

Индустриальный шлюз безопасности ViPNet Coordinator IG: линейка моделей, ВОЗМОЖНОСТИ

Андрей Иванов
Архитектор решений



техно infotecs
2023 Фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ



ViPNet Coordinator IG

Индустриальный
шлюз безопасности

Предназначен для:

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



Функционал

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



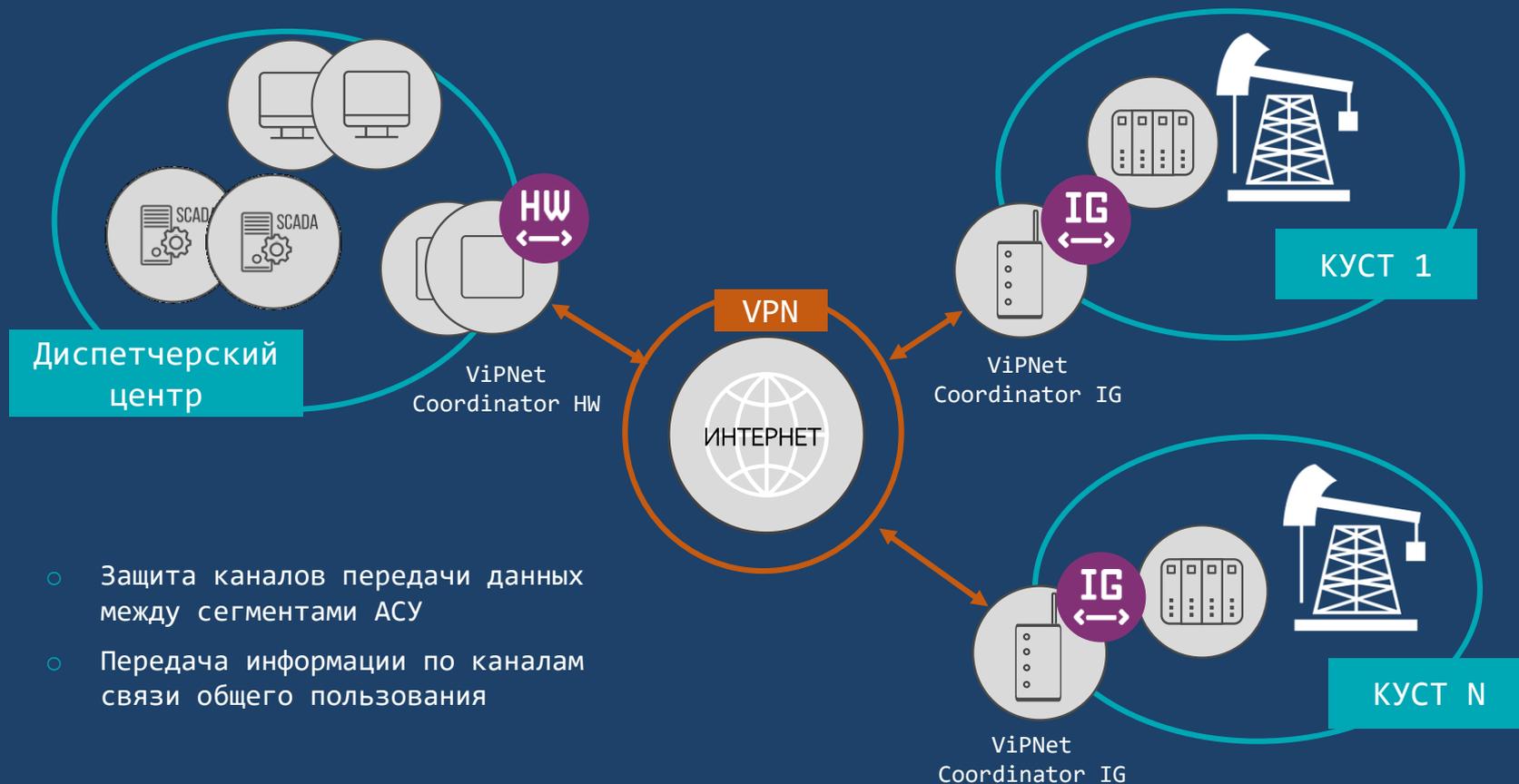
Криптографическая защита



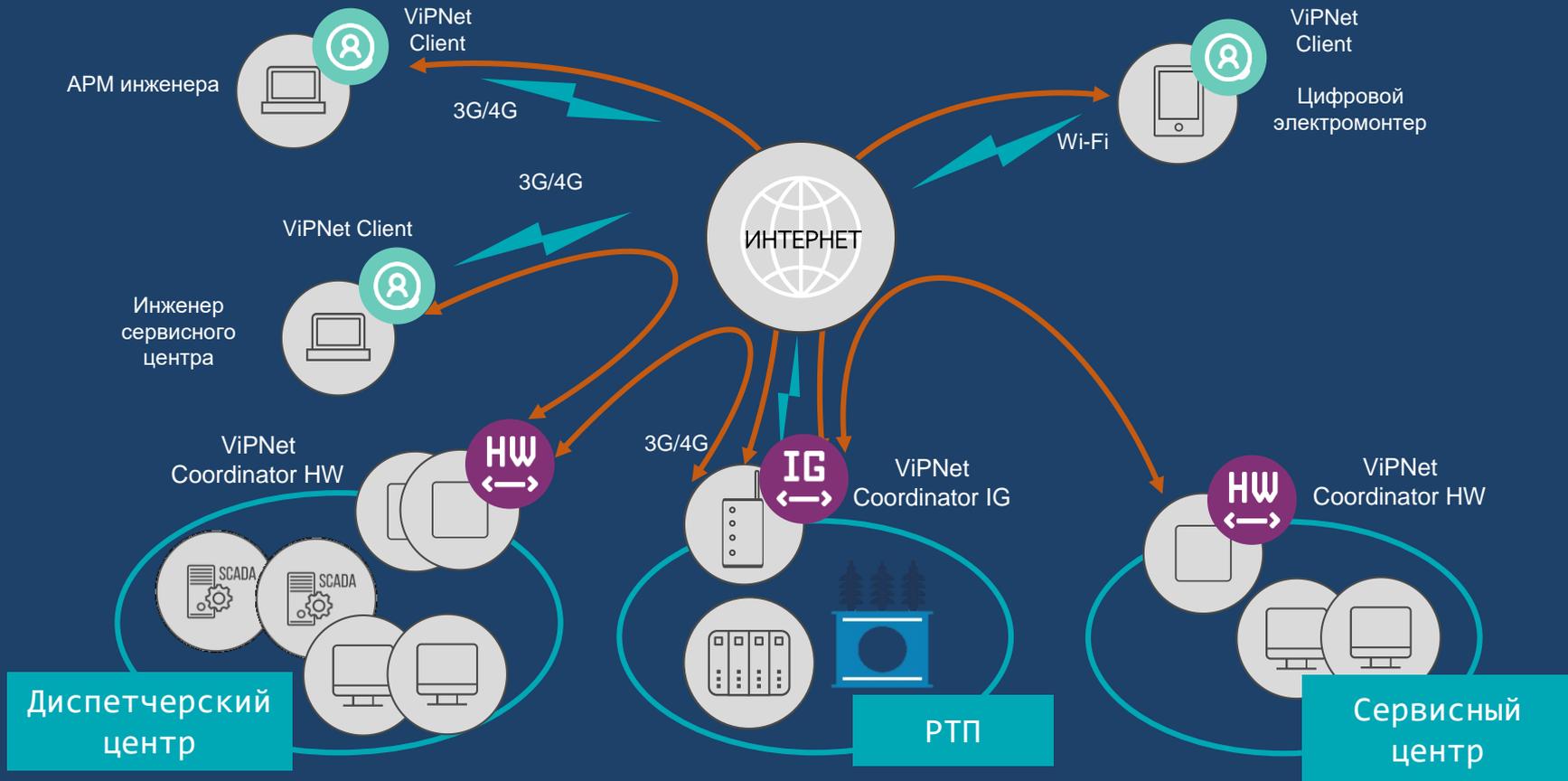
- каналов передачи данных с использованием алгоритмов ГОСТ
- каналов связи между сегментами АСУ
- каналов связи (в том числе беспроводных) при подключении к сетям связи общего пользования
- доступа удаленных и мобильных пользователей
- удаленного мониторинга
- подключения для сервисного обслуживания

