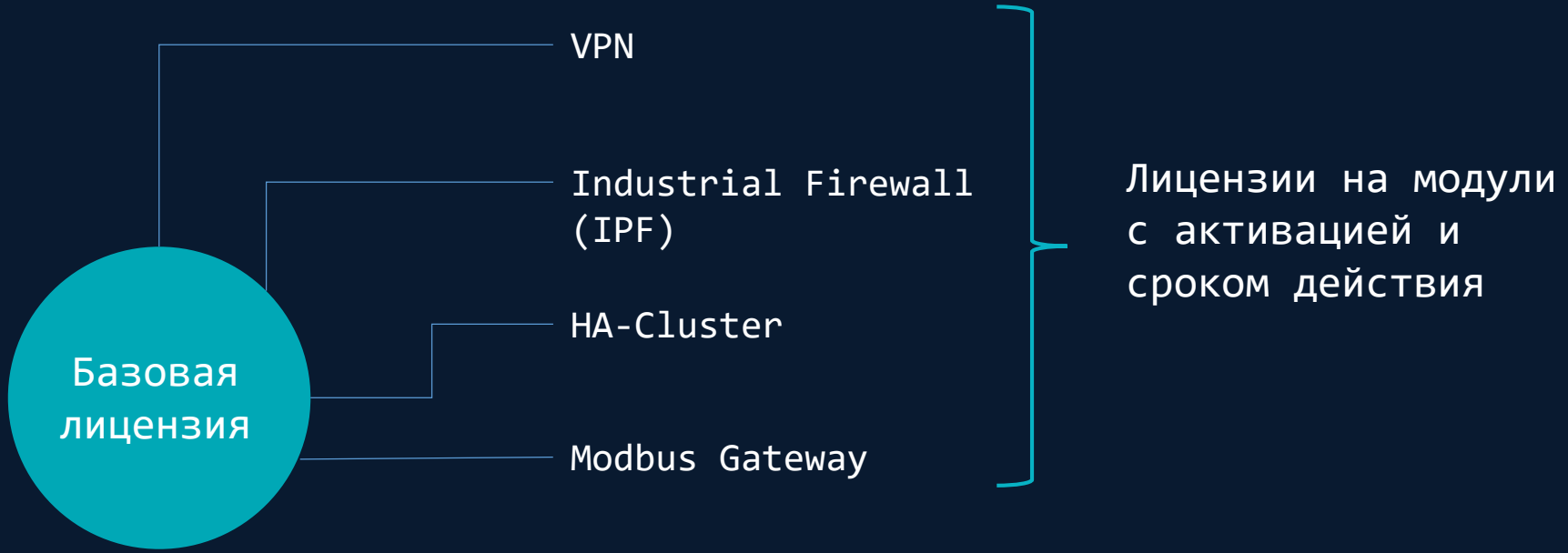
```
Root: ~$ info IPlir 6
[1] рекомендация по стандартизации
Р 1323565.1.034-2020  «Информационная
технология. Криптографическая защита
информации. Протокол безопасности сетевого
уровня»
[2] Разработана ТК26
```

КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ:

