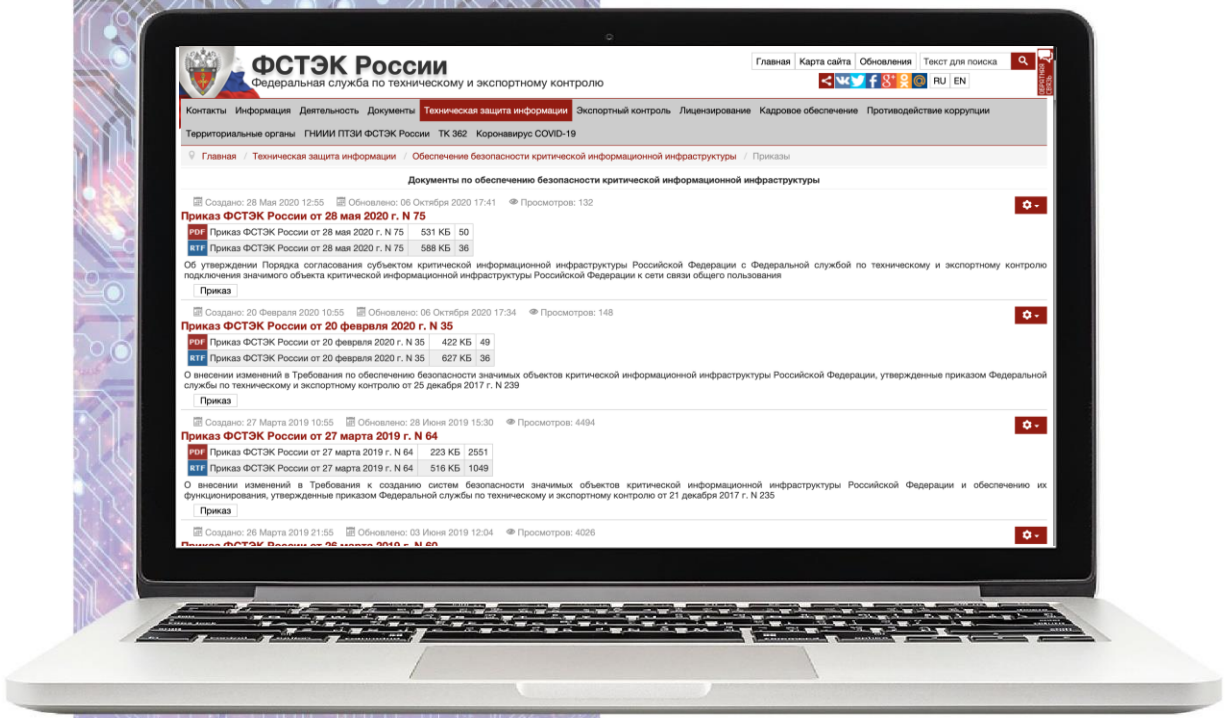
Защита объектов КИИ при подключении к сетям связи общего пользования с помощью ПАК ViPNet Coordinator IG

Марина Сорокина

Нормативная сторона вопроса



Приказ ФСТЭК №75 от 28.05.2020 г.

"Об утверждении Порядка согласования субъектом КИИ РФ с ФСТЭК подключения значимого объекта КИИ РФ к сети связи общего пользования"

Зарегистрировано в Минюсте России 15.09.2020 N 59866

Назначение Приказа №75 ФСТЭК России от 28.05.2020 г.

- Процедура согласования для значимого объекта КИИ при подключении его к сети передачи общего пользования.
- Согласование осуществляется в части оценки достаточности применяемых СЗИ для значимого объекта КИИ
- Согласование осуществляется до ввода действия объекта КИИ
- Если объект КИИ на момент включения в реестр значимых объектов КИИ имел подключение к сети передачи общего пользования, то согласование не требуется.

Основные положение Приказа №75 ФСТЭК России от 28.05.2020

Необходимо предоставление информации:

- об объекте КИИ
- цели подключения к Интернет
- способах подключения с указанием типа доступа и протоколов взаимодействия
- сведения о СЗИ, применяемых для обеспечения безопасности (наименование, версия, номера сертификатов или реквизиты протоколов испытаний с результатами оценки соответствия)

Основные положение Приказа №75 ФСТЭК России от 28.05.2020

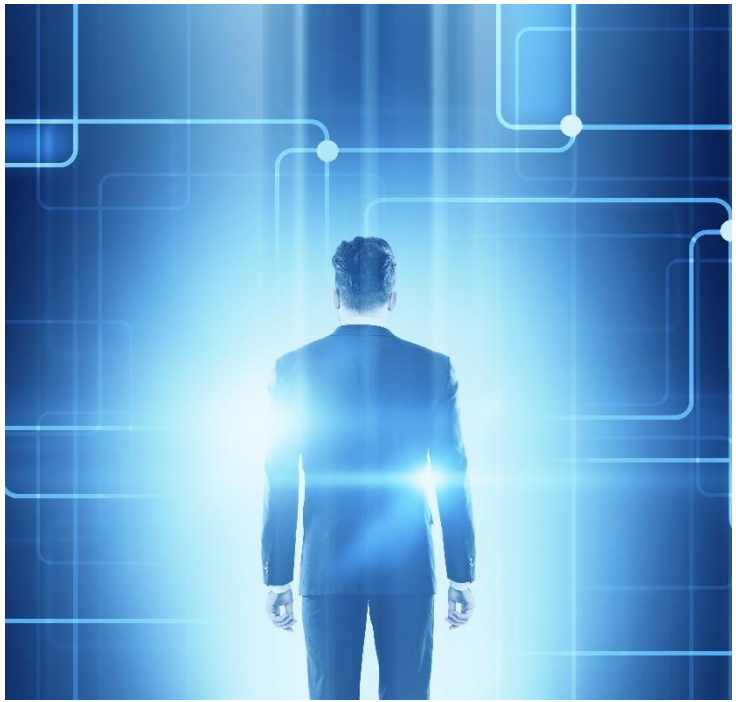
Необходимо предоставление документов:

- Копия модели угроз безопасности информации
- Копии протоколов испытаний с результатами оценки соответствия (для СЗИ, прошедших оценку соответствия в форме испытаний, приемки)
- Схема организации связи

Основные положение Приказа №75 ФСТЭК России от 28.05.2020

ФСТЭК России может отказать в согласовании:

- предоставление неполного объема сведений и документов
- Несоответствие наименований, моделей, версий ПО данным, указанным в сертификатах соответствия или протоколах испытаний
- Несоответствие СЗИ требованиям к созданию систем безопасности объектов КИИ, утвержденных Приказами ФСТЭК России №239 от 25.12.2017 г. и №235 от 21.12.2017 г.



Проект Приказа от весны 2020 г.

infotecs

СЗИ, прошедшие оценку на соответствие требованиям по безопасности в форме обязательной сертификации, испытания или приемки

	1 КЗ	2 КЗ	3 КЗ
МЭ (ПАК) уровня сети (Тип А и Д?)	+	+	+
Граничный маршрутизатор (ПАК)	+	+	+
• с выделенным интерфейсом для публичного сервиса	+	+	
Средство антивирусной защиты	+	+	+
• с антиспамом, черным списком и централизованным управлением	+	+	
СКЗИ (VPN – шлюз или пр)	+	+	+
СОВ	+	+	

Основные выводы по анализу Приказа №75 ФСТЭК России от 28.05.2020 г.

- Приказ не содержит дополнительных требований по защите КИИ
- Все применяемые СЗИ должны соответствовать Приказам ФСТЭК России №239 от 25.12.2017 г. и №235 от 21.12.2017 г.
- Проект Приказа показал «эталонный» вариант реализации требований от ФСТЭК России

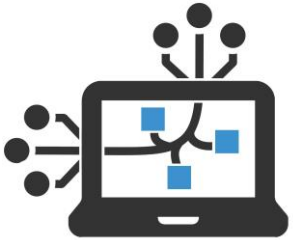
Зачем объекту КИИ типа АСУ подключение к Интернет?

Цели подключения к сетям связи общего пользования согласно Приказу №75 ФСТЭК России от 28.05.2020 г.