Соответствие требованиям ФСБ России
к СКЗИ класса КСЗ

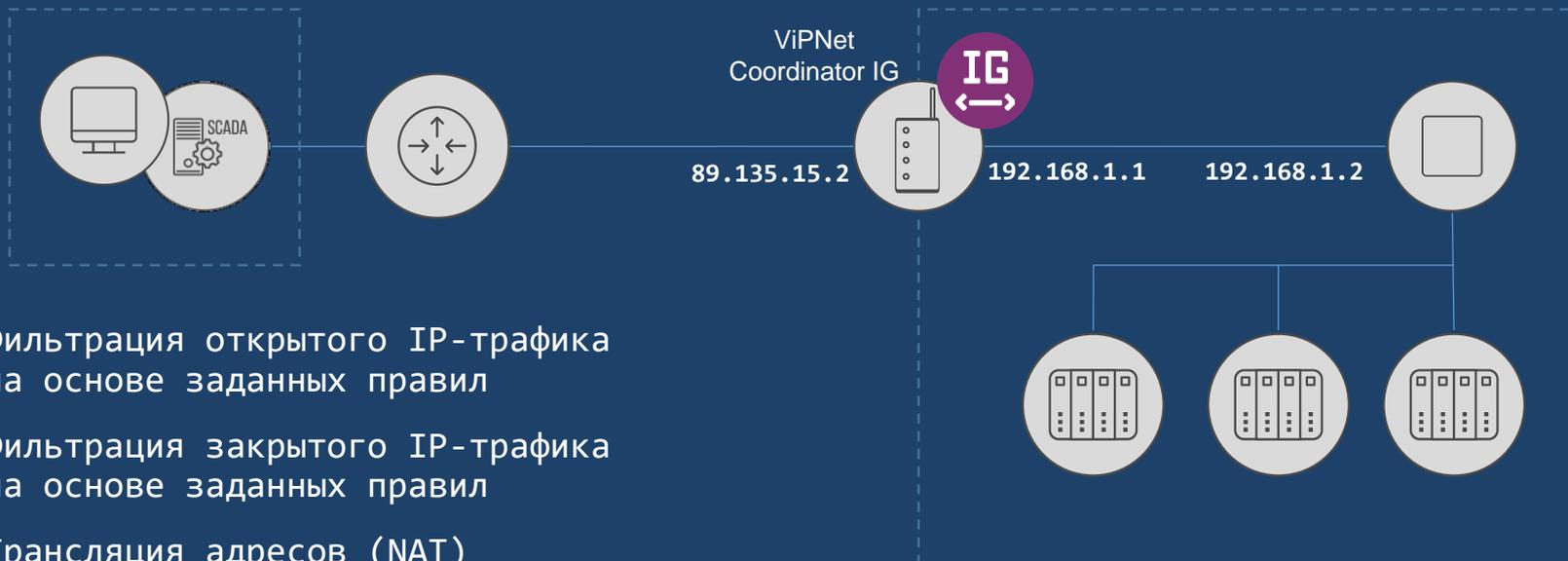
Защищенная сеть ViPNet



Защищенный удаленный доступ



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

Настройка набора правил фильтрации Modbus

Набор правил включен

Название набора:

[Правила транспортного уровня](#) [Правила прикладного уровня](#)

[+](#) Добавить

Таблица	Адрес сервера	Адрес клиента	Протокол	Порт назначения
Local	89.175.26.1	192.168.11.5	tcp	502
VPN	@local	0x00010201	tcp	24358

№	Статус	Имя	Действие	ID	FC	R	W
1	<input checked="" type="checkbox"/>	rule_1	✓ Пропуск...	1, 10-15	2, 3	100-200	Любой
2	<input checked="" type="checkbox"/>	rule_2	✗ Блокиро...	Любой	20	Любой	Любой

Фильтрация протокола МЭК 60870-5-104 (4.5.1)

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

Набор правил фильтрации протокола МЭК104 ✕

Набор правил активен

* Название набора правил:

Правила транспортного уровня Правила прикладного уровня Формат протокола

+ Добавить Правил: 57

№	Статус	Имя правила	Общий адрес	Адрес ОИ	Тип	Действие
⋮ 1	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить
⋮ 2	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	⊖ Блокировать
⋮ 3	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить
⋮ 4	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	⊖ Блокировать
⋮ 5	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить

Сохранить
Отмена

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:

Время по умолчанию на ожидание запроса: мс

Время по умолчанию на ожидание ответа: мс

Настройки интерфейса RS-232

Скорость TTY устройства: бод

Контроль бита четности:

Настройки интерфейса RS-485

Скорость TTY устройства: бод

Контроль бита четности:

Задержка до отправки: мс

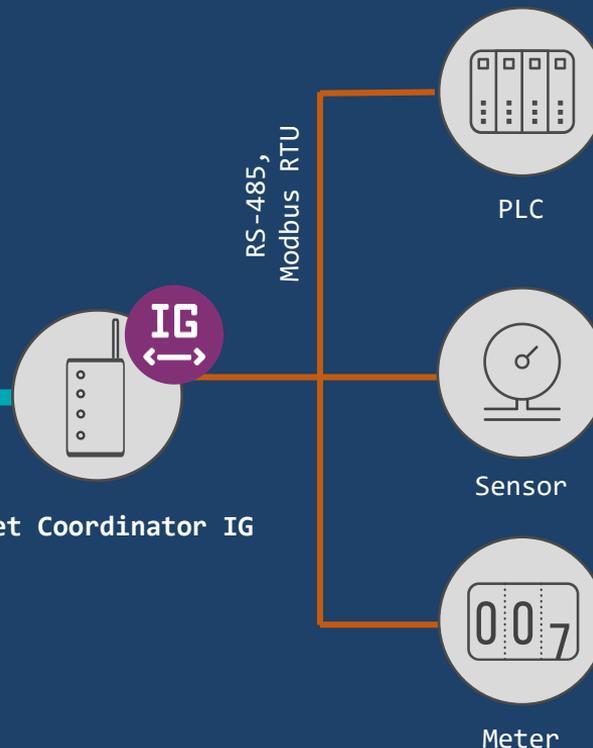
Задержка после отправки: мс

другой

S-485),

Ethernet,
Modbus TCP

ViPNet Coordinator IG



Сетевые сервисы

DNS
(client/server)

DHCP
(server/relay)

NTP
(client/server)

VLAN

QoS

EtherChannel

OSPF

Failover

Wi-Fi
(client/AP)

3G/LTE -modem

Шлюз Modbus
TCP/RTU

Сетевые сервисы L2

- VLAN
- Агрегирование интерфейсов

Создание VLAN интерфейса

Разрешено взаимодействие интерфейса с сервисами

Статус и основные настройки

Родительский интерфейс:

Идентификатор:

Класс:

Получаемые параметры

Получать параметры автоматически:

IP-адрес:

Маска:

DNS-сервера

NTP-сервера

Маршруты

Метрика:

Создание bond интерфейса

Разрешено взаимодействие интерфейса с сервисами

Статус и основные настройки

Идентификатор:

Класс:

Режим:

Сетевые интерфейсы:

Частота опроса: мс

Получаемые параметры

Получать параметры автоматически:

IP-адрес:

Маска:

DNS-сервера

NTP-сервера

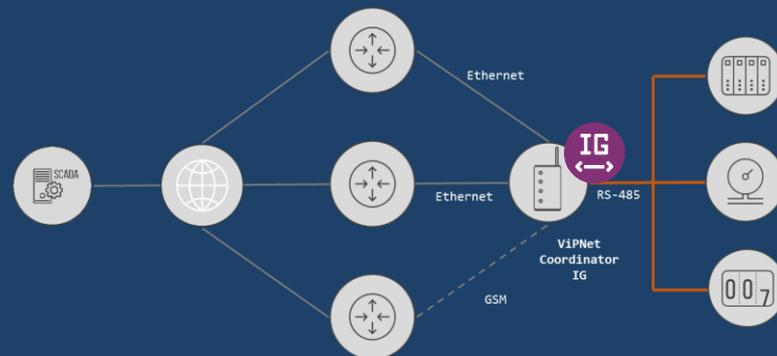
Маршруты

Метрика:

Сетевые сервисы L3

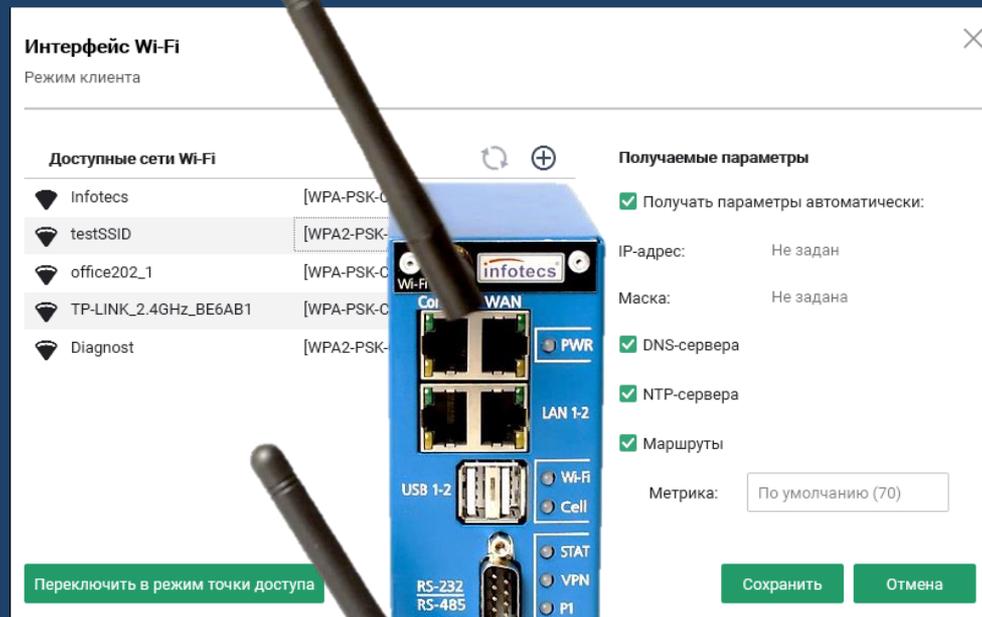
- Статическая и динамическая маршрутизация по протоколам DHCP/PPP и OSPF
- Резервирование каналов
- Балансировка трафика
- Обработка трафика в соответствии с приоритетом (поддержка протокола DiffServ)

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	



Wi-Fi

- Клиент
- Точка доступа



Внимание! Wi-Fi модуль устанавливается только на производстве!

GSM-модуль

Для установки можно выбрать один из видов GSM-модулей:

- 3G-модуль
- LTE-модуль

В комплект GSM-модуля входит внешняя GSM-антенна.

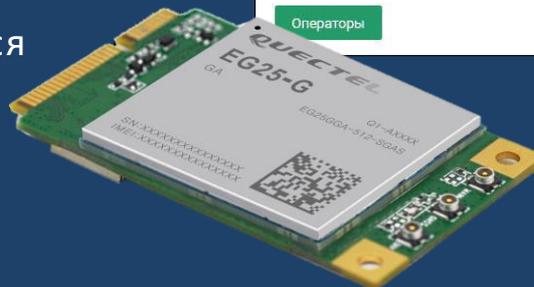
Внимание! GSM-модуль устанавливается только на производстве!

USB-модем подключен

Параметры подключения	Информация об устройстве	Получаемые настройки
Метод настройки:	Модель: 3G/4G	<input checked="" type="checkbox"/> DNS-сервера
Оператор (MNC): N/A (0)	Производитель: Quectel UC20	<input checked="" type="checkbox"/> Маршруты
Страна (MCC): N/A (0)	Уровень сигнала: (0 dBm)	Метрика: По умолчанию (60)
DNS-адрес APN: N/A	SIM-карта: Установлена	
Имя пользователя: N/A	PIN-код: Не задан	
Пароль: N/A		
Набираемый номер: N/A		

