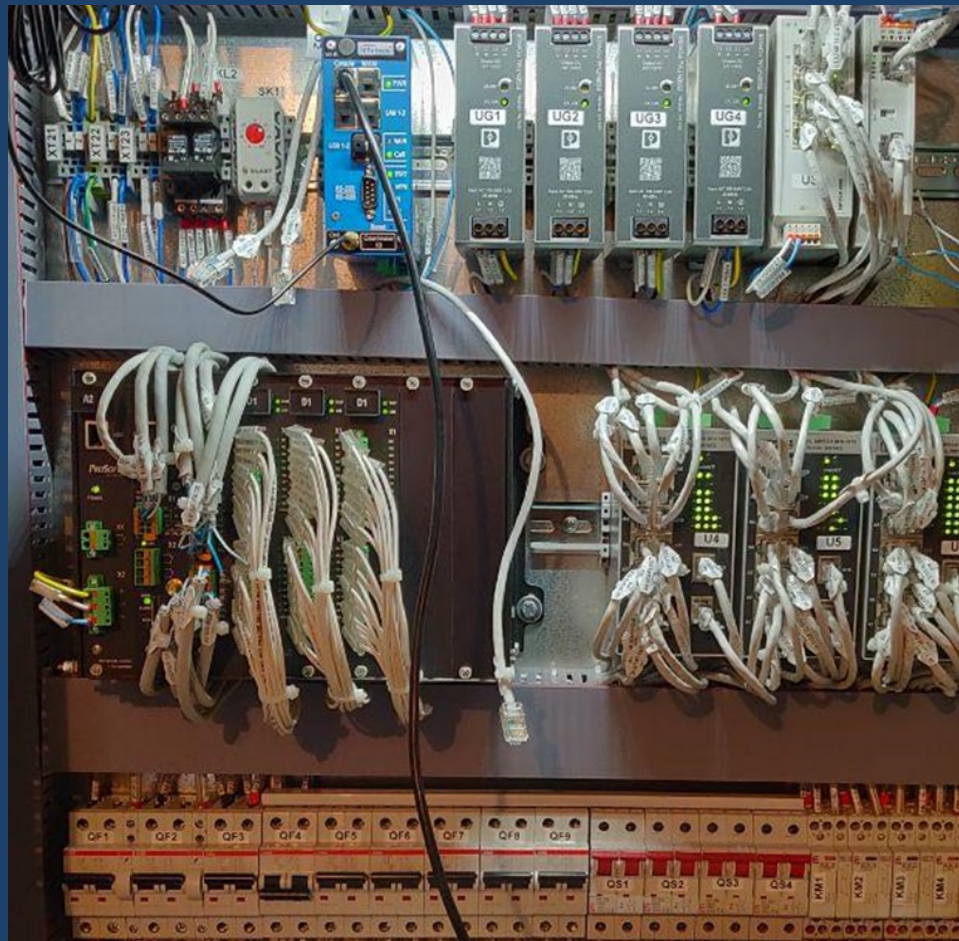


Межсетевой экран и криптошлюз для АСУТП и не только

Андрей Иванов
Архитектор решений



Индустриальный шлюз безопасности

VIPNet
Coordinator IG

Предназначен для:

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



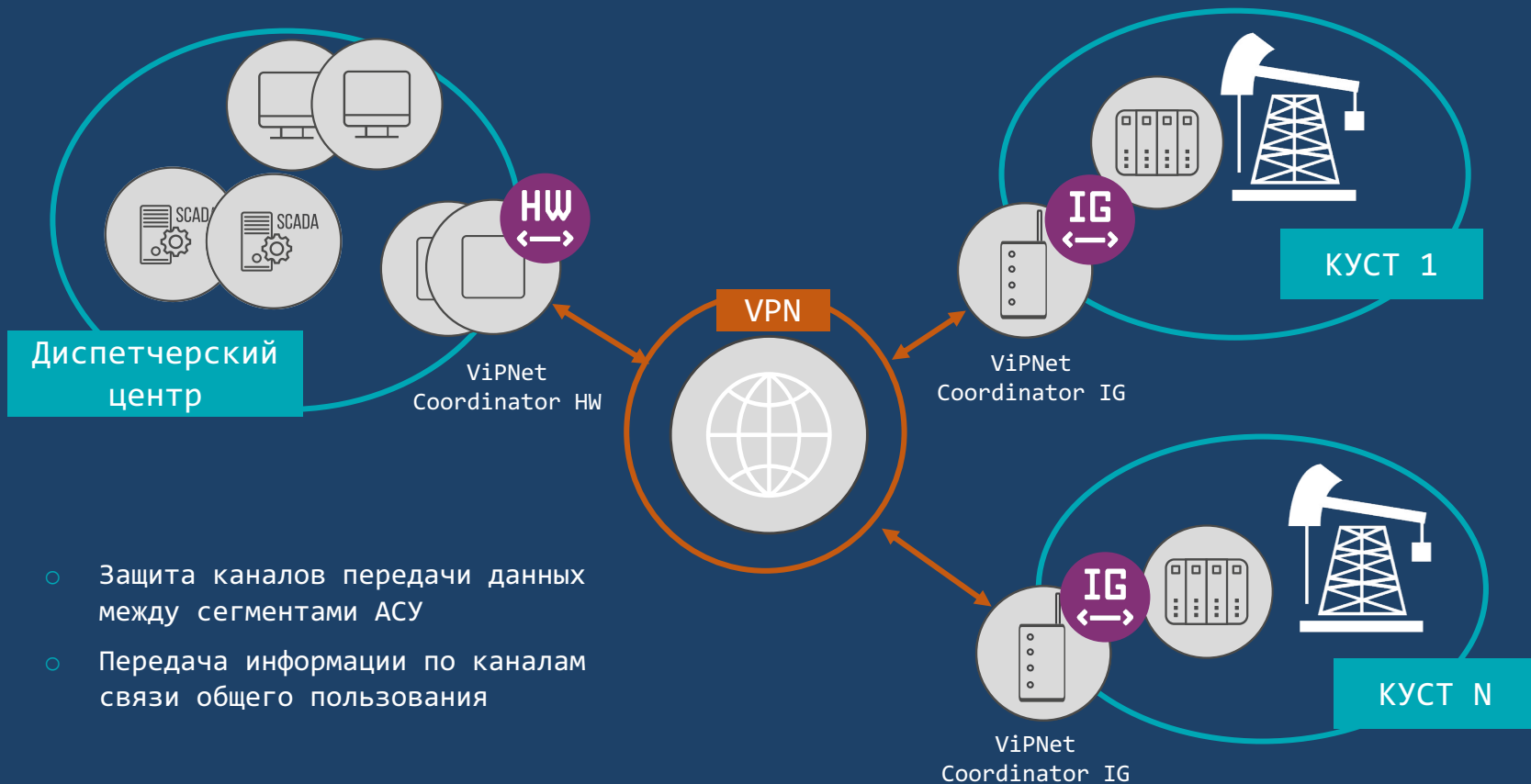
Криптографическая защита



- каналов передачи данных с использованием алгоритмов ГОСТ:
 - между сегментами АСУ
 - при подключении к сетям связи общего пользования
- доступа удаленных и мобильных пользователей