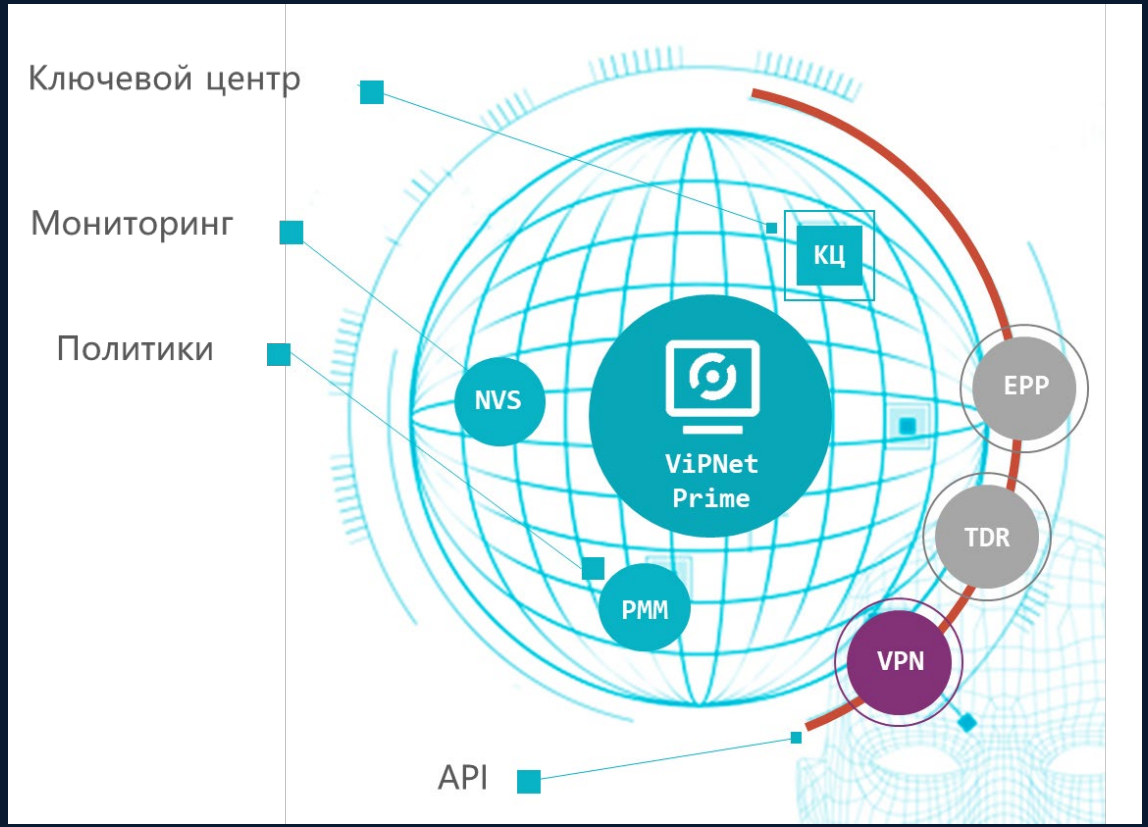
- IPlir 6 – протокол безопасности сетевого уровня

Новая схема лицензирования

Базовая лицензия: VPN для системы управления и межсетевой экран (SPI)- бессрочная



Новая система управления - ViPNet Prime



Совместимость

ViPNet Coordinator IG 5

ViPNet Coordinator IG10 I1

ViPNet Coordinator IG10 I2

ViPNet Coordinator IG100 I1

ViPNet Coordinator IG100 I4

ViPNet Coordinator IG100 I5

ViPNet Coordinator VA
Для тестов, не сертифицируется (шлюз и GPIO - через преобразователи).

ViPNet Coordinator IG1000 Q1

Только обновление с Coordinator IG 4

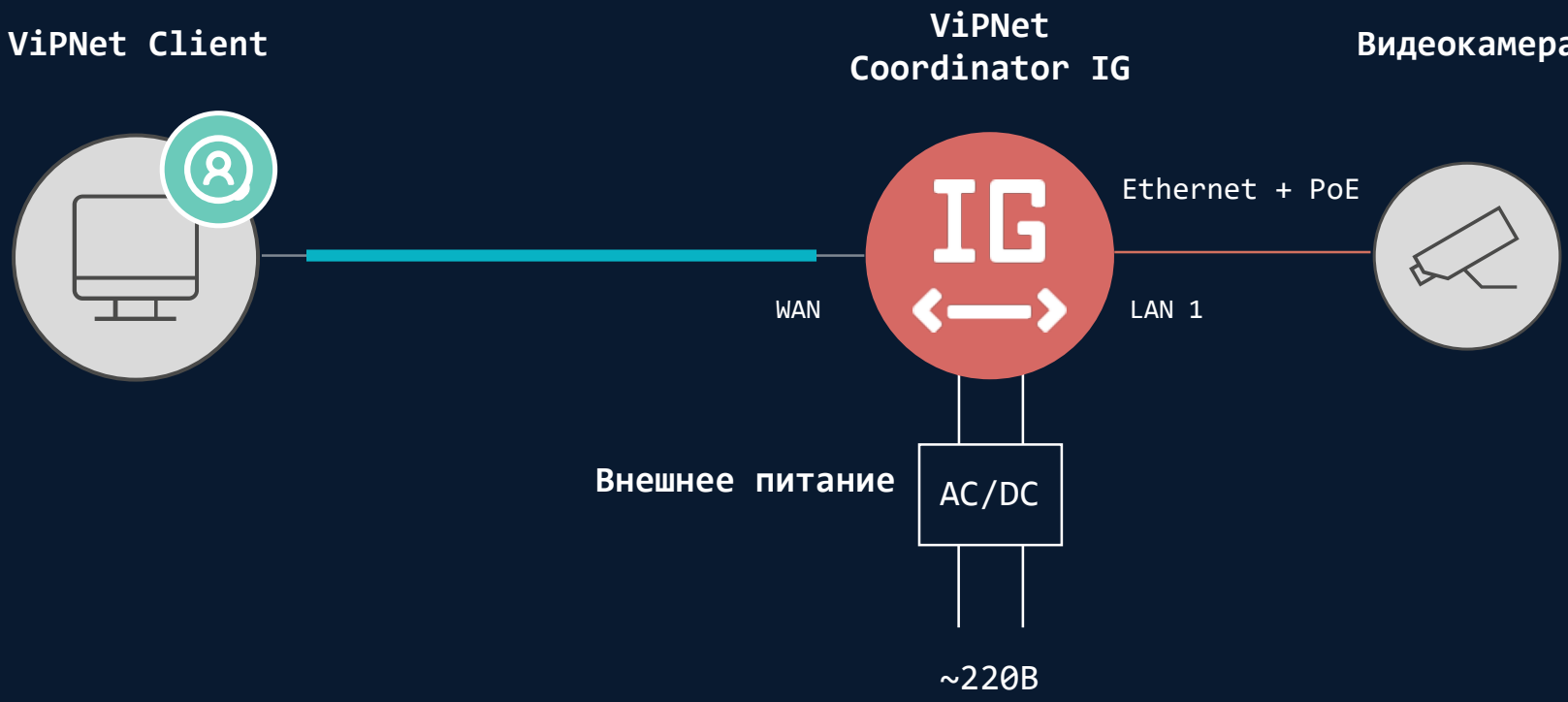
Новые поставки и обновление с Coordinator IG 4

