ViPNet Coordinator IG. Практика применения

Марина Сорокина

ViPNet Coordinator IG 4.3.2

Индустриальный шлюз безопасности ViPNet Coordinator IG 4

Предназначен для использования:

- в ГИС до класса защищенности К1 включительно
- в АСУ ТП до класса защищенности К1 включительно
- в ИС для обеспечения 1 и 2 уровня защищенности персональных данных
- в ИС, ИТС и АСУ критической информационной инфраструктуры (КИИ) до 1 категории значимости

ViPNet Coordinator IG

- защита периметра сети
- сегментирование сети и разграничение доступа к ее сегментам
- защита проводных и беспроводных каналов связи сети
- организация ДМЗ
- управление сетевыми потоками
- сокрытие реальных адресов и архитектуры сети
- организация удаленного доступа для стационарных и мобильных пользователей, в том числе с мобильных устройств

Исполнения ViPNet Coordinator IG

ПАК ViPNet Coordinator IG10

- Производительность L3 VPN – до 10 Мбит/с
- Производительность L2 VPN – до 10 Мбит/с
- Производительность МЭ – до 10 Мбит/с
- Максимальное количество одновременных сессий – до 1000
- Рабочая температура - -40^{0}C…+60^{0}C

ПАК ViPNet Coordinator IG100

- Производительность L3 VPN – до 60 Мбит/с
- Производительность L2 VPN – до 60 Мбит/с
- Производительность МЭ – до 60 Мбит/с
- Максимальное количество одновременных сессий – до 15000
- Рабочая температура - -20^{0}C…+60^{0}C

Лицензия типа 1: 5 туннелируемых адресов, поддержка шлюза RS-232/485 – Ethernet
Лицензия типа 2: нет ограничений по количеству туннелируемых узлов, поддержка шлюза RS-232/485 – Ethernet

Промышленное исполнение ViPNet Coordinator IG

- ARM-платформа
- Безвентиляторный дизайн
- Рабочая температура: -20^{0}C(-40^{0}C) … +60^{0}C
- IP30
- Напряжение питания: 12…24 В DC
- Крепление на din-рейку
- 50x120x120 мм, 0.6 кг
- ЭМС: ГОСТ 51318.22/CISPR22, ГОСТ CISPR 24

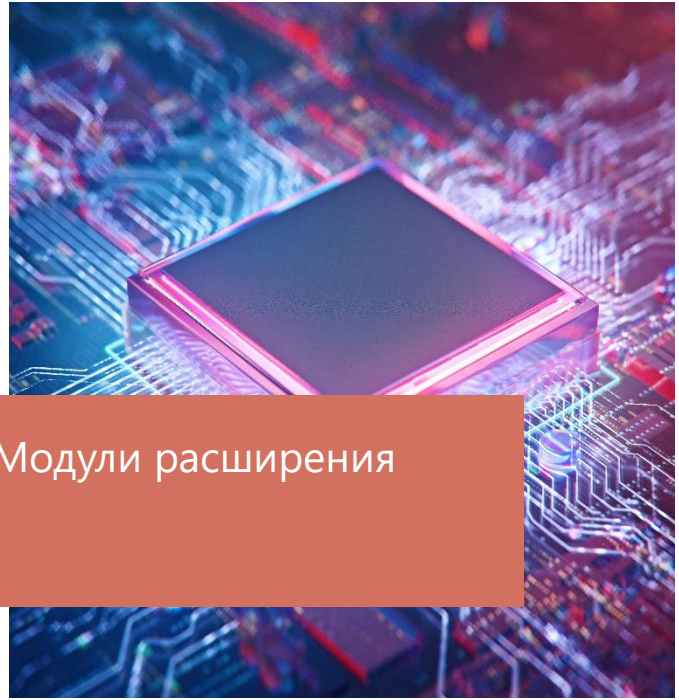
Беспроводные модули для ViPNet Coordinator IG

- Модуль расширения 3G для ПАК ViPNet Coordinator IG10/IG100 (комплект)

  Рабочая температура модуля: -20^{0}C … +60^{0}C
  Рабочая температура ПАК с модулем: -20^{0}C … +60^{0}C

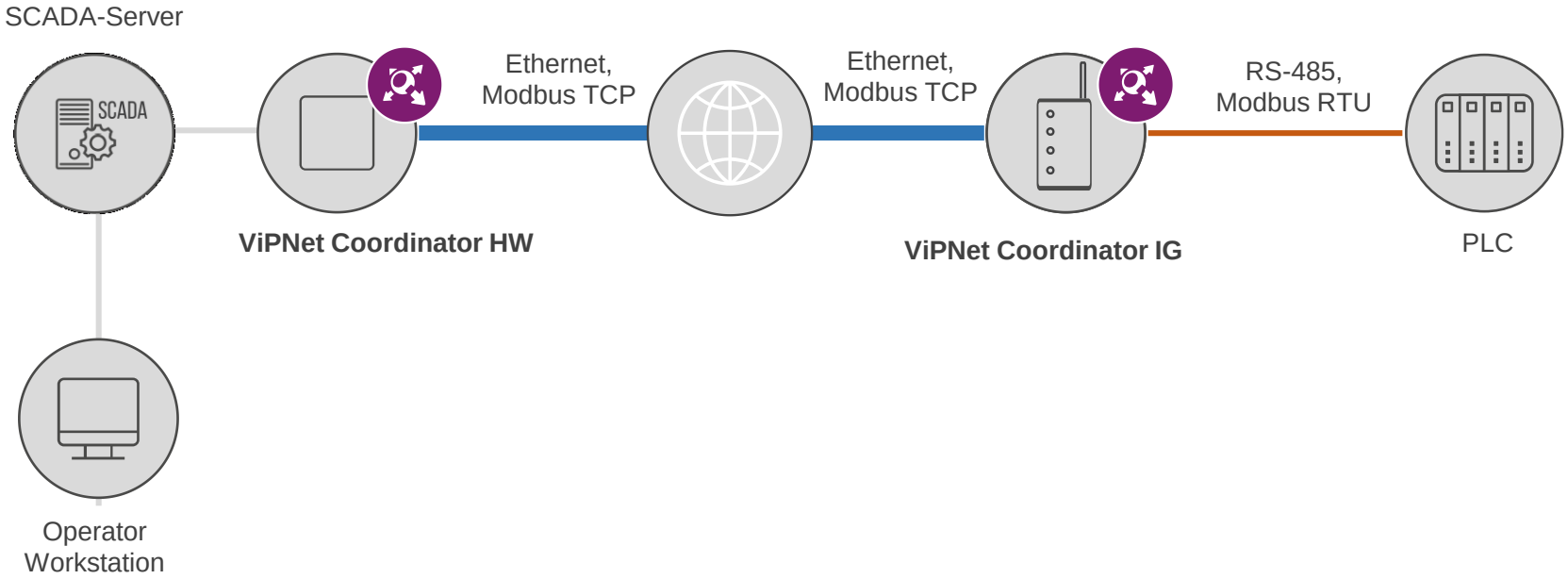
- Модуль расширения WiFi для ПАК ViPNet Coordinator IG10/IG100 (комплект)