Управление в АСУ/ Контроль выполнения тех.процесса/ взаимодействие между сегментами ОКИИ

Доступ к информационным ресурсам

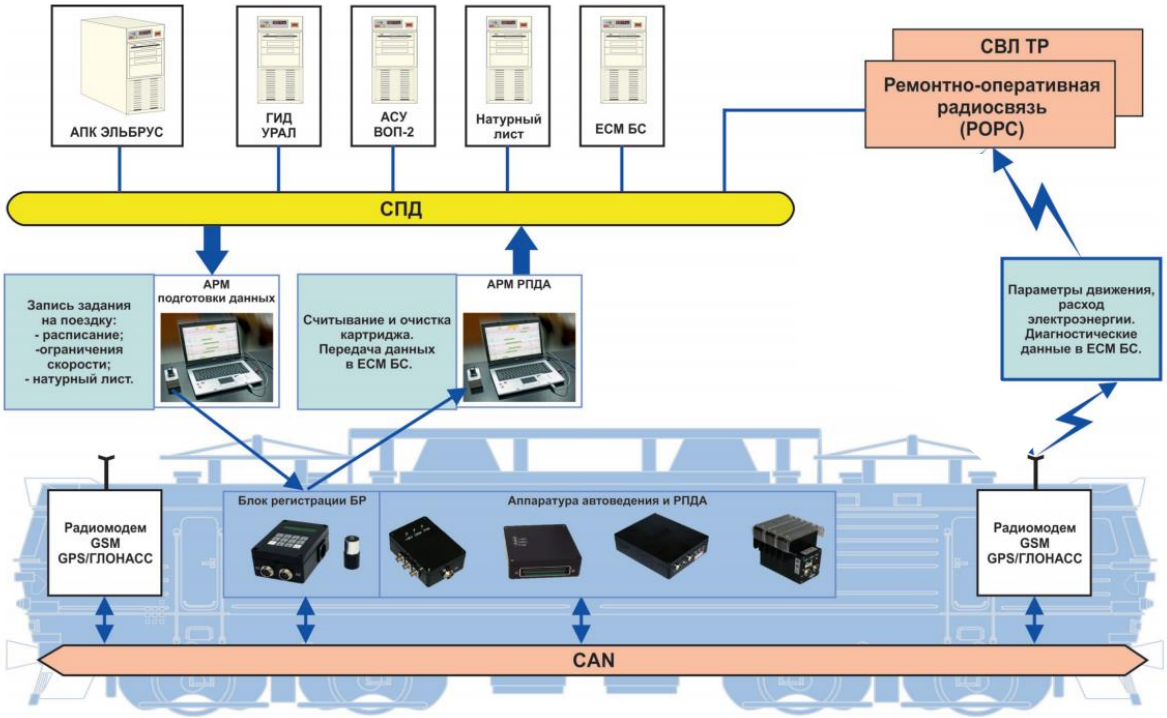
Контроль за производственным оборудованием



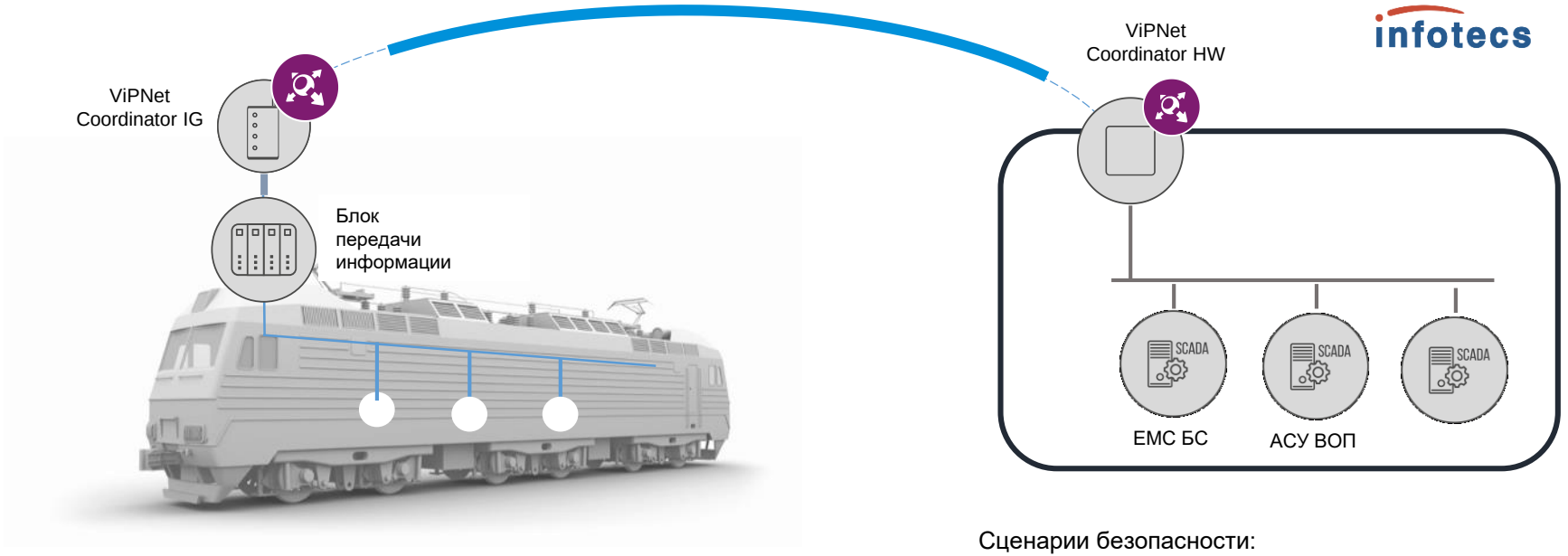
Взаимодействие с иными системами/межсетевое взаимодействие

Оказание услуг

Мониторинг технологического процесса



Передача информации о параметрах движения локомотива



Сценарии безопасности:

- Защита каналов передачи(ЗИС.6, ЗИС.13, ЗИС.19, ЗИС.20, ЗИС.27,ЗИС.32, ОЦЛ.2, ОЦЛ.6)
- Ограничение доступа (ЗИС.2/ЗИС.4, ЗИС.6, ЗИС.27, ЗИС.33)
- Антивирусная защита (АЗВ.1)

Защита информации для системы передачи информации о параметрах движения локомотива (минимальный вариант)