Coordinator IG 5.2

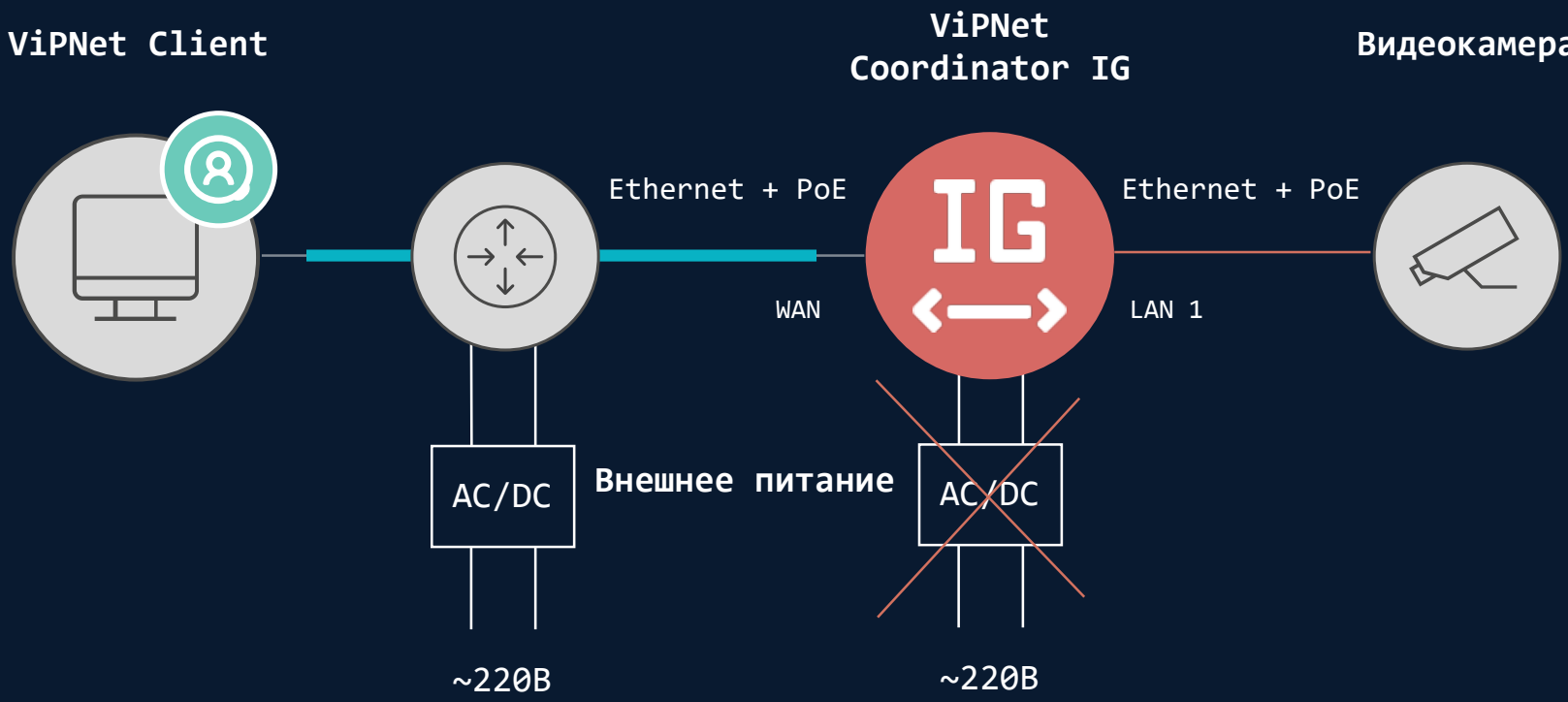
ViPNet Coordinator IG100 I5

- 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)