  Рабочая температура: -20^{0}C … +60^{0}C
  Рабочая температура ПАК с модулем: -20^{0}C … +60^{0}C

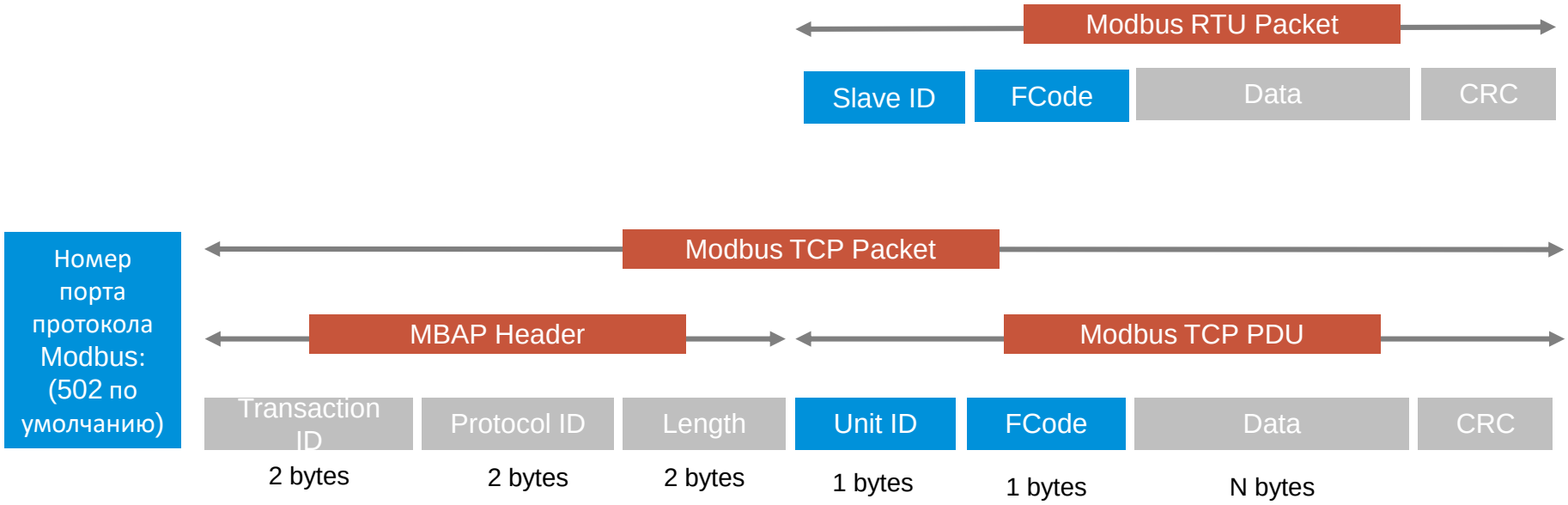


Модули расширения

Шлюз Modbus TCP-RTU и RTU-TCP



Глубокая фильтрация протокола Modbus



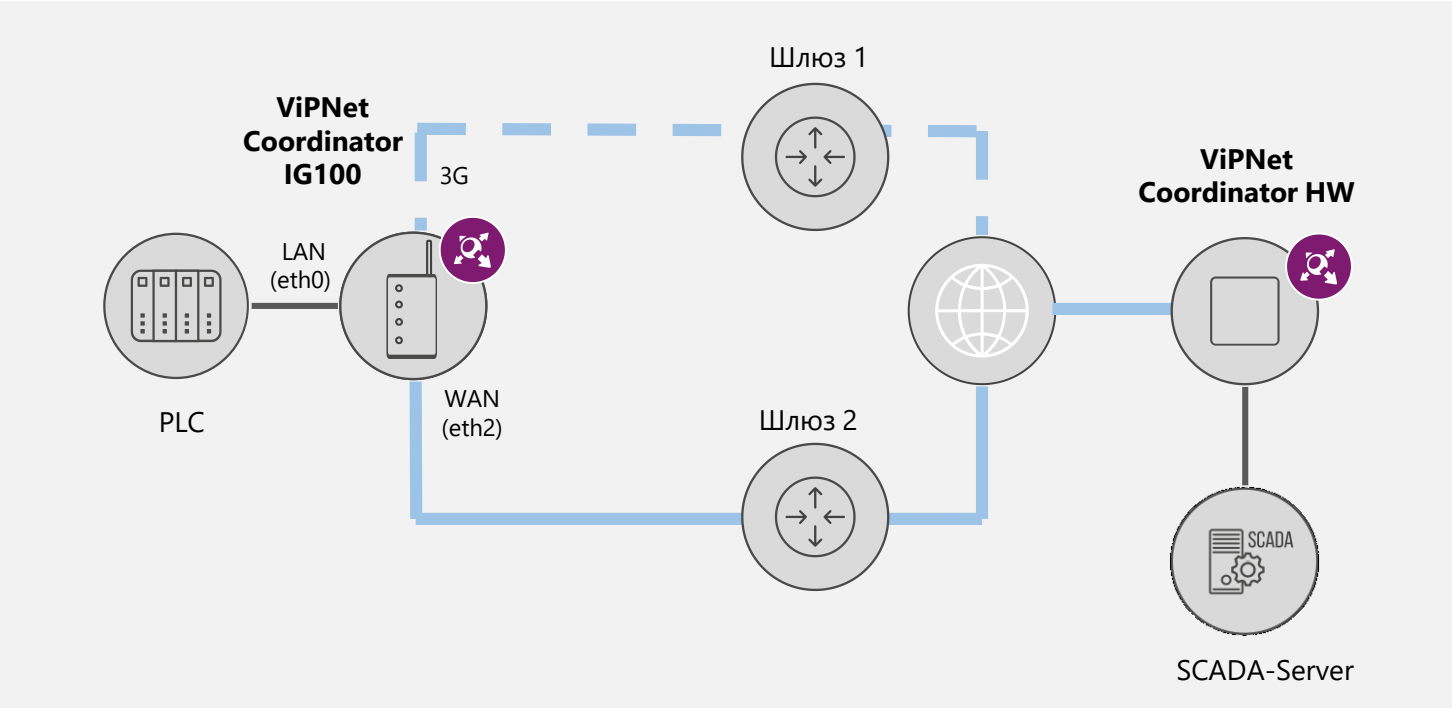
Глубокая фильтрация протокола Modbus

Фильтрация:

- Группа сетевых узлов ViPNet (для защищенной сети и туннелируемого трафика)
- Группа IP-адресов (IP, диапазон IP, DNS-имена) для открытой сети, туннелируемого траффика, NAT
- Группа сетевых интерфейсов
- Группа протоколов
- Группа расписаний

Глубокая фильтрация Modbus TCP:

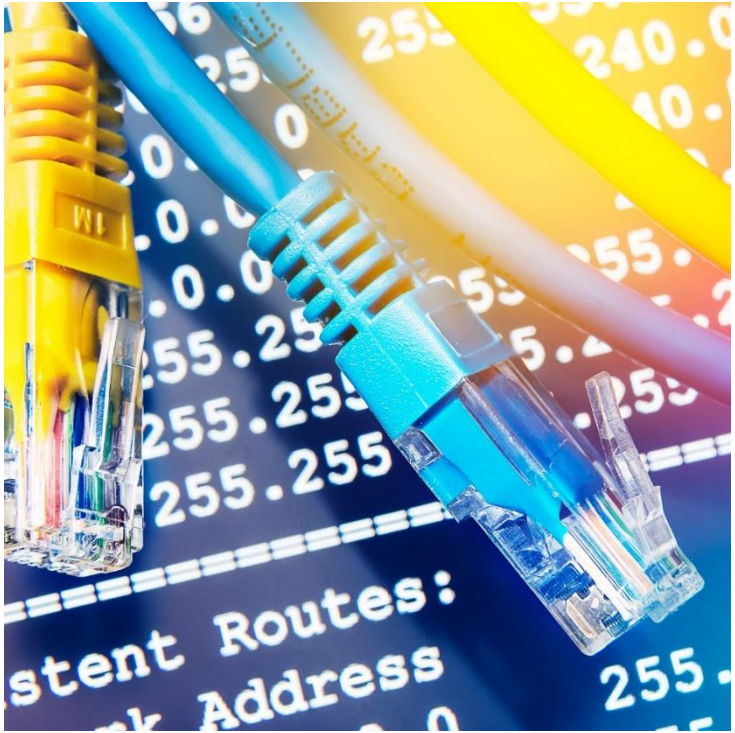
- Контроль пакетов на аномалии
- Возможность фильтрации Modbus на нестандартных портах
- Возможность разрешения/запрета сообщений от конкретных адресов
- Возможность разрешения/запрета сообщений с конкретными командами



MultiWAN: резервирование каналов WAN-3G

Схема работы

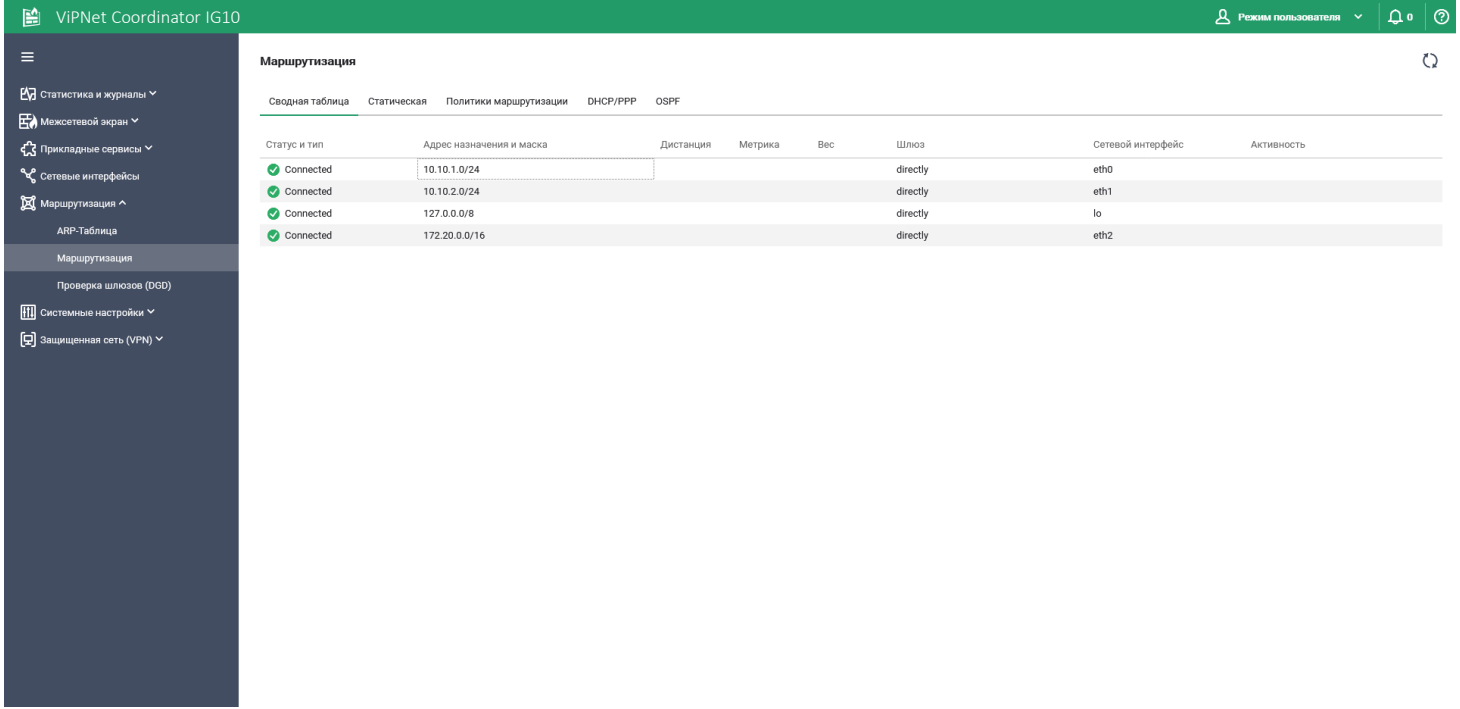
MultiWAN



- Политики маршрутизации (PolicyRouting)
- Проверка состояния шлюзов (Dead Gateway Detection)