ViPNet Coordinator IG

ViPNet Coordiantor IG10 I1

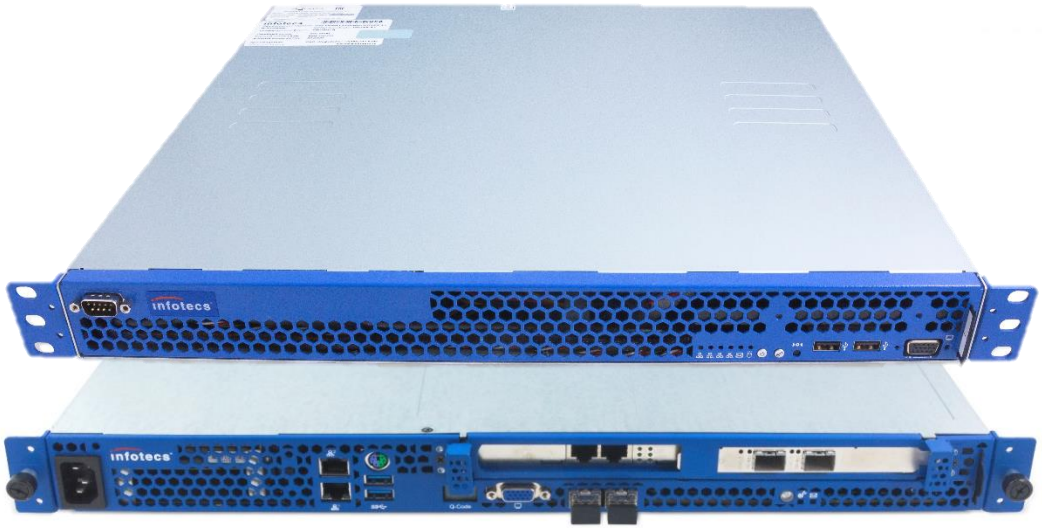
ViPNet Coordiantor IG100 I1

ViPNet Coordiantor IG10 I2*

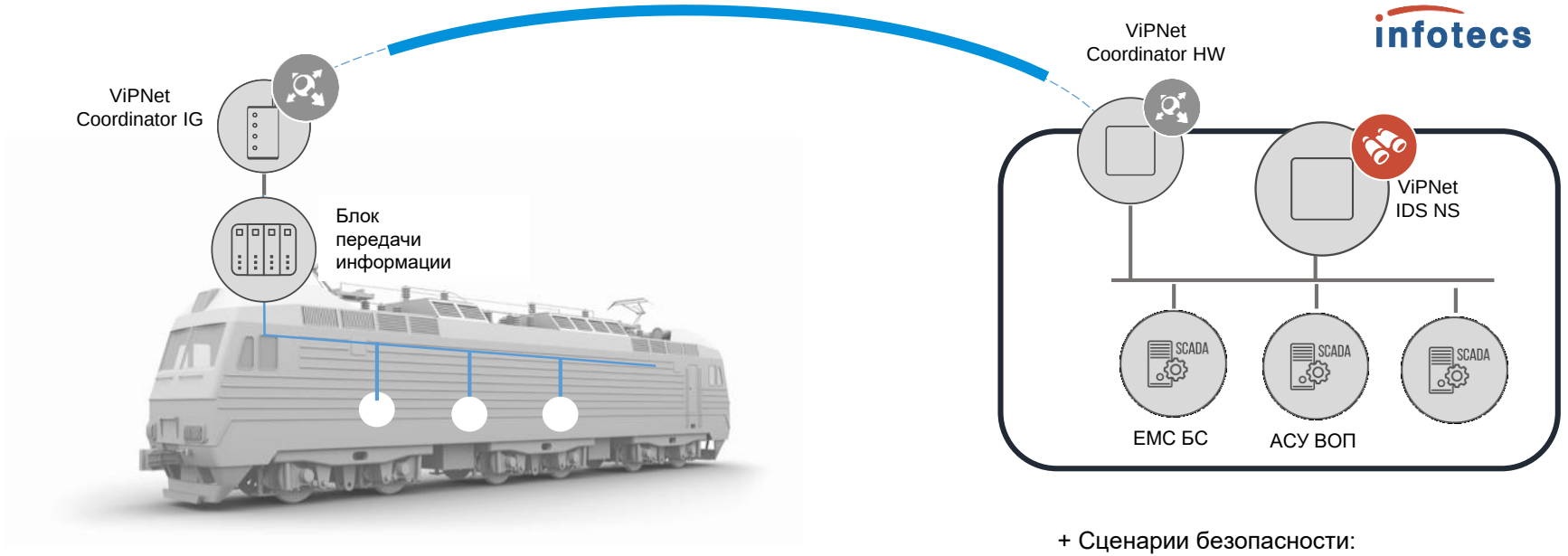
- VPN-шлюз СКЗИ КС3
- МЭ 4 класса по требованиям ФСБ России
- Завершение сертификации МЭ по требованиям ФСТЭК России ИТ.МЭ.А4.ПЗ и ИТ.МЭ.Д4.ПЗ и 4 классу ТДБ
- Устройство маршрутизации и коммутации по требования Минкомсвязи России
- Абонентская радиостанция стандарта GSM-900/1800 и UMTS по требования Минкомсвязи России

* Планы сертификации как СКЗИ и МЭ - Q3/Q4 2021

ViPNet Coordinator HW



- VPN-шлюз СКЗИ КС3
- МЭ 4 класса по требованиям ФСБ России
- МЭ по требованиям ФСТЭК России ИТ.МЭ.А4.ПЗ и 4 класс ТДБ
- Устройство маршрутизации и коммутации по требования Минкомсвязи России
- Встроенный поточный антивирус

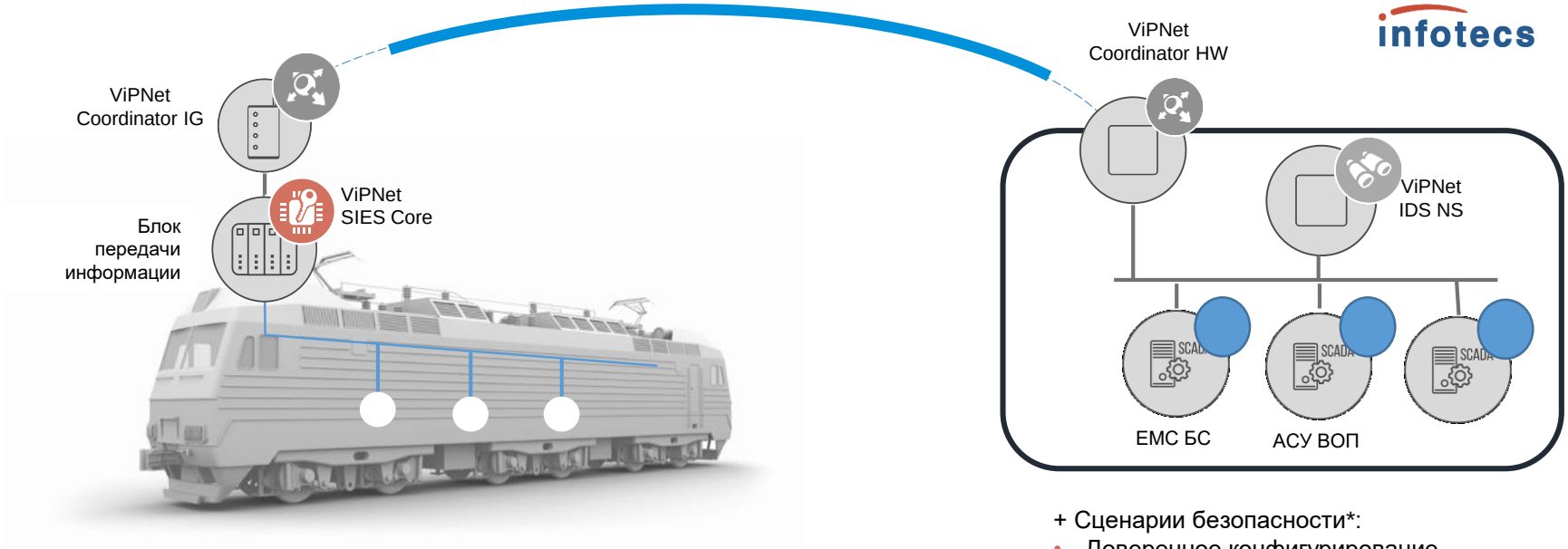


+ Сценарии безопасности:
- Система обнаружения вторжений (СОВ.2, ИНЦ.1, ИНЦ.2)

Защита информации для системы передачи информации о параметрах движения локомотива (классический вариант)

ViPNet IDS NS

- СОА класса В по требованиям ФСБ России
- Завершается сертификация по СОВ уровня сети 4 класса по требованиям ФСТЭК России



+ Сценарии безопасности*:

- Доверенное конфигурирование
- Доверенная загрузка
- Доверенное обновление
- Строгая аутентификация инженера

Защита информации для системы передачи информации о параметрах движения локомотива (Расширенный вариант)

* Защита серверов и рабочих станций может иметь разную реализацию

ViPNet SIES Core

- СКЗИ класса КС3 по требованиям ФСБ России
- Интеграция в защищаемые устройства (PLC, PAC, датчики, исполнительные механизмы) для реализации сценариев безопасности в концепции security-by-design

ViPNet SIES Core: вебинары

Реализация мер по обеспечению информационной безопасности для контроллеров АСУ

31 октября 2019

[Посмотреть вебинар от 31.10.2019]

ViPNet SIES в разрезе требований Приказа №239

30 мая 2019

[Посмотреть вебинар от 30.05.2019]

Компоненты решения SIES для защиты узлов АСУ

28 марта 2019

[Посмотреть вебинар от 28.03.2019]

Обзор решения ViPNet SIES для защиты информации в промышленных информационных системах

25 октября 2018

[Посмотреть вебинар от 25.10.2018]

Защита серверов и рабочих станций

infotecs

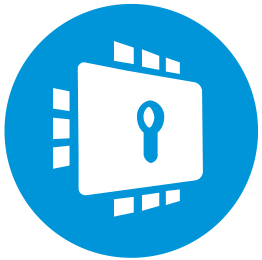
Доверие к платформе и обеспечение доверенной загрузки ОС