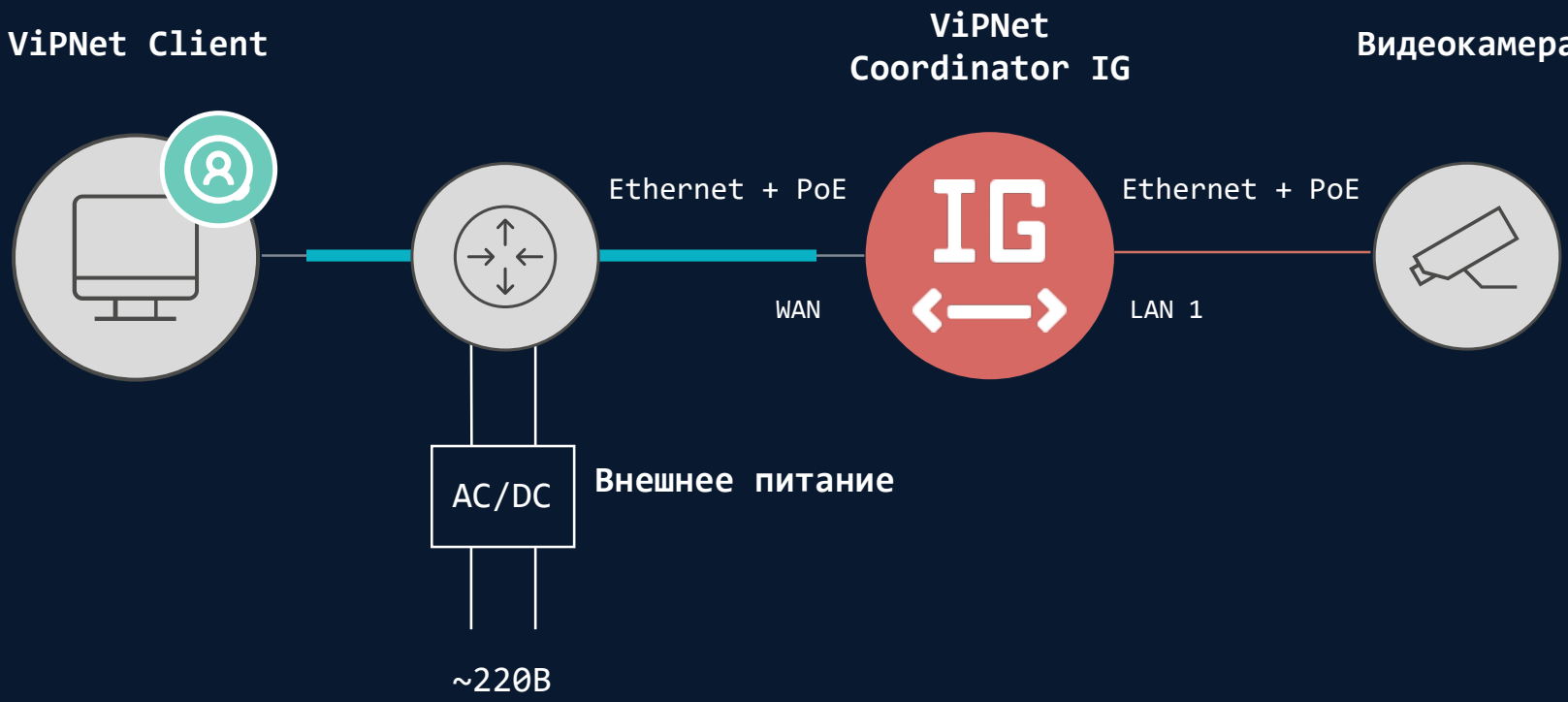
PoE-источник (PSE)