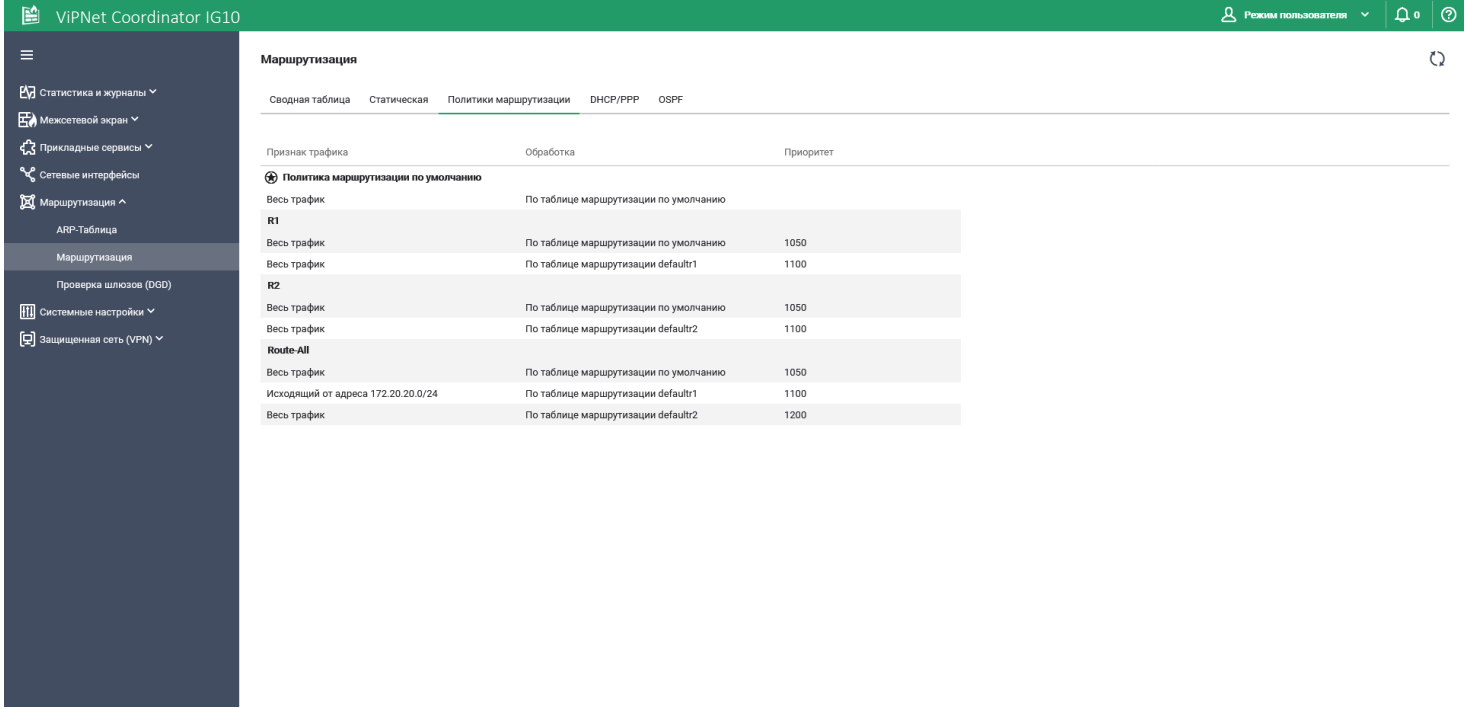
MultiWAN

- Пользовательские таблицы маршрутизации
- Политики маршрутизации
- Проверка состояния шлюзов



MultiWAN: резервирование каналов WAN-WAN

Таблицы маршрутизации

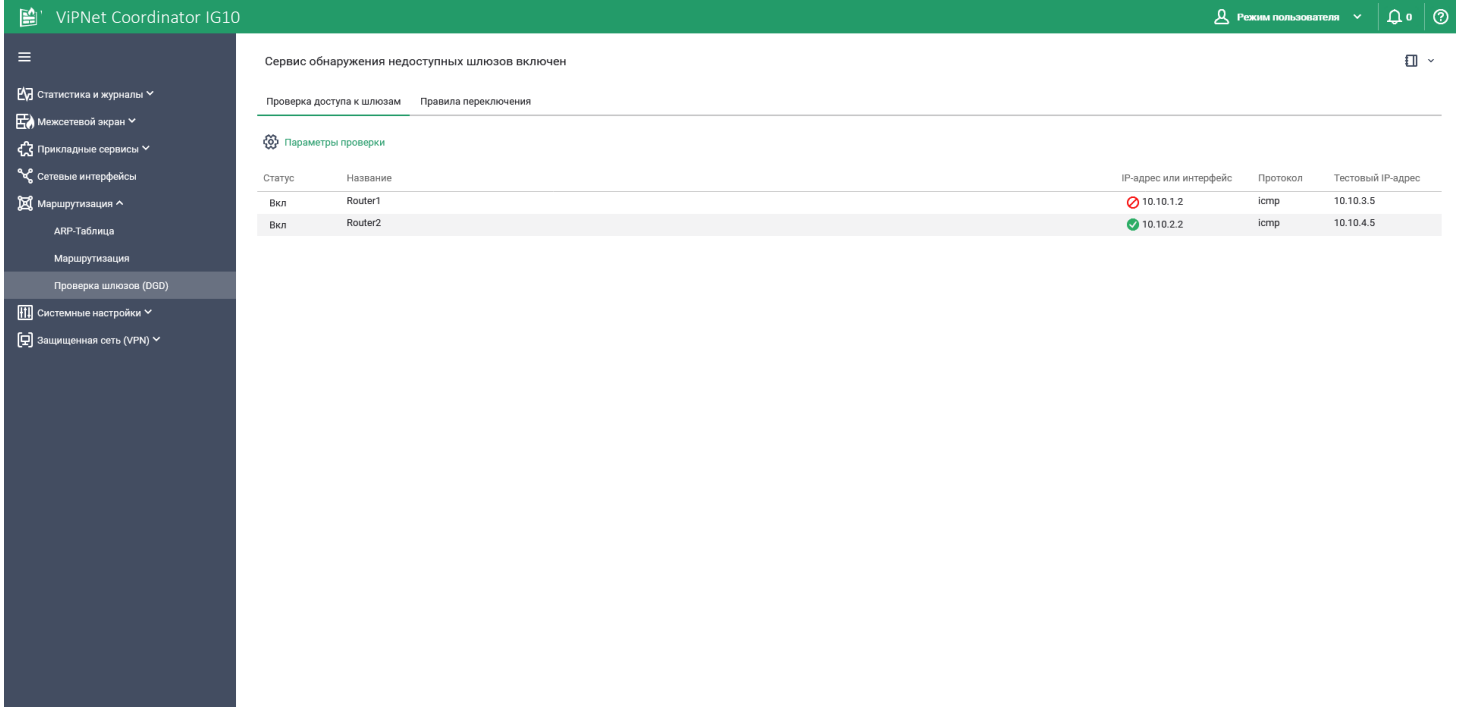


Условия:

- Интерфейс
- Адрес
- Метка DSCP
- Действие match/block/reject
- Приоритет

MultiWAN: резервирование каналов WAN-WAN

Политики маршрутизации



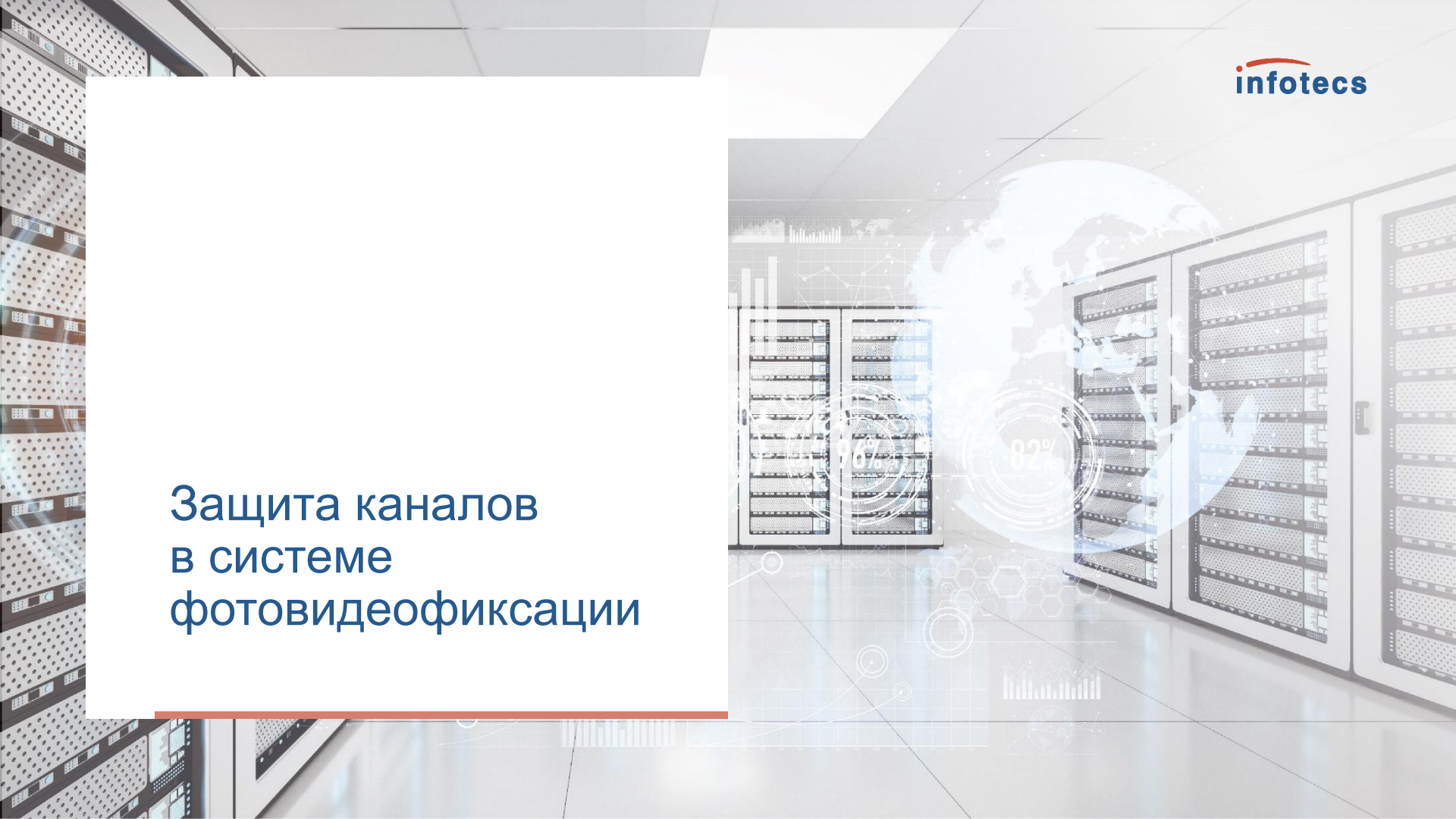
MultiWAN: резервирование каналов WAN-WAN

Проверка состояния шлюзов (DGD)

Метод проверки: ICMP, TCP:80, TCP:443

Работает для проводных и беспроводных каналов

Параметры: время ожидания ответа, интервал между проверками, число проверок

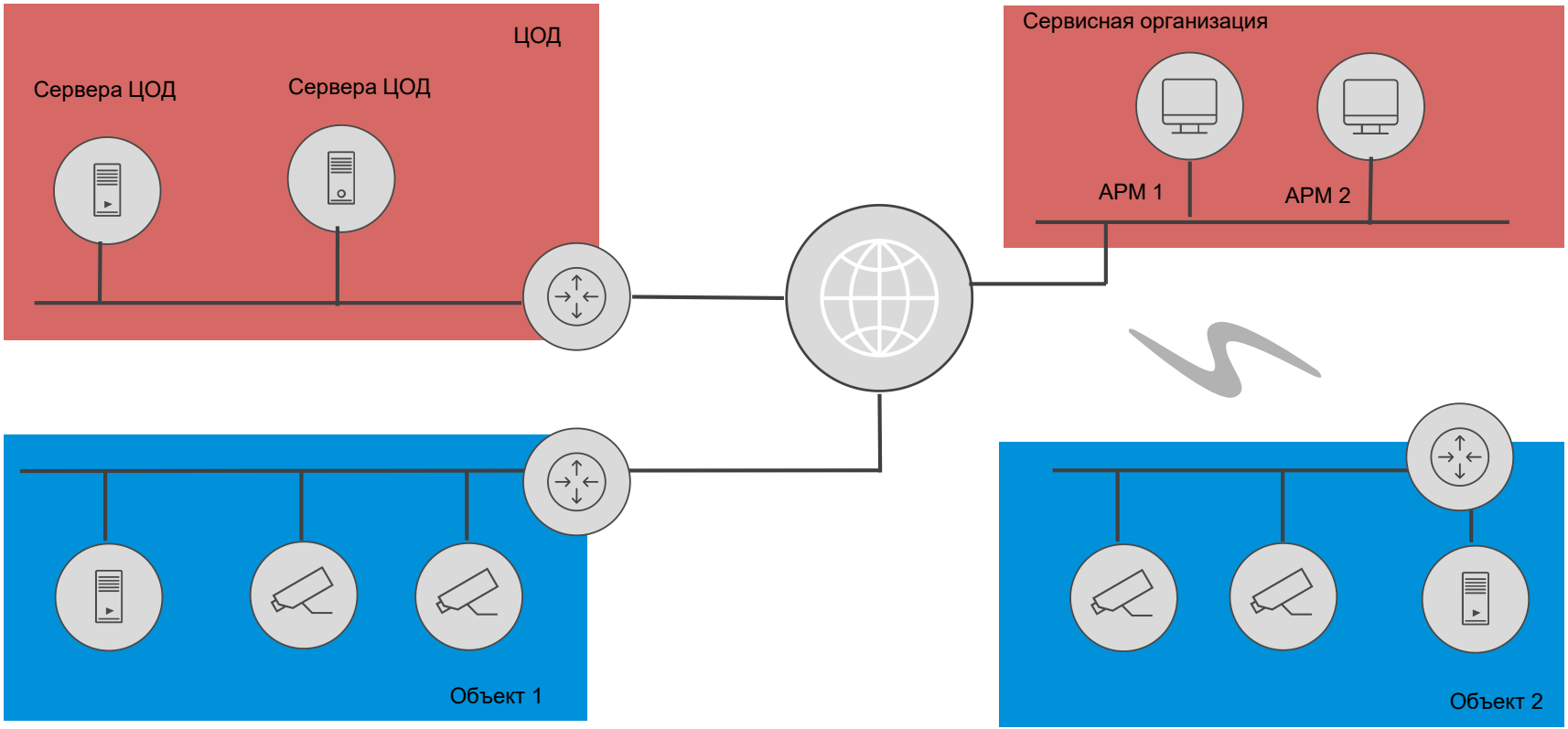


Защита каналов в системе фотовидеофиксации

Система стационарных комплексов фотовидеофиксации

- Контроль за движением автотранспорта на автотрассах, перекрестках и пешеходных переходах
- Оперативный анализ дорожной ситуации
- Управление транспортными потоками
- Фиксация правонарушений