Разграничение доступа и защита данных

Защита от внешних атак и угроз

Обеспечение защищённых коммуникаций

Защита серверов и рабочих станций на продуктах ИнфоТеКС



ViPNet SafeBoot

Доверие к платформе и обеспечение доверенной загрузки ОС

ViPNet SafePoint

Разграничение доступа и защита данных

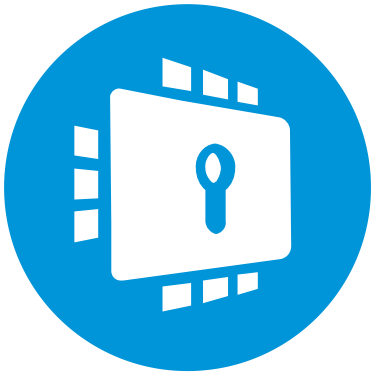
ViPNet Client 4U

Обеспечение защищённых коммуникаций

ViPNet EndPoint Protection

Защита от внешних атак и угроз

ViPNet SafeBoot



- Высокотехнологичный программный модуль доверенной загрузки, устанавливаемый в UEFI BIOS различных производителей. Предназначен для защиты компьютеров и серверов (в т.ч. и серверов виртуализации) от современных угроз НСД, связанных с загрузкой ОС и атак на сам BIOS
- Сертифицирован по требованиям РД к средствам доверенной загрузки уровня базовой системы ввода-вывода 2 класса

ViPNet SafePoint

- СЗИ от несанкционированного доступа, устанавливаемое на рабочие станции и сервера, предназначенное для мандатного и дискреционного разграничения доступа к критически важной информации.
  - Двухфакторная аутентификация пользователей
  - Мандатный контроль пользователя и процессов
  - Замкнутая программная среда
  - Контроль устройств
- Проходит сертификация по линии ФСТЭК России:
  - 5 классу защищенности СВТ
  - 4 классу защиты СКН (ИТ.СКН.П4.ПЗ)
  - 4 классу ТДБ

ViPNet SafeBoot, ViPNet SafePoint: вебинары

Обеспечение защиты рабочих станций и серверов продуктами ИнфоТеКС. Обзор новых версий продуктов направления Endpoint Security

27 февраля 2020

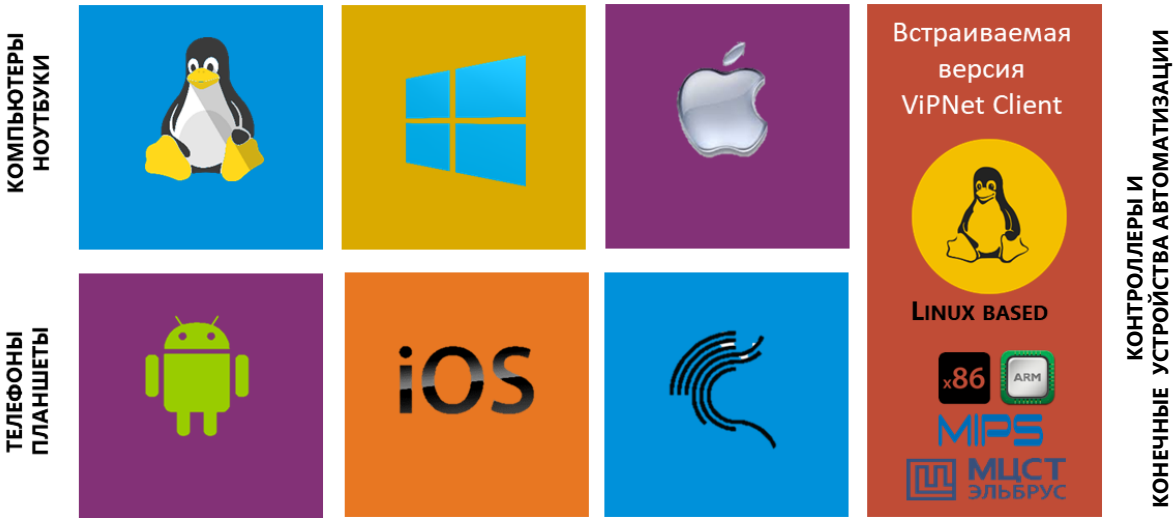
[Посмотреть вебинар от 27.02.2020]

Обзор новых версий продуктов для защиты рабочих станций и серверов от компании ИнфоТеКС

26 сентября 2019

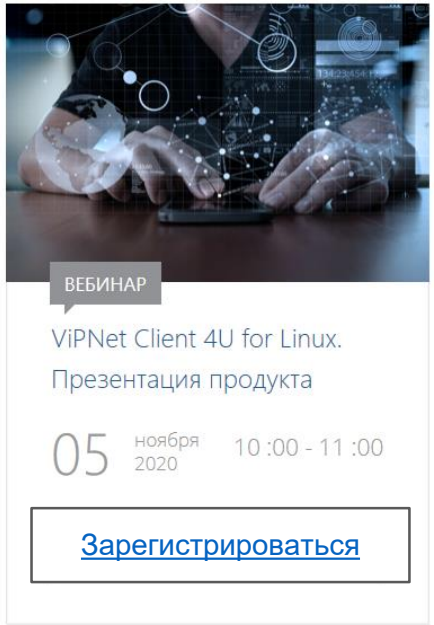
[Посмотреть вебинар от 26.09.2019]

ViPNet Client 4U



- VPN-client
- СКЗИ класса КС1 по требованиям ФСБ России
- Завершается сертификация СКЗИ класса КС3 по требованиям ФСБ России

ViPNet Client 4U: анонс вебинара



05 ноября 2020 | время проведения 10 :00 - 11 :00

Вебинар «ViPNet Client 4U for Linux. Презентация продукта»

Спикер: Александр Василенков, руководитель направления развития продуктов

На вебинаре будут представлены особенности и возможности новой версии продукта ViPNet Client 4U for Linux, а также информация по наличию действующих сертификатов соответствия требованиям ФСБ России.

ViPNet EndPoint Protection

Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия.

- персональный межсетевой экран,
- система обнаружения и предотвращения вторжений
- контроль приложений.

Проходит сертификация по линии ФСТЭК России:

- Системам обнаружения вторжений уровня узла 4 класса ИТ.СОВ.У4.ПЗ
- Межсетевым экранам типа В класса 4 (ИТ.МЭ.В4.ПЗ)
- 4 классу ТДБ

ViPNet EndPoint Protection: анонс вебинара

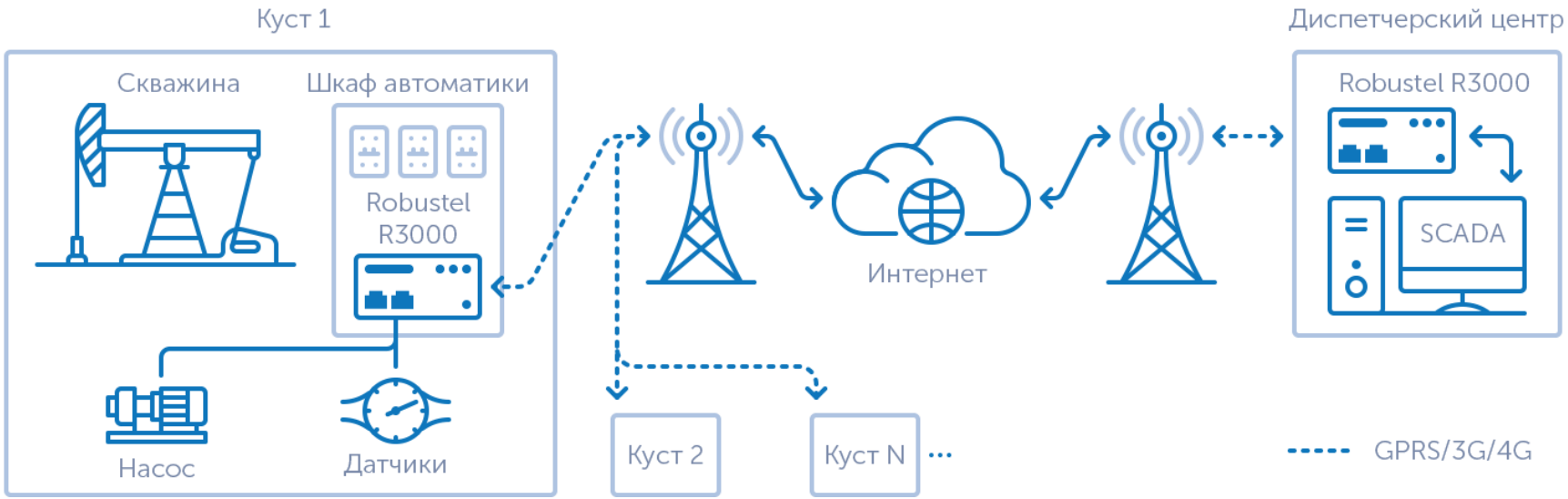
19 ноября 2020 | время проведения 10 :00 - 11 :00

Вебинар «ViPNet EndPoint Protection – обзор нового продукта для защиты рабочих станций»

Спикер вебинара: Иван Кадыков, руководитель направления
На вебинаре будет представлено новое решение ViPNet EndPoint Protection.
Иван расскажет про:
•Состав продукта и его функциональность,
•Ключевые сценарии использования и применения.
Особое внимание будет уделено перспективам развития и планам по сертификации продукта.