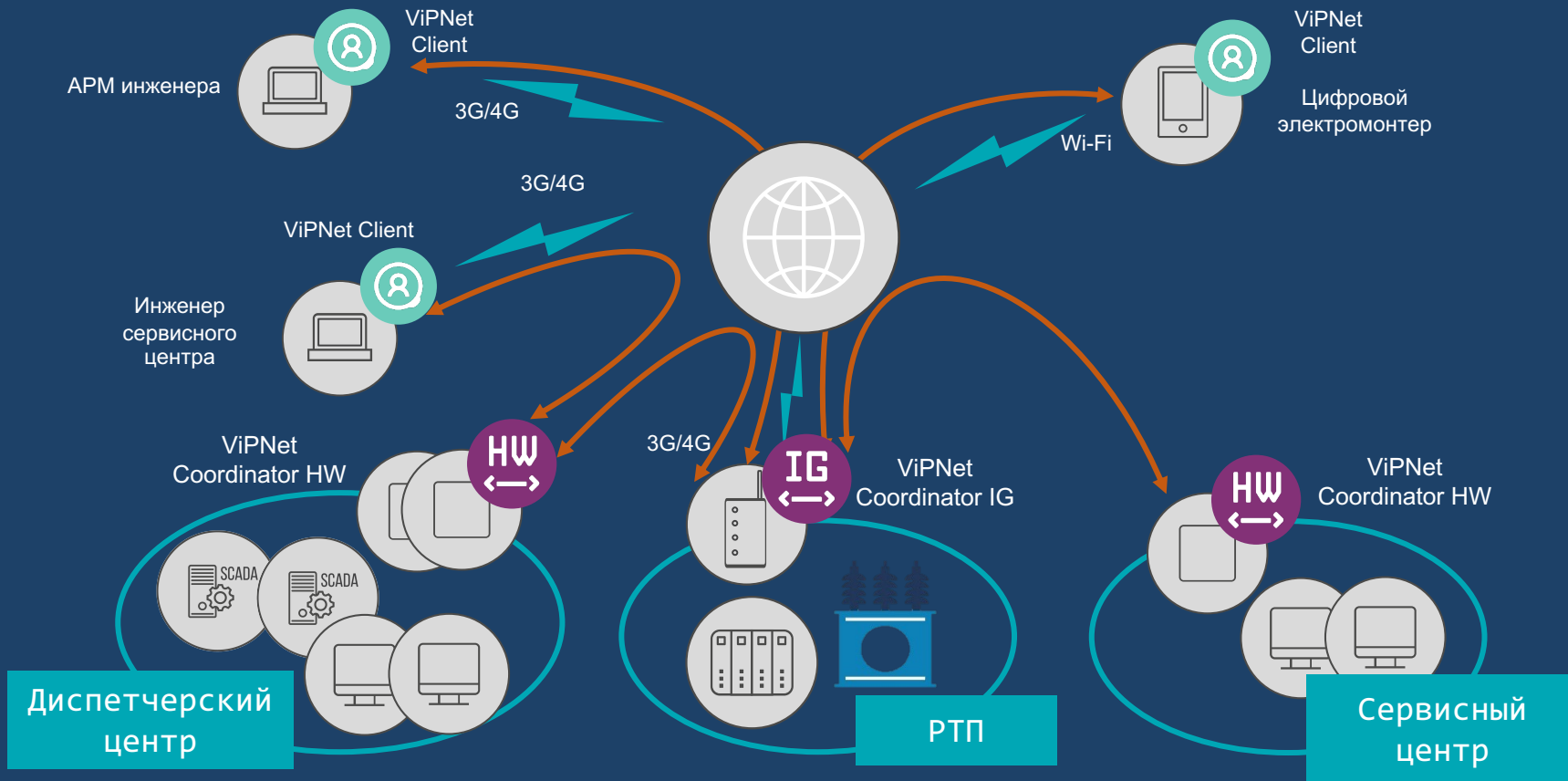
Соответствует требованиям ФСБ России к СКЗИ класса КСЗ