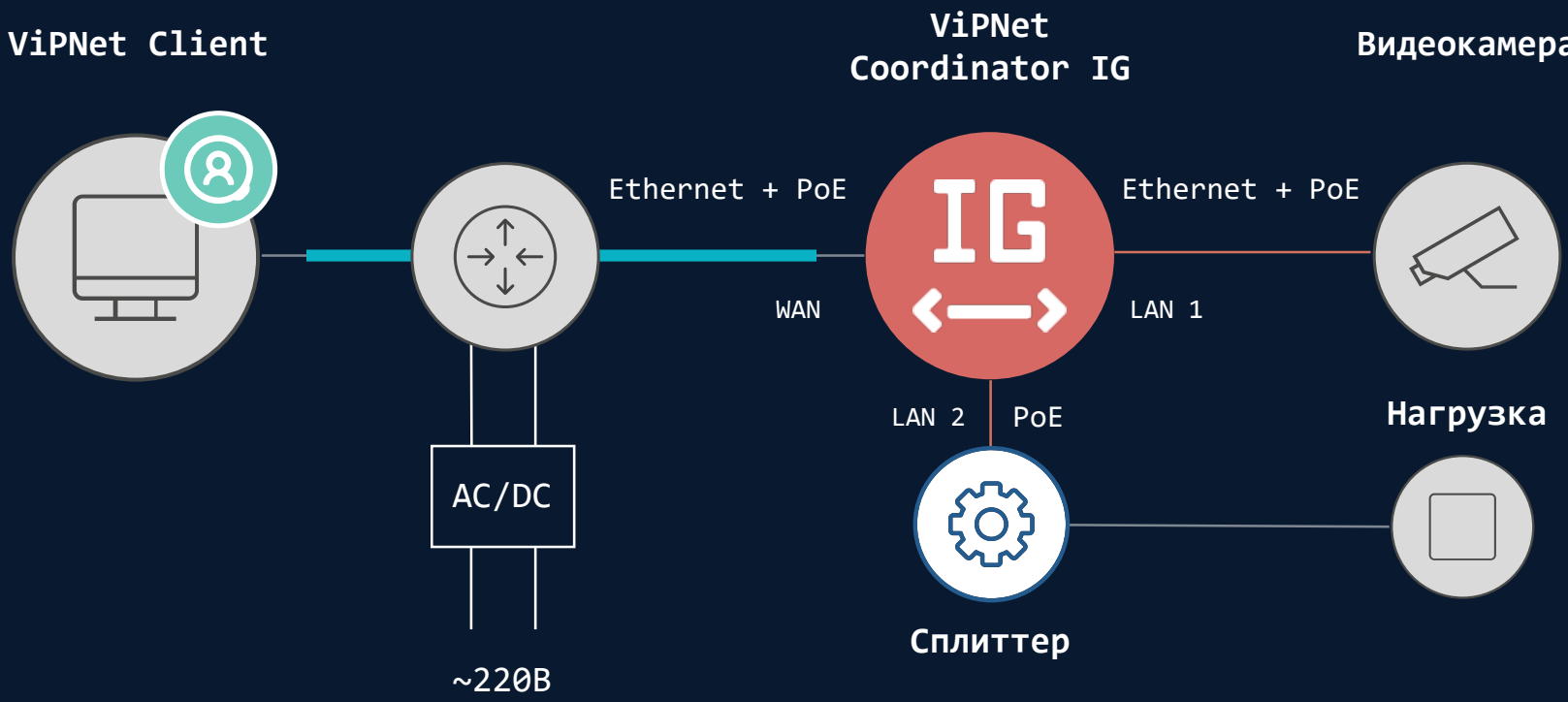
PoE-Delivery (PD + PSE)