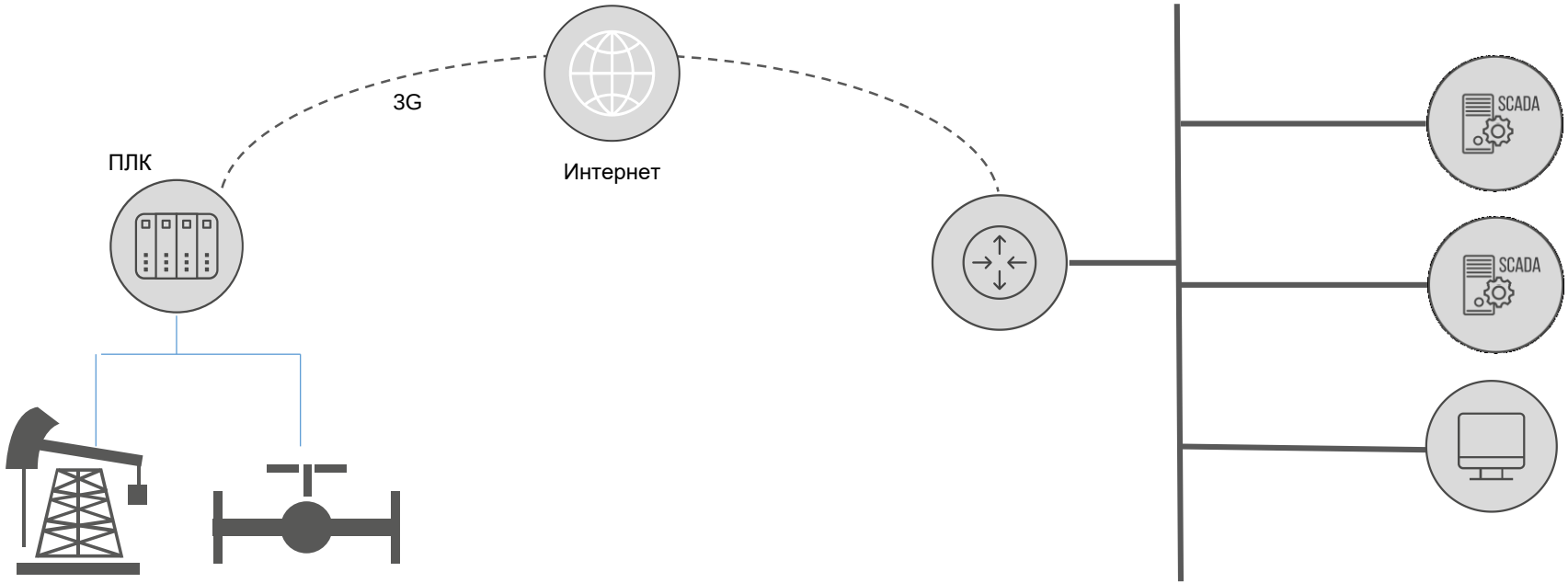
Управление в АСУ

Система кустовой телемеханики нефтегазодобычи

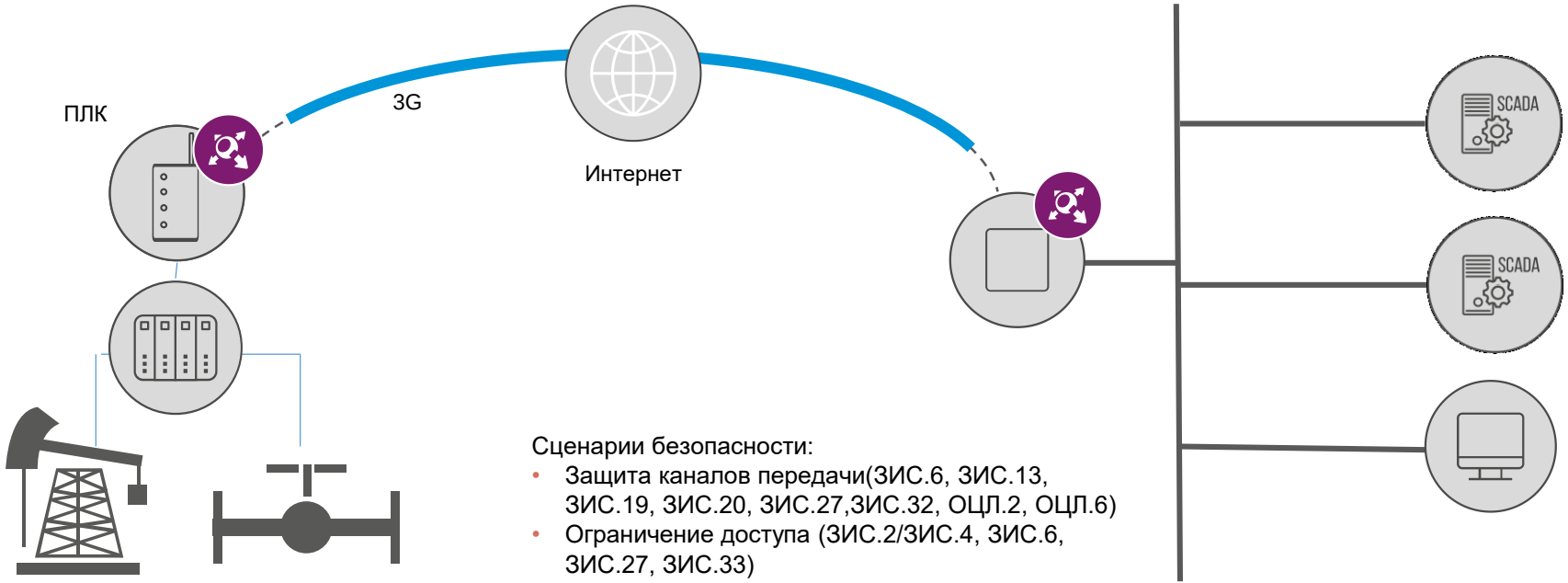


https://www.euromobile.ru/solutions/neftedobycha/nablyudenie-i-monitoring-neftyanykh-obektov/

Система кустовой телемеханики нефтегазодобычи



Защита информации системы кустовой телемеханики нефтегазодобычи (минимальный вариант)



Сценарии безопасности:

- Защита каналов передачи(ЗИС.6, ЗИС.13, ЗИС.19, ЗИС.20, ЗИС.27,ЗИС.32, ОЦЛ.2, ОЦЛ.6)
- Ограничение доступа (ЗИС.2/ЗИС.4, ЗИС.6, ЗИС.27, ЗИС.33)
- Антивирусная защита (АЗВ.1)

ViPNet Coordinator IG

ViPNet Coordiantor IG10 I1

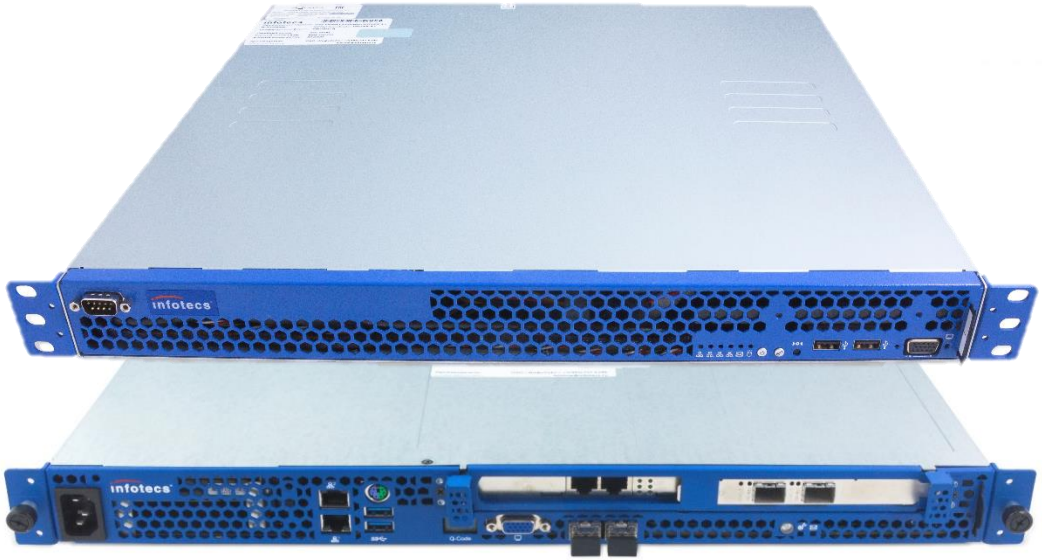
ViPNet Coordiantor IG100 I1

ViPNet Coordiantor IG10 I2*

- VPN-шлюз СКЗИ КС3
- МЭ 4 класса по требованиям ФСБ России
- Завершение сертификации МЭ по требованиям ФСТЭК России ИТ.МЭ.А4.ПЗ и ИТ.МЭ.Д4.ПЗ
- Устройство маршрутизации и коммутации по требования Минкомсвязи России
- Абонентская радиостанция стандарта GSM-900/1800 и UMTS по требования Минкомсвязи России