Защищенная сеть ViPNet

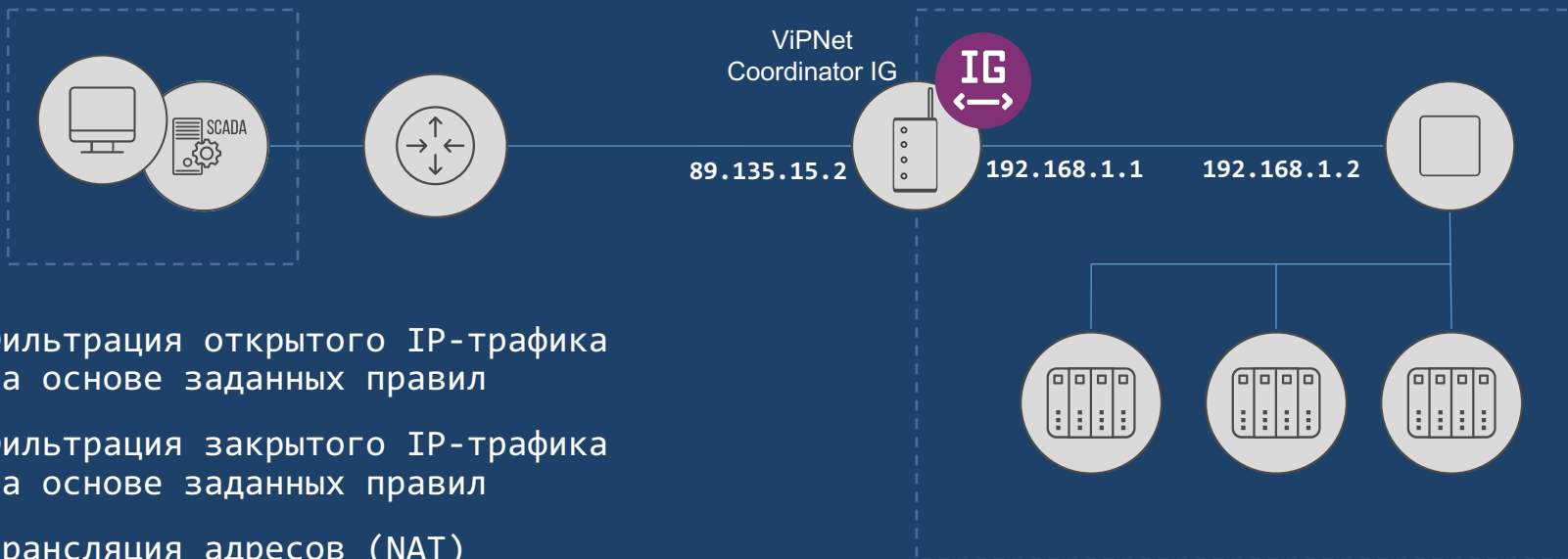


- Защита каналов передачи данных между сегментами АСУ
- Передача информации по каналам связи общего пользования

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 протоколов

Modbus

- Номер порта
- Адреса устройств
- Коды функций
- Регистры чтения и записи

МЭК 60870-5-104

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

Настройка набора правил фильтрации Modbus

Набор правил включен

Название набора:

Правила транспортного уровня

[+](#) Добавить

Таблица	Адрес устройства
Local	89.175.200.1
VPN	@local

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](#)