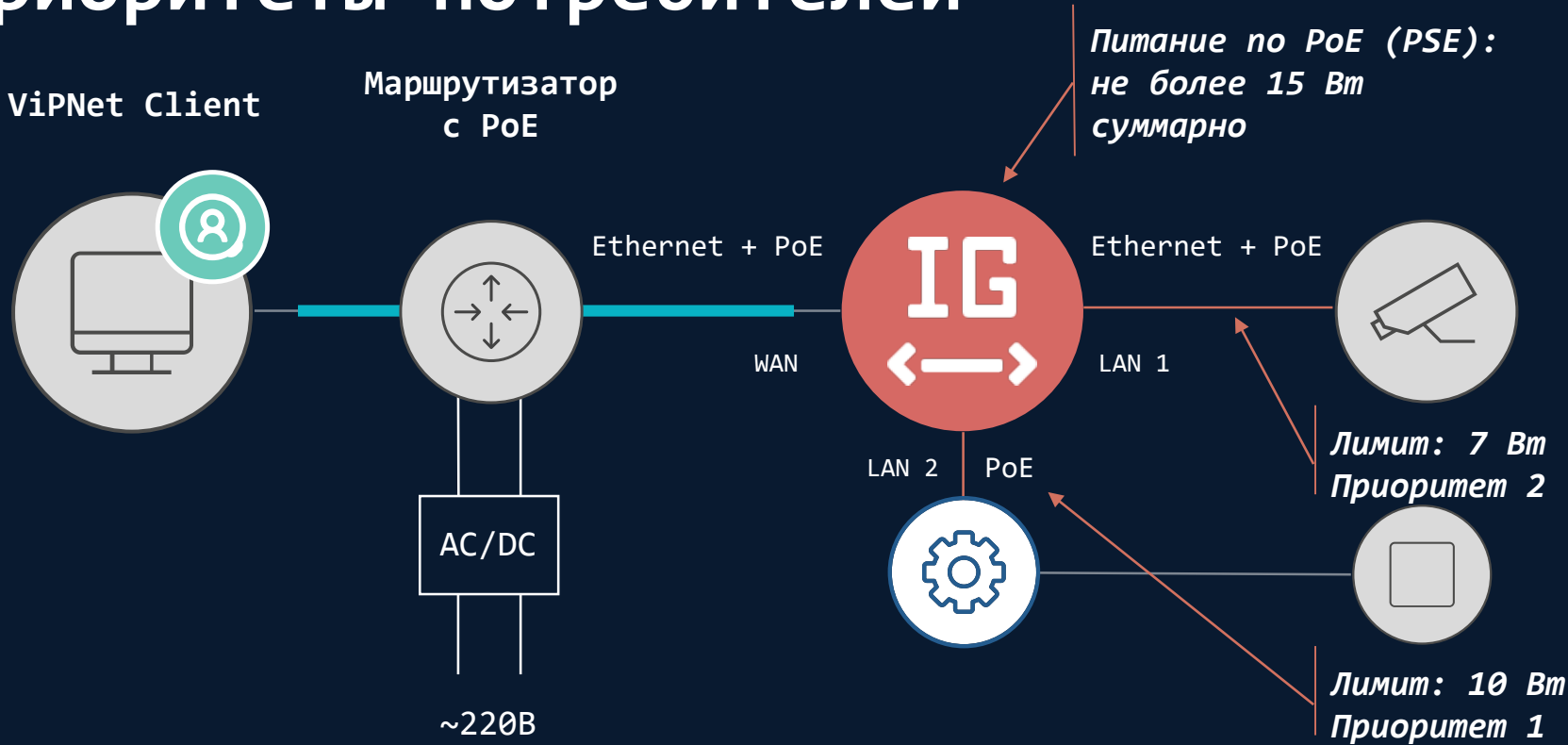
PoE-Delivery (PD + PSE)