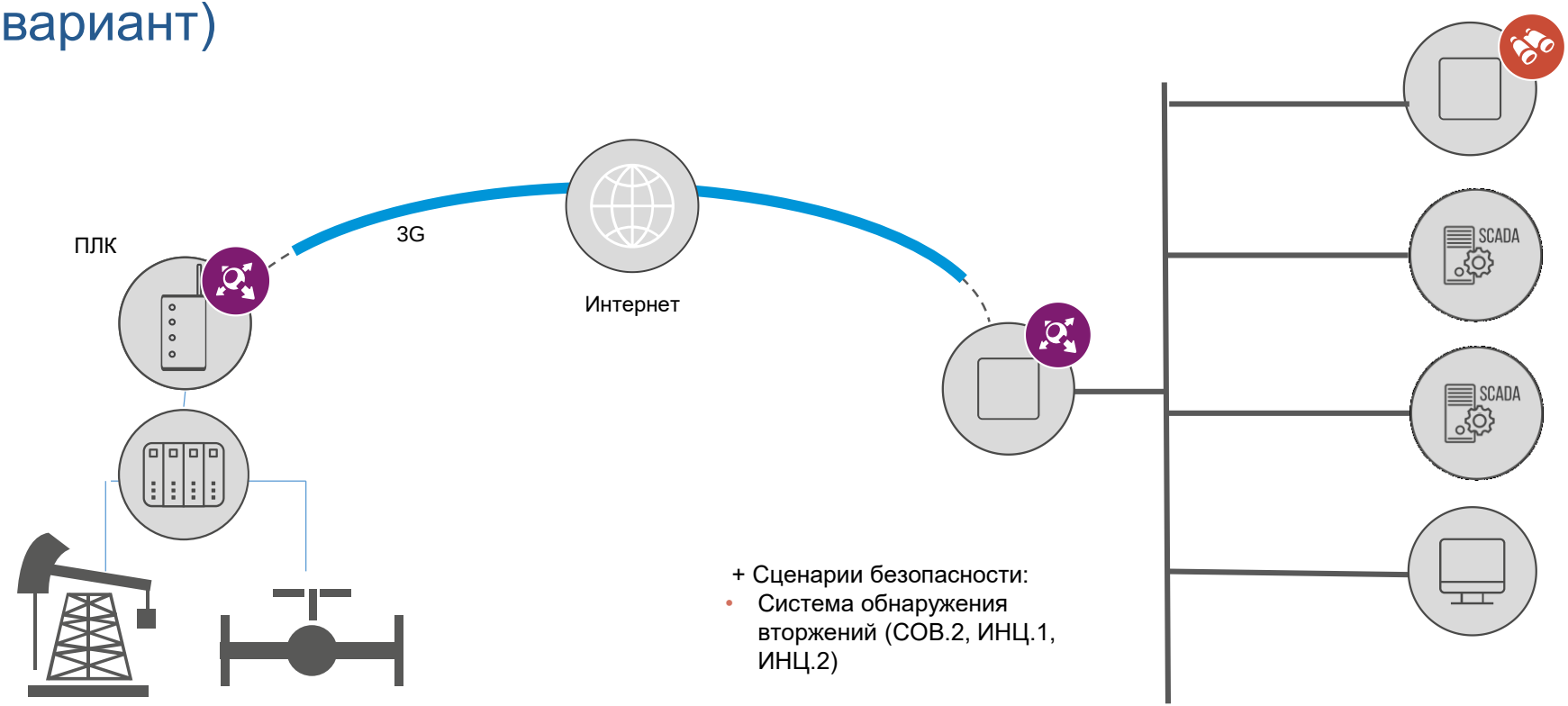
* Планы сертификации как СКЗИ и МЭ - Q3/Q4 2021

ViPNet Coordinator HW



- VPN-шлюз СКЗИ КС3
- МЭ 4 класса по требованиям ФСБ России
- МЭ по требованиям ФСТЭК России ИТ.МЭ.А4.ПЗ
- Устройство маршрутизации и коммутации по требования Минкомсвязи России
- Встроенный поточный антивирус

Защита информации системы кустовой телемеханики нефтегазодобычи (минимальный вариант)



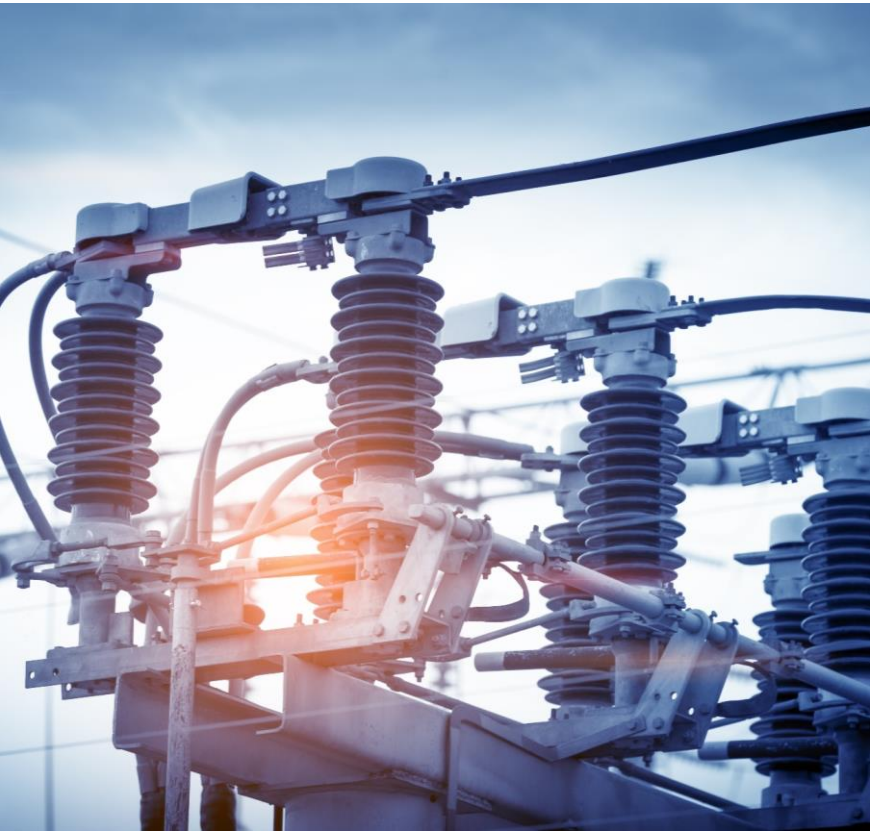
+ Сценарии безопасности:
- Система обнаружения вторжений (СОВ.2, ИНЦ.1, ИНЦ.2)