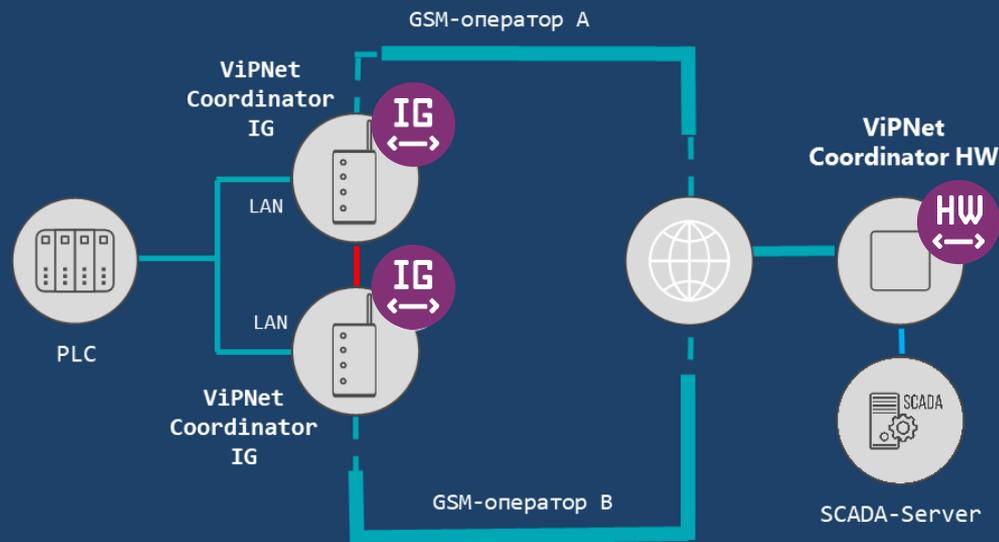
[Сбросить параметры подключения](#)

[Операторы](#) [Сохранить](#) [Отмена](#)