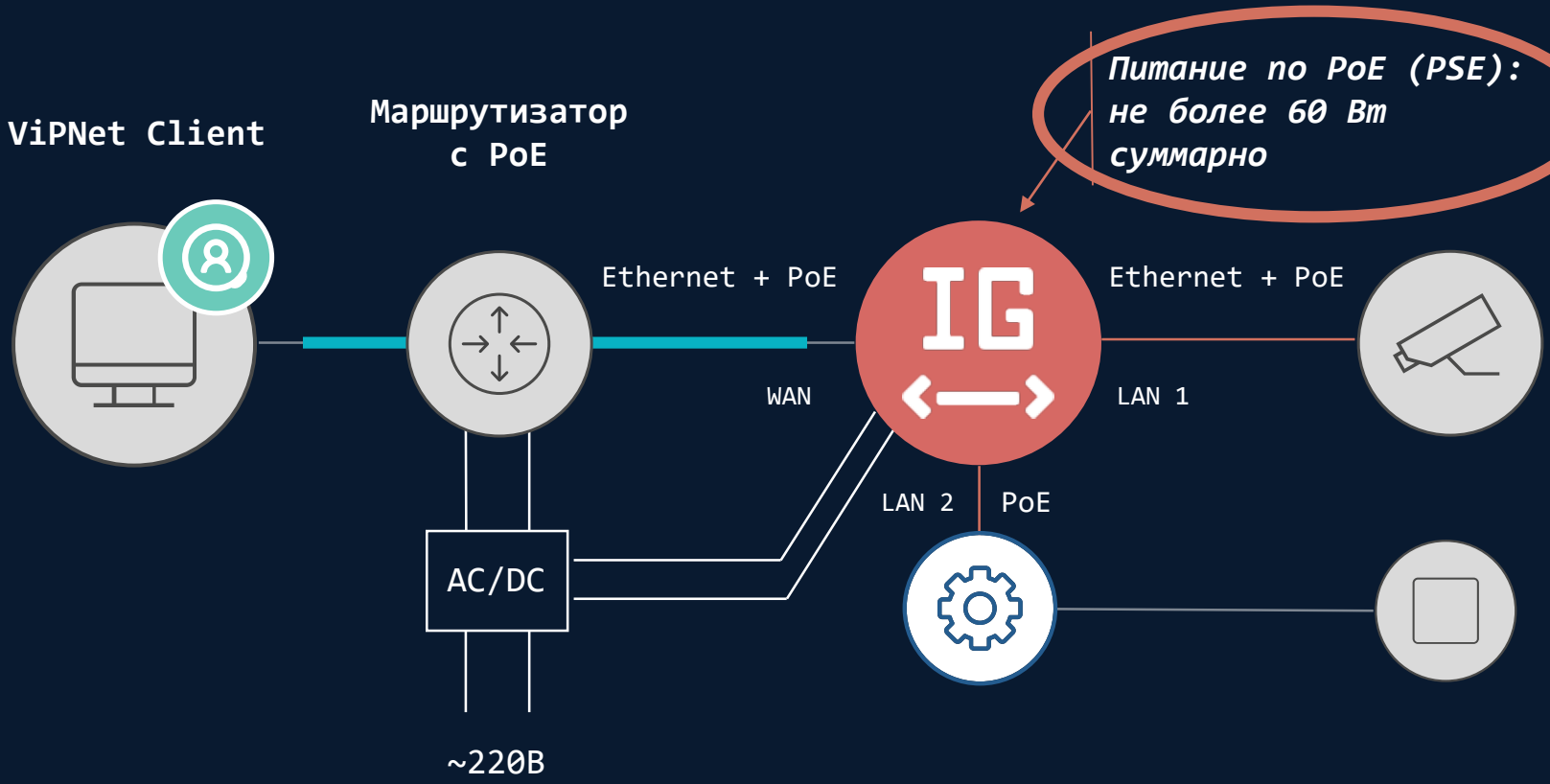
Питание потребителей по двум каналам



Ограничение мощности и приоритеты потребителей



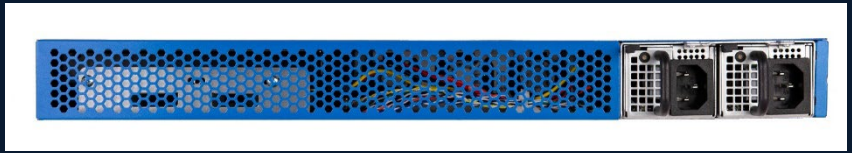
Power Delivery



Аппаратная платформа IG1000 Q1

Релиз 5.2.0, план – Q3 2024

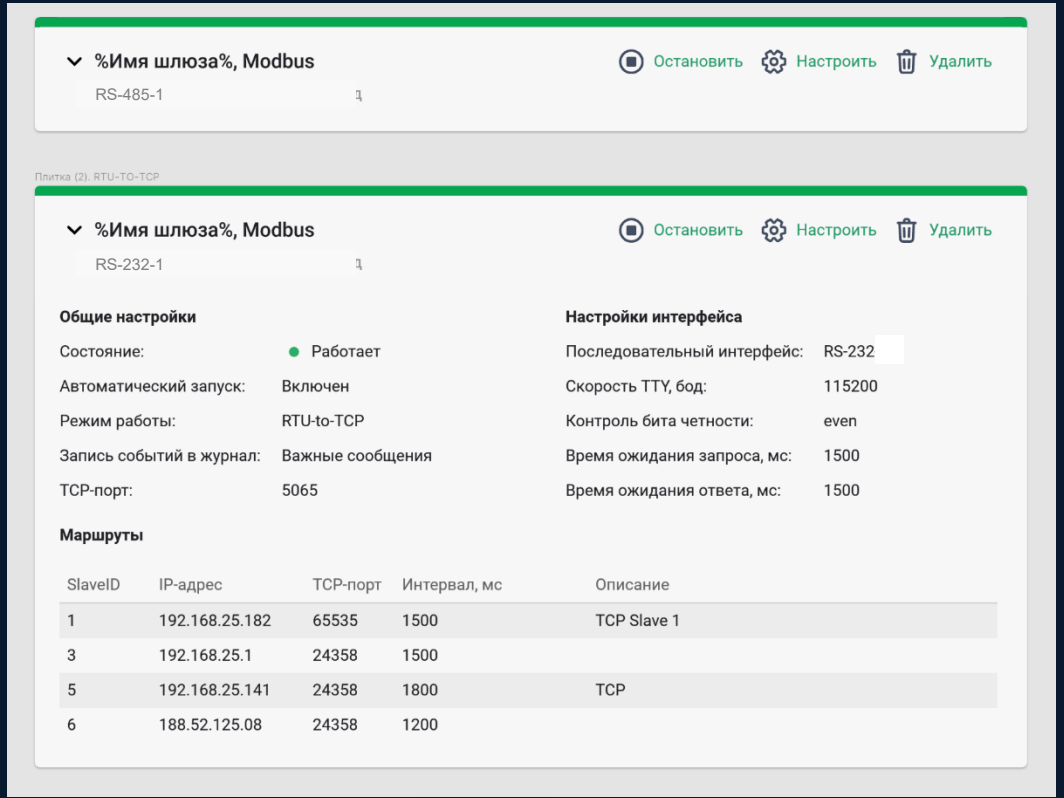
- VPN - 2 500 Мбит/с
- МЭ UDP 1518 байт - 2 800 Мбит/с
- МЭ TCP - 2 800 Мбит/с
- Application Control (МЭ + DPI) - 1 000 Мбит/с
- NGFW Throughput (МЭ + DPI + IPS) - 380 Мбит/с
- Количество соединений - 3 000 000
- Сетевые интерфейсы:
  - 4 x 1G RJ-45
  - 4 x 1G SFP
- GPIO