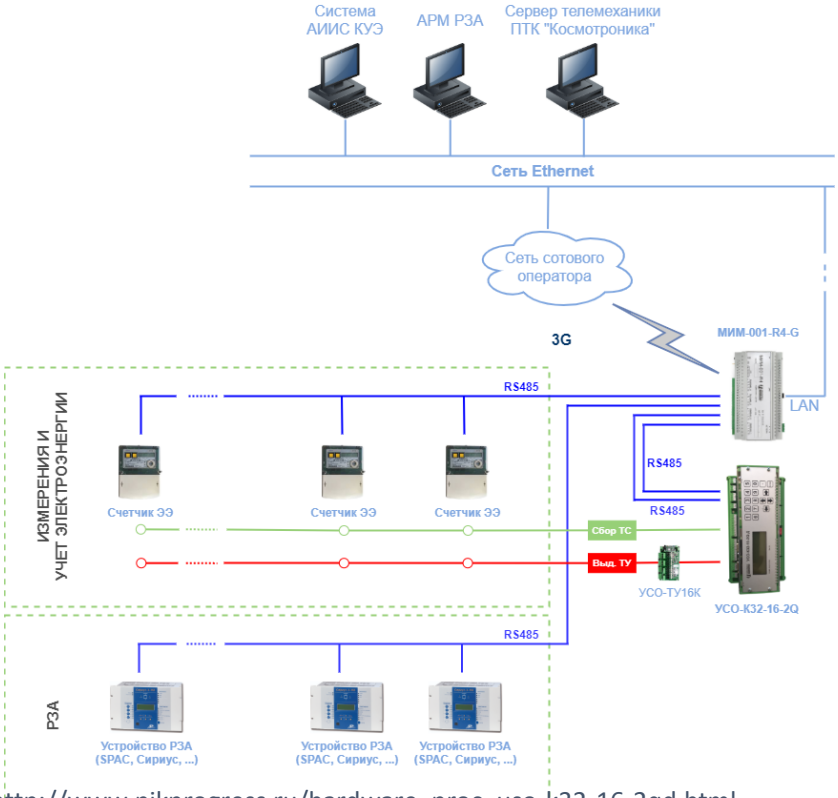
ViPNet IDS NS

- СОА класса В по требованиям ФСБ России
- Завершается сертификация по СОВ уровня сети 4 класса по требованиям ФСТЭК России

Взаимодействие между сегментами сети

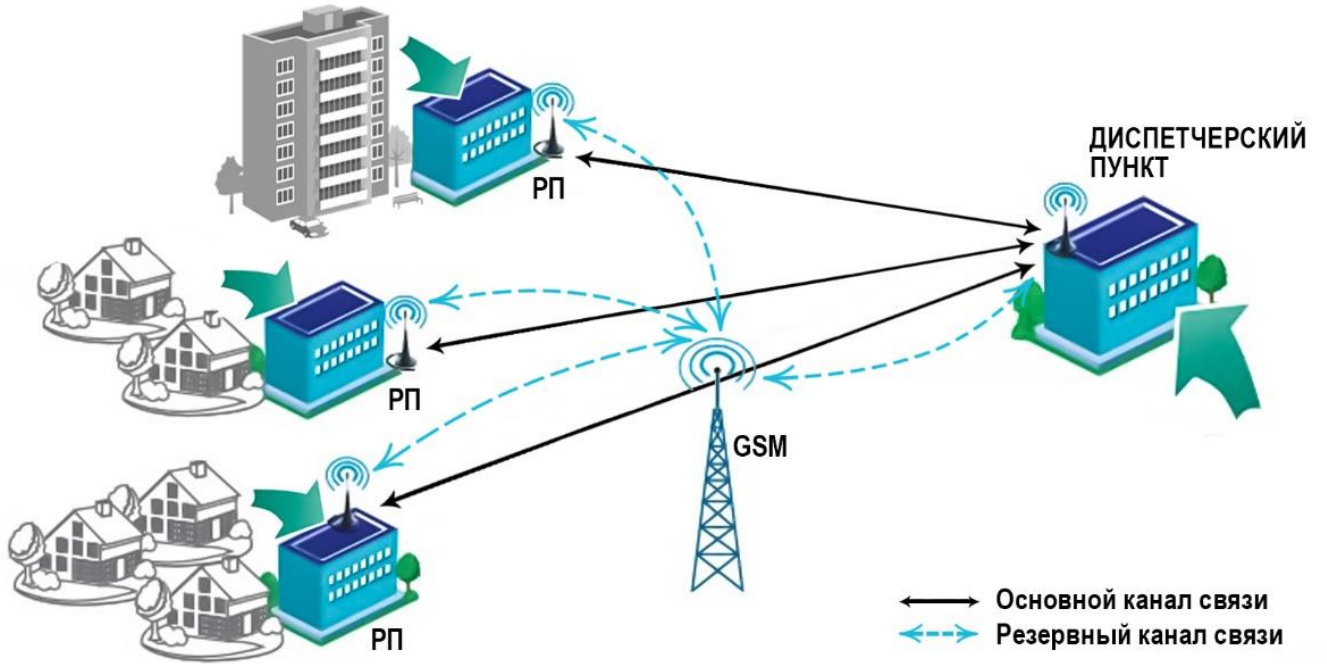
Распределительная электроподстанция





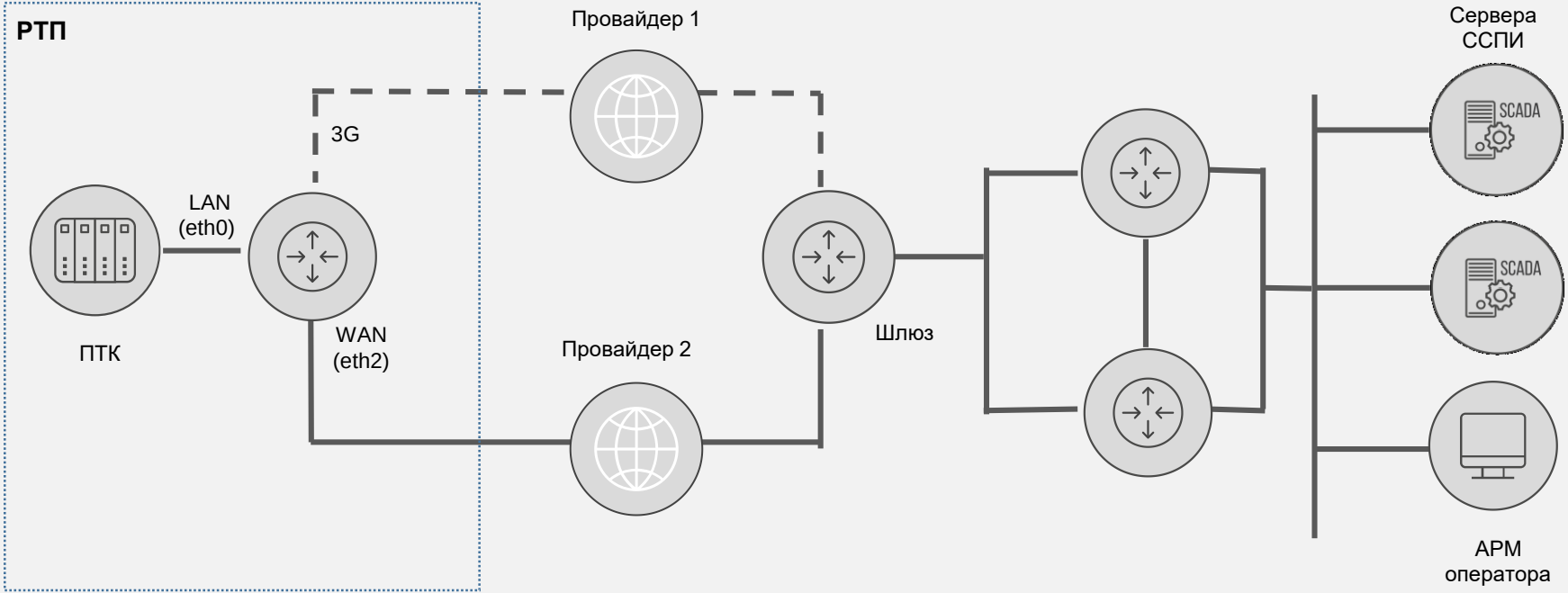
http://www.pikprogress.ru/hardware_proc_uso-k32-16-2qd.html