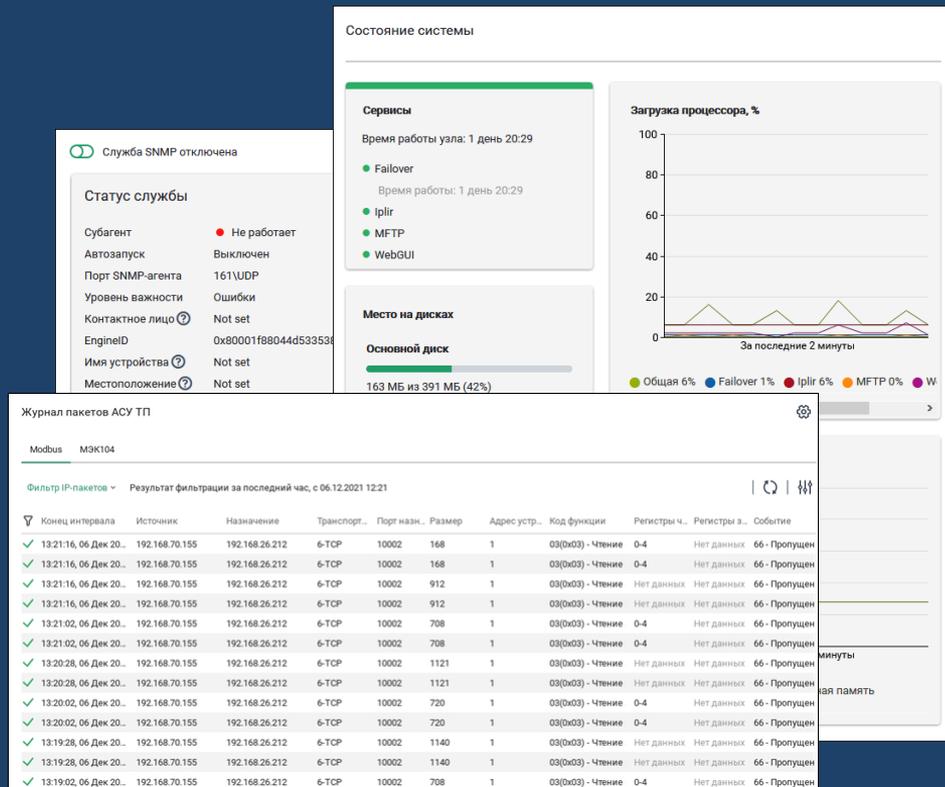
Отказоустойчивость

- Защита от 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

- Мониторинг состояния ViPNet Coordinator IG
- Мониторинг по протоколу SNMP
- Просмотр статистики IP-пакетов
- Просмотр журналов:
 - регистрации IP-пакетов
 - пакетов промышленных протоколов
 - транспортных конвертов (MFTP)
 - системного журнала
- Экспорт журналов по протоколу syslog



general-purpose input/output - интерфейс ввода/вывода общего назначения



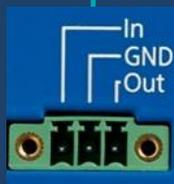
Входной сигнал

- Датчик вскрытия внешнего шкафа
- Переключение режима работы МЭ типа Д
- Сигнал с пользовательского устройства



Выходной сигнал

- Кластер с шлюзом Modbus TCP-RTU.
- Индикатор событий:
 - работа в регламентном обслуживании
 - работа в штатном режиме
 - работа в специальном режиме
 - вскрыт шкаф
 - сигнал с пользовательского устройства