Система стационарных комплексов фотовидеофиксации



Требования к средствам защиты информации

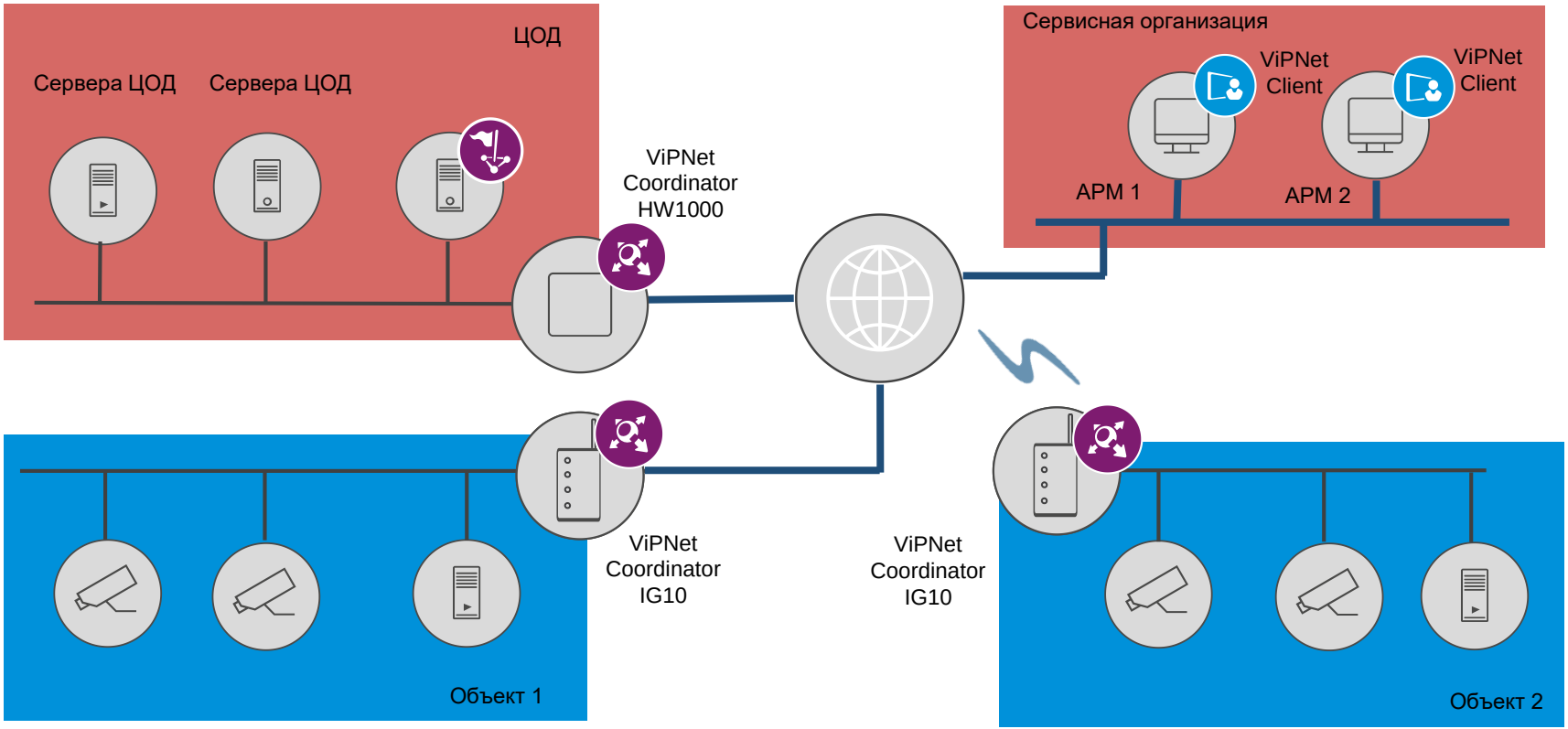
Меры защиты:

- Защита каналов
- Сегментирование сети
- Разграничение доступа к сегментам сети

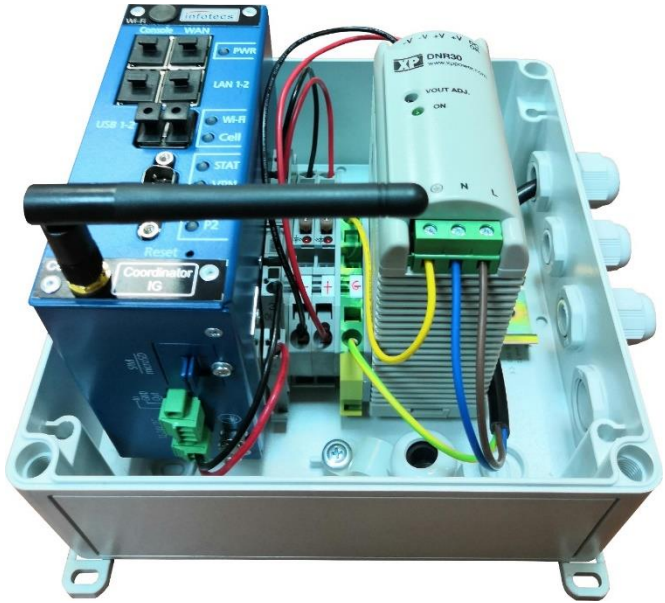
Требования к размещению на стороне объекта:

- Уличное размещение
- Питание ~220В

Защита каналов системы стационарных комплексов фотовидеофиксации



Размещение ViPNet Coordinator IG10



- Поликарбонатный герметичный бокс IP67 182x180x165 мм
- Блок питания AC/DC 220В/24В 2,5А с креплением дин-рейку
- В качестве каналов связи используется проводной и беспроводной канал 3G, нет необходимости выноса антенны

Итого

- Реализованные проекты в нескольких регионах России начиная с 2018 года
- Нет необходимости использовать термостабилизированные шкафы для размещения СЗИ на уровне объектов
- Малые габариты дополнительного оборудования
- Простота монтажа