№	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

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

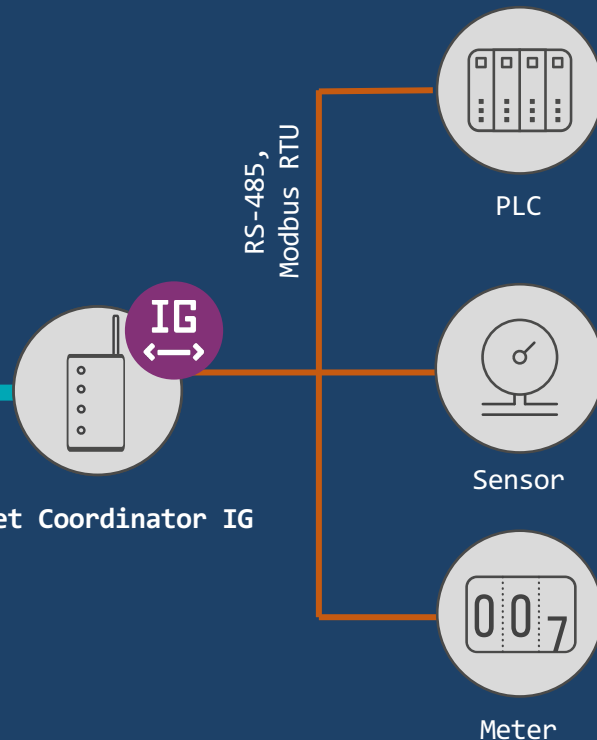
Задержка после отправки: мс

другой

(S-485),

Ethernet,
Modbus TCP

VipNet Coordinator IG



Сетевые сервисы

Уровень L2

- VLAN
- Агрегирование интерфейсов

Уровень L3

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

Создание VLAN интерфейса

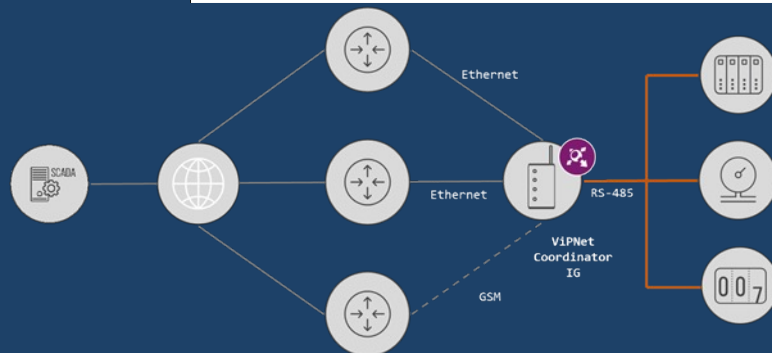
Создание bond интерфейса

Разрешено взаимодействие интерфейса с сервисами

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, GSM

Wi-Fi модуль:

- Клиент
- Точка доступа

GSM-модуль:

- 3G-модуль
- LTE-модуль

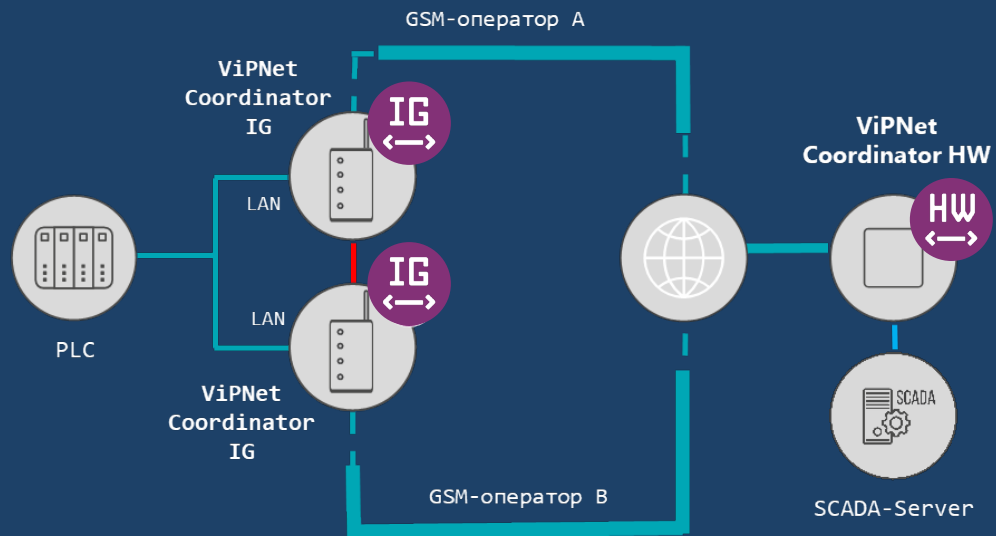
В комплекты модулей входят внешние антенны

Внимание! Wi-Fi и GSM-модули устанавливаются только на производстве!