ViPNet Coordinator IG



ViPNet
Coordinator
IG10 I1



ViPNet
Coordinator
IG100 I1



ViPNet
Coordinator
IG10 I2



ViPNet
Coordinator
IG100 I4



ViPNet
Coordinator
IG100 I5

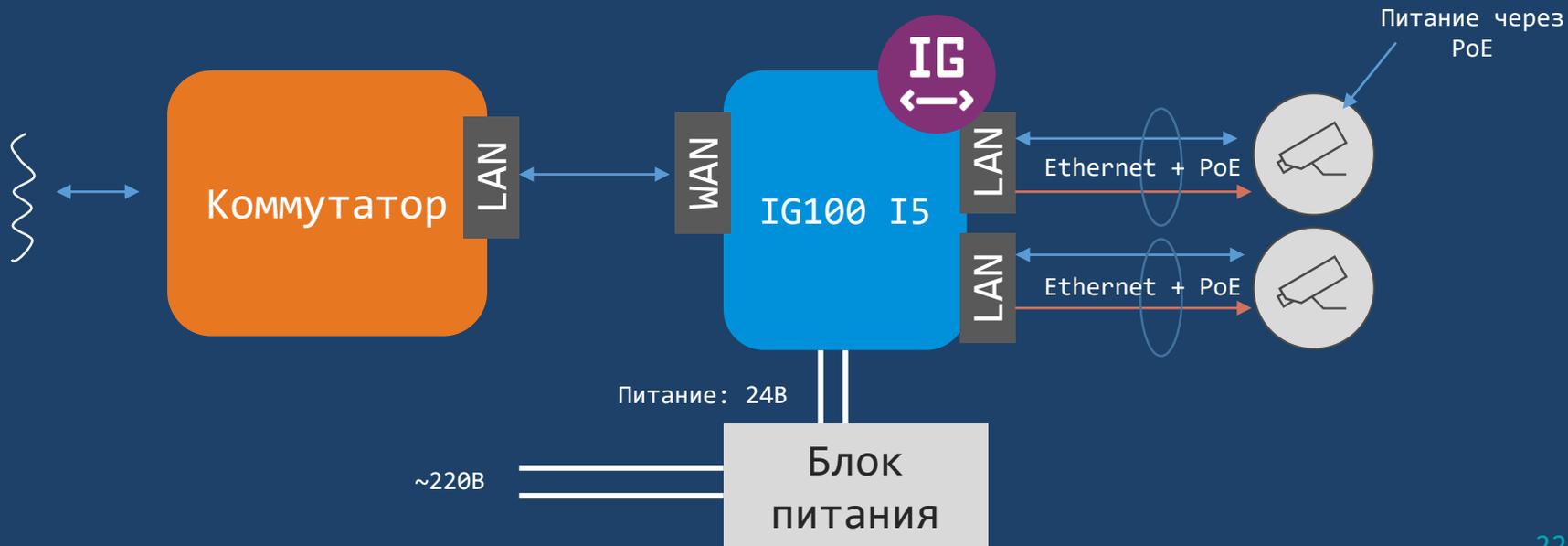
Сертифицированные
исполнения

Ближайшие планы

VIPNet Coordinator IG100 I5

Сценарий 1: PoE-источник

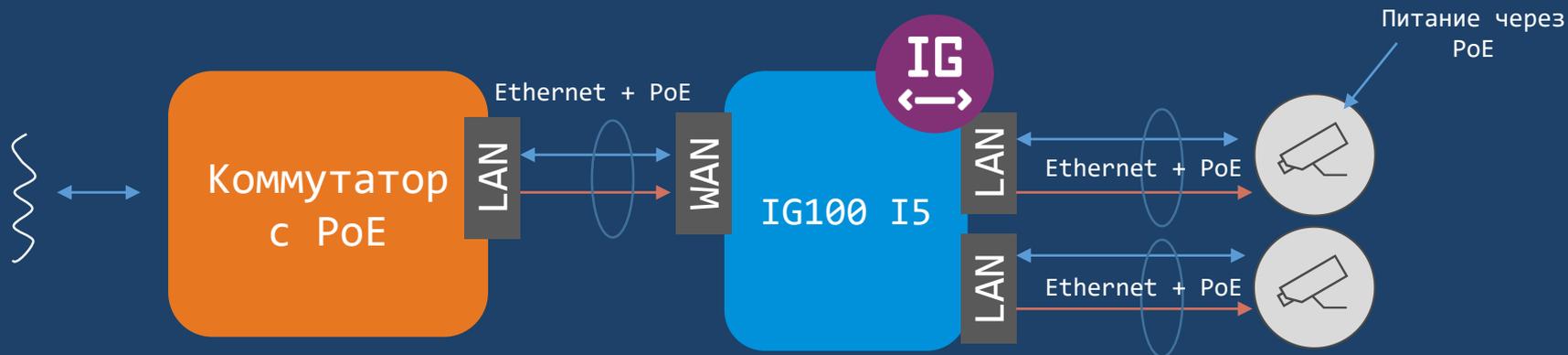
- Питание устройств, подключенных к IG
- Приоритезация питания подключенных устройств



VIPNet Coordinator IG100 I5

Сценарий 2: Power Delivery

- Питание самого IG от устройства с PoE
- Питание устройств, подключенных к IG
- Приоритезация питания подключенных устройств





Сертификация

Сертификаты соответствия по требованиям ФСБ России



ViPNet Coordinator IG 4.3.3:

- Сертификат № СФ/124-4247 по требованиям к СКЗИ класса КСЗ
- 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 4.3.3:

- 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)

Сертификация по требованиям Минкомсвязи России



Получены сертификаты на ПАК ViPNet Coordinator IG 4.3.x для применения на сетях связи общего пользования и технологических сетях связи как оборудование маршрутизации и коммутации пакетов и как базовая станция для беспроводной передачи данных стандарта 802.11 b/g частотой 2,4 ГГц:

- № ОС-4-РД-1385 – на ViPNet Coordinator IG10 I1 и ViPNet Coordinator IG100 I1
- № ОС-4-РД-1384 – на ViPNet Coordinator IG10 I2

Зарегистрированы декларации на ПАК ViPNet Coordinator IG на АП IG10 I1, IG10 I2, IG100 I1 по требованиям:

- к абонентским станциям стандарта GSM-900/1800, UMTS, LTE, LTE-Advanced
- к оборудованию проводных и оптических систем передачи абонентского доступа

Реестры РПО, ТОРП, РЭП



- ПО ViPNet Coordinator IG включен в реестр российского ПО – рег.номер 5102 (19.01.2019)
- ПАК ViPNet Coordinator IG включен в реестр телекоммуникационного оборудования российского происхождения (ТОРП) и в единый реестр российской радиоэлектронной продукции (реестр РЭП) (продление от 06.2022г.)



Ответы на вопросы

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363



Спасибо за внимание!

Андрей Иванов

e-mail: Andrey.Ivanov2@infotecs.ru

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363