Распределительная электроподстанция

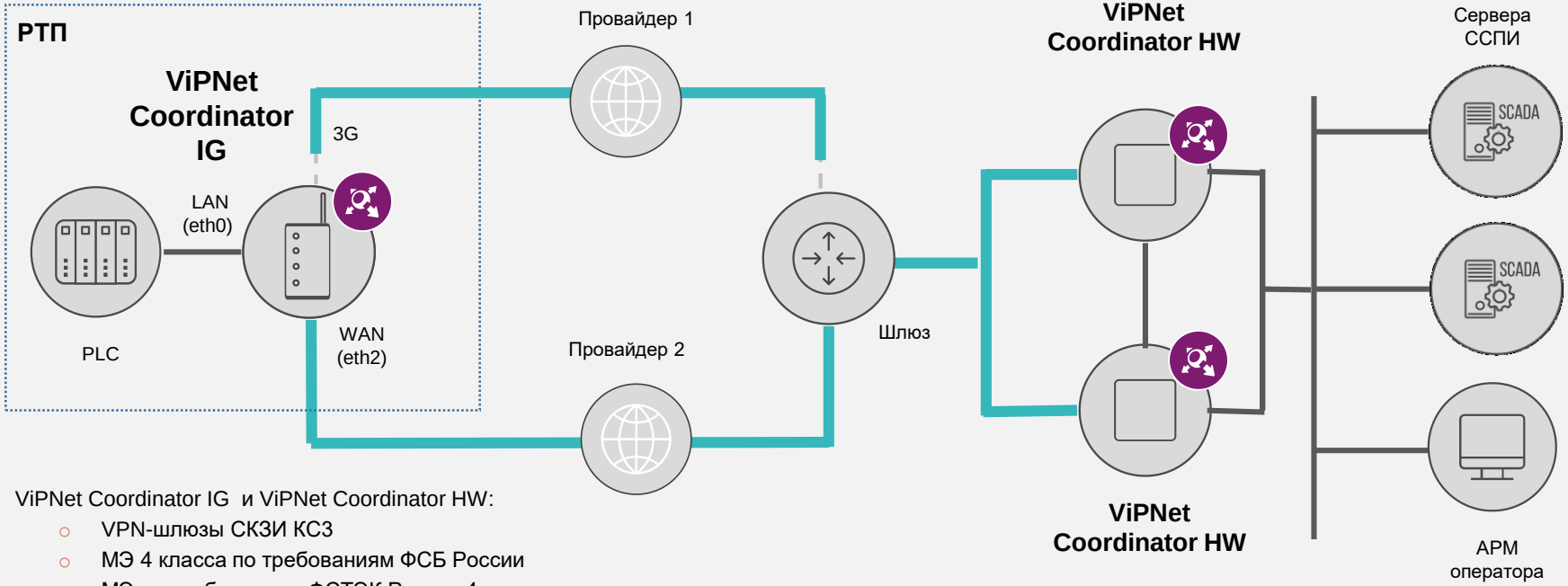


http://svyazstandart.ru/news/201/

Распределительная электроподстанция

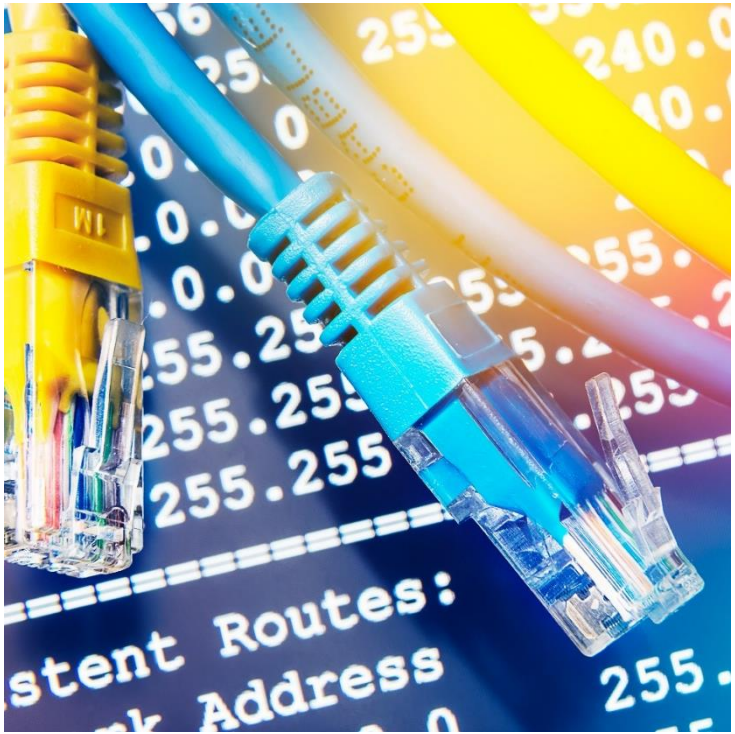


Защита информации для распределительной электроподстанция (минимальный вариант)



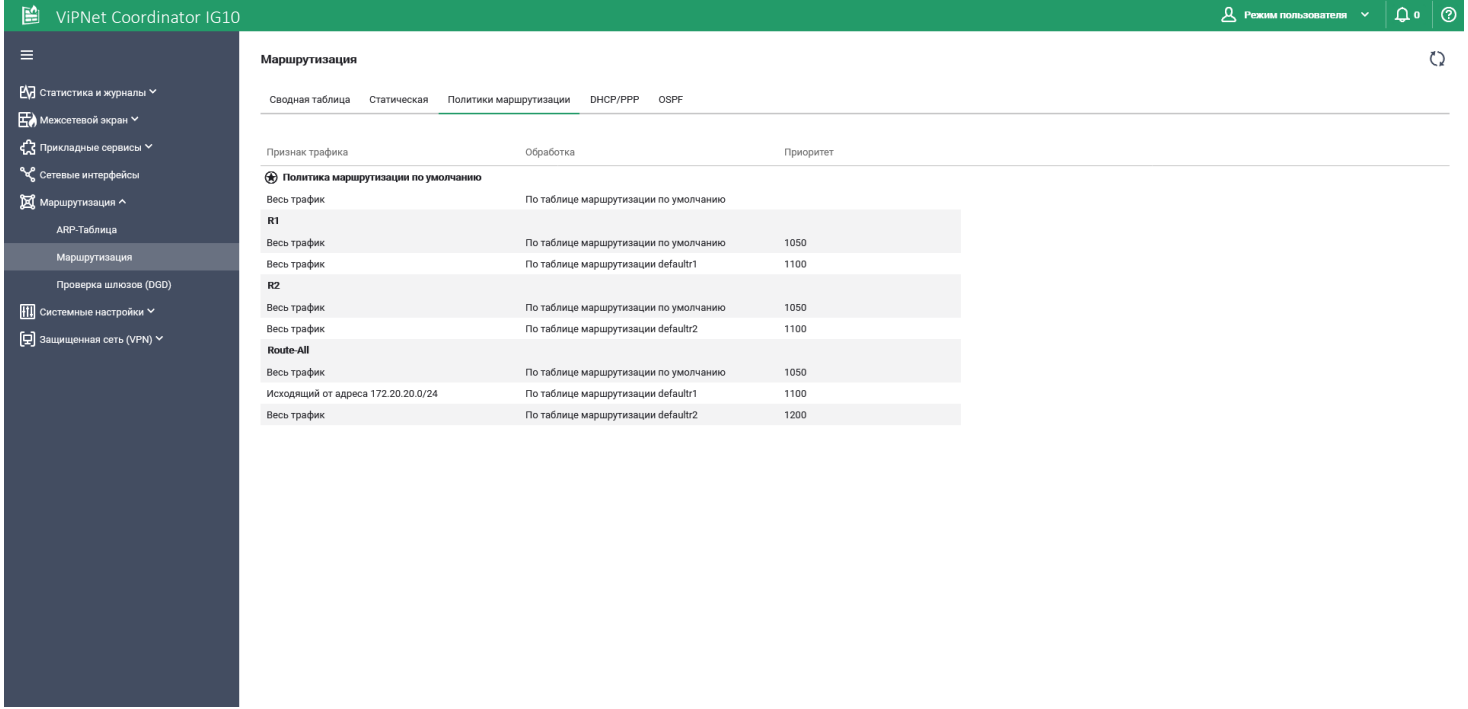
- ViPNet Coordinator IG и ViPNet Coordinator HW:
  - VPN-шлюзы СКЗИ КС3
  - МЭ 4 класса по требованиям ФСБ России
  - МЭ по требованиям ФСТЭК России 4 класса
  - Устройство маршрутизации и коммутации по требования Минкомсвязи России
- ViPNet Coordinator IG - Абонентская радиостанция стандарта GSM-900/1800 и UMTS по требования Минкомсвязи России
- ViPNet Coordinator HW имеет поточный антивирус

MultiWAN в ViPNet Coordinator HW и ViPNet Coordinator IG



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

MultiWAN