Защита каналов передачи данных на электроподстанции

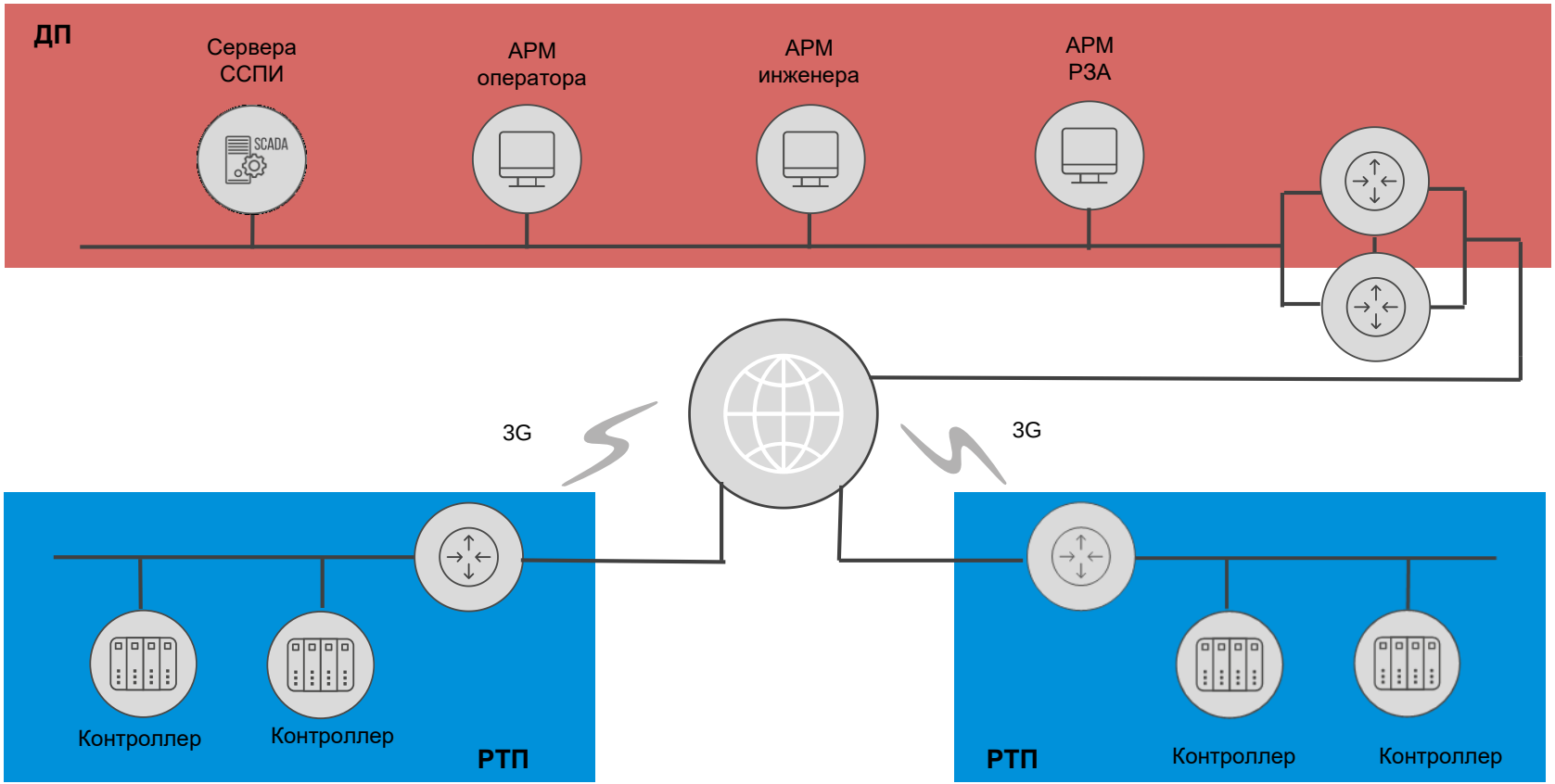
Распределительная трансформаторная подстанция

РТП - электроустановка, предназначенная для приема, преобразования и распределения электрической энергии

Задачи в эпоху цифровой трансформации:

- Снижение средней длительности нарушений электроснабжения
- Снижение времени на выполнение технических мероприятий
- Сокращение уровней диспетчерского управления
- Использование современных средств контроля и управления

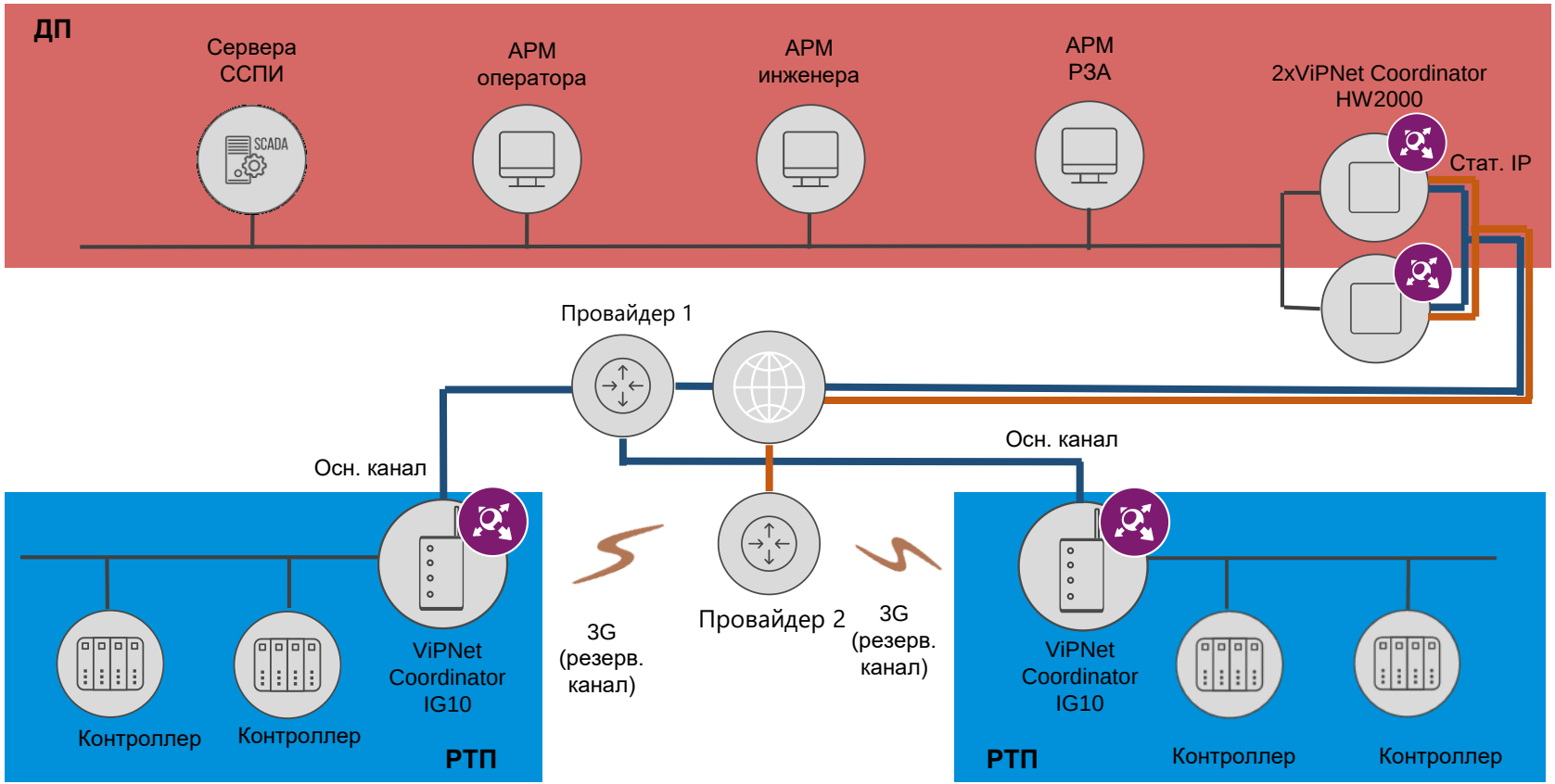
РТП


ДП
Сервера ССПИ
SCADA
АРМ оператора
АРМ инженера
АРМ РЗА
3G
3G
Контроллер
Контроллер
РТП
РТП
Контроллер
Контроллер