ViPNet Coordinator IG 5.2

Планы на 2024 г.

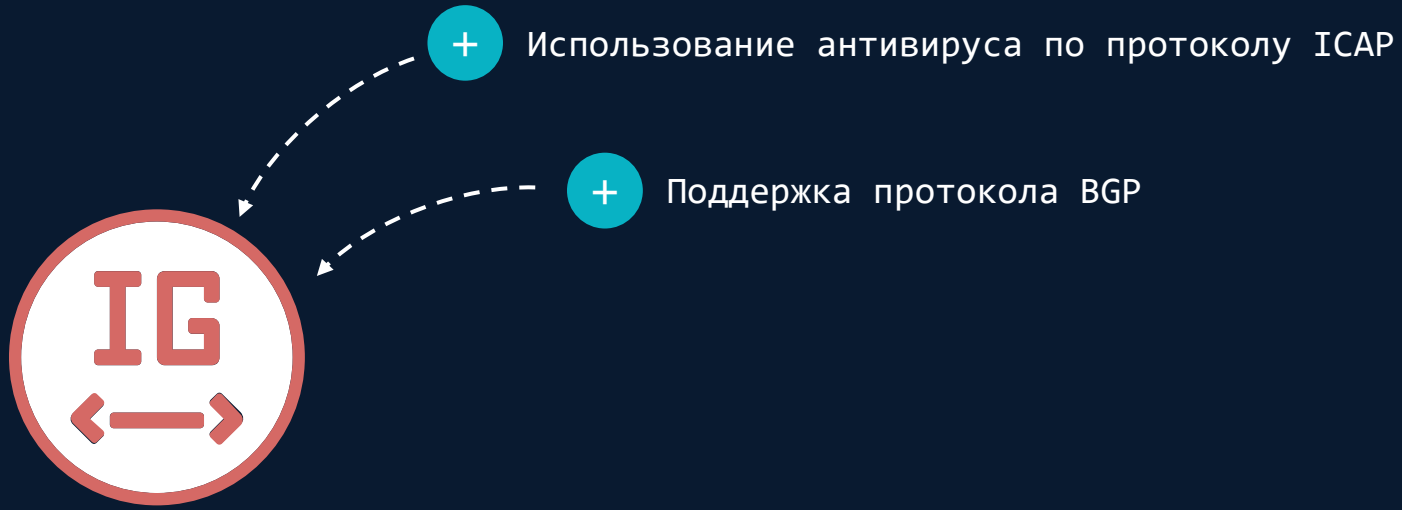
Два интерфейса для шлюзов



Только для новых платформ

ViPNet Coordinator IG 5.2

Планы на 2024 г.



Только для новых платформ – IG100 I4, I6, I7, IG1000 Q1

Сертификаты соответствия по требованиям ФСБ России

ViPNet Coordinator IG 4.3.3:

- Сертификат № СФ/124-4823 по требованиям к СКЗИ класса КС3 – до 04.2027
- Сертификат № СФ/525-4591 по требованиям к МЭ 4 класса – до 08.2024

ViPNet Coordinator IG 4.5.1:

- Ожидаем заключение

Сертификат соответствия по требованиям ФСТЭК России

ViPNet Coordinator IG 4.5.1:

Сертификат № 4379 до 03.2026

- 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) – включен как ПАК ViPNet Coordinator IG4 (14.05.2024)

IG 5.1 - сертификация

По требованиям ФСБ – тематические исследования идут,

ожидаемые сроки – Q4 2024-Q1 2025

Внесение в реестр Минцифры (ПО) – ожидаемый срок Q4 2024

Внесение в реестр Минпромторга – ожидаемый срок Q4 2024

ТЕХНО 2024 infotecs Фест

Андрей Иванов

Andrey.Ivanov2@infotecs.ru

Подписывайтесь на наши соцсети