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

Состояние системы

Сервисы
Время работы ула: 1 день 20:29

- Failover
- Iplir
- MFTP
- WebGUI

Место на дисках
Основной диск
163 МБ из 391 МБ (42%)

Загрузка процессора, %
За последние 2 минуты

Общая 6% Failover 1% Iplir 6% MFTP 0% W

Журнал пакетов АСУ ТП

Modbus МЭК104

Фильтр IP-пакетов Результат фильтрации за последний час, с 06.12.2021 12:21

✓	Конец интервала	Источник	Назначение	Транспорт.	Порт назн.	Размер	Адрес устр.	Код функции	Регистры ч.	Регистры з.	Событие
✓	13:21:16, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	168	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	168	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	912	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	912	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:21:02, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:02, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:20:28, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	1121	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:20:28, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	1121	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:20:02, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	720	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:20:02, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	720	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:19:28, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	1140	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:19:28, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	1140	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:19:02, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен

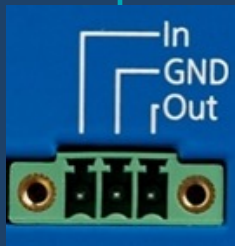
Ввод/вывод для внешних устройств

GPIO - интерфейс ввода/вывода общего назначения

Входной сигнал



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



Выходной сигнал

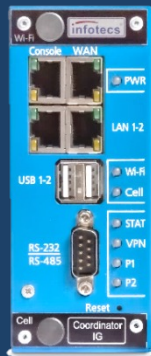


- Кластер с шлюзом Modbus TCP-RTU.
- Индикатор событий:
 - работа в регламентном обслуживании
 - работа в штатном режиме
 - работа в специальном режиме
 - вскрыт шкаф
 - сигнал на пользовательское устройство