Требования к СЗИ

- Защита каналов
- Сегментирование сети
- Разграничение доступа к сегментам сети
- Работа на уровне РТП для СЗИ на полевом уровне
- Резервирование каналов на уровне РТП
- Резервирование на уровне ДП

Защита каналов РТП



Итого

- Реализованные проекты на 50+ РТП в 2019 году, планы по внедрению 70+ в 2020
- Малые габариты дополнительного оборудования
- Простота монтажа в шкафах ТМ
- Работа со специализированным оператором связи
- Организация переключение с основного Ethernet на канала 3G при недоступности

infotecs

Защита каналов в системе мониторинга и предиктивной аналитики

Системы предиктивной аналитики

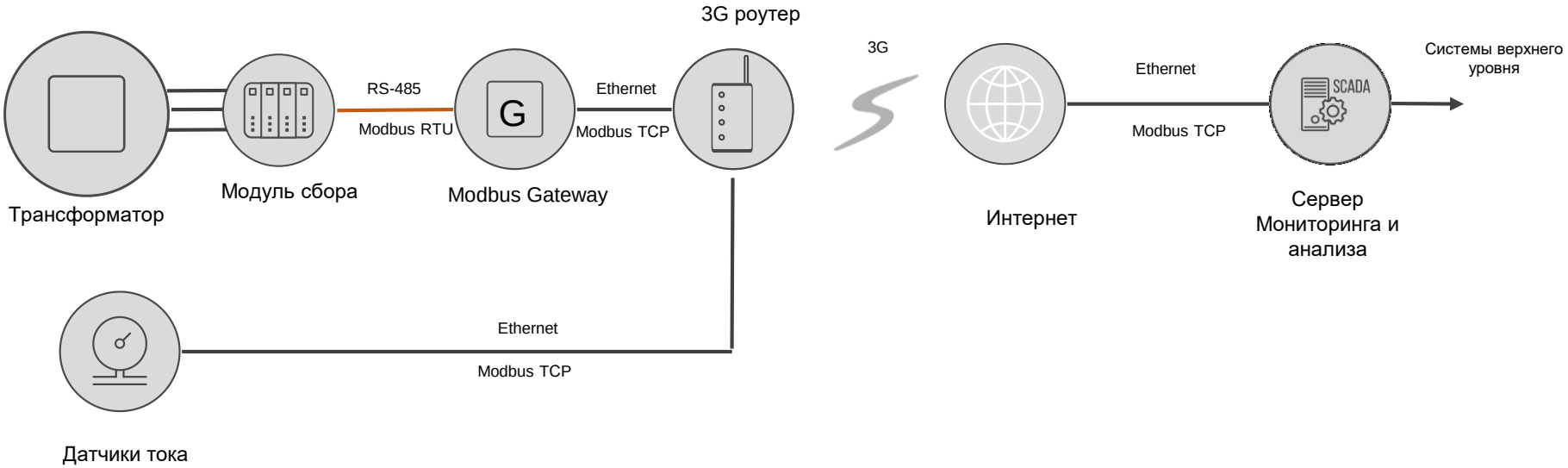
Системы, основанные на методах анализа данных, статистики, которые используются для прогнозирования событий в будущем

- Прогнозирование отказов оборудования - переход от обслуживания по регламенту к обслуживанию по состоянию
- Прогнозирование и анализ влияния воздействий факторов на параметры продукции
- Прогнозирование производства продукции и потребления энергии и ресурсов

Системы мониторинга высоковольтного оборудования

- Контроль соответствия текущих параметров работы трансформатора нормативным требованиям
- Проведение автоматизированной экспертной диагностики дефектов и оценки технического состояния трансформатора
- Передача системой в АСУ-ТП более высокого уровня первичной и обработанной информации для использования в более сложных интегрированных системах контроля

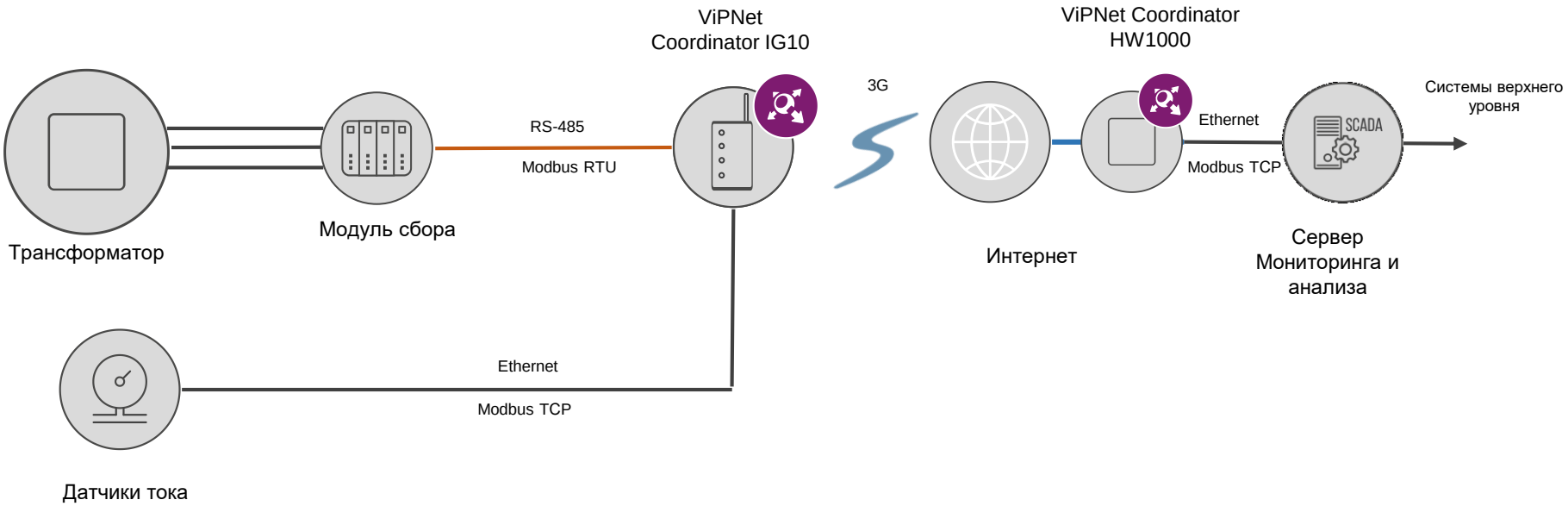
Системы мониторинга высоковольтного оборудования



Требования к СЗИ

- Защита каналов
- Сегментирование сети
- Разграничение доступа к сегменту сети
- Работа на полевом уровне рядом с силовым оборудованием
- Исключение дополнительного оборудования

Системы мониторинга высоковольтного оборудования



Итого

- Исключено дополнительное оборудование – Modbus Gateway, 3G-роутер
- Есть возможность контроля сообщений внутри протокола Modbus по технологии DPI

Marina.Sorokina@infotecs.ru
Марина Сорокина

infotecs®

Спасибо за внимание!