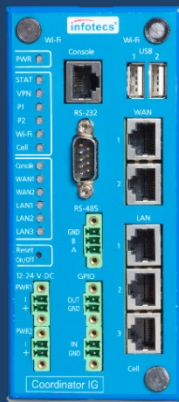
Исполнения



ViPNet
Coordinator
IG10 I1



ViPNet
Coordinator
IG100 I1



ViPNet
Coordinator
IG10 I2



ViPNet
Coordinator
IG100 I4



ViPNet
Coordinator
IG100 I5

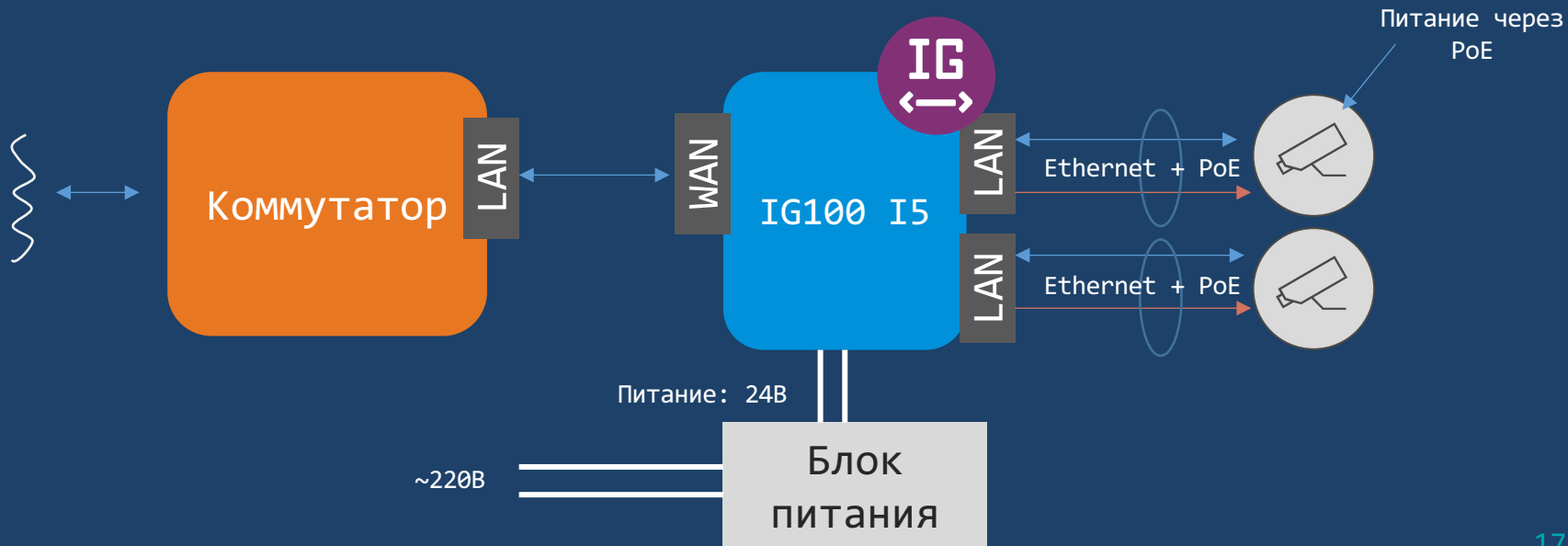
Сертифицированные
исполнения

Ближайшие планы

VIPNet Coordinator IG100 I5

Сценарий 1: PoE-источник

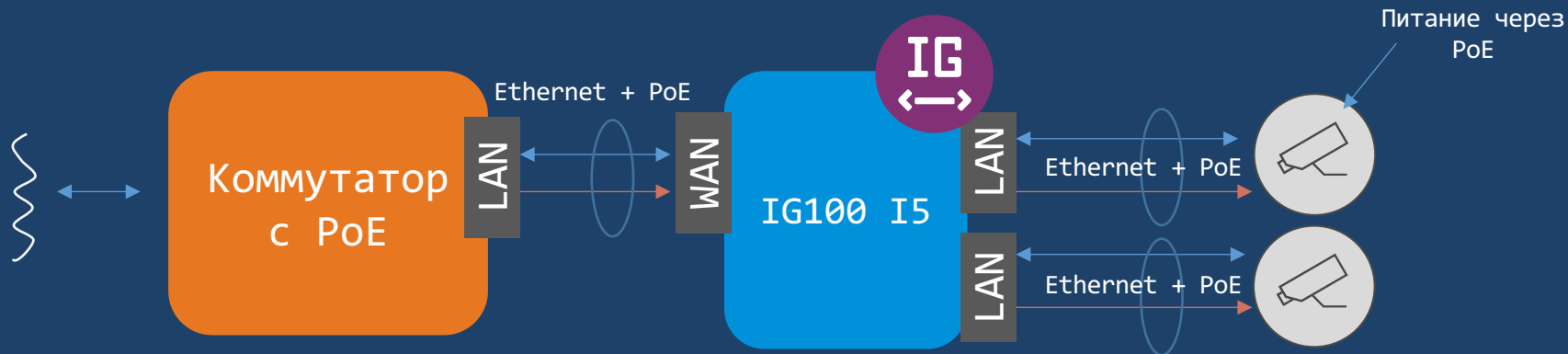
- Питание устройств, подключенных к IG
- Приоритезация питания подключенных устройств



VIPNet Coordinator IG100 I5

Сценарий 2: Power Delivery

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



Сертификаты соответствия

ViPNet Coordinator IG 4.3.3

По требованиям ФСБ России

- СКЗИ класса КСЗ

По требованиям ФСТЭК России

- Требования к МЭ
- Профиль защиты МЭ типов А,Б,Д 4 класса защиты
- 4 уровень доверия по ТДБ (2020 г)

По требованиям Минкомсвязи России

- Оборудование маршрутизации и коммутации пакетов, базовая станция стандарта 802.11 b/g частотой 2,4 ГГц:
- Декларации соответствия 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.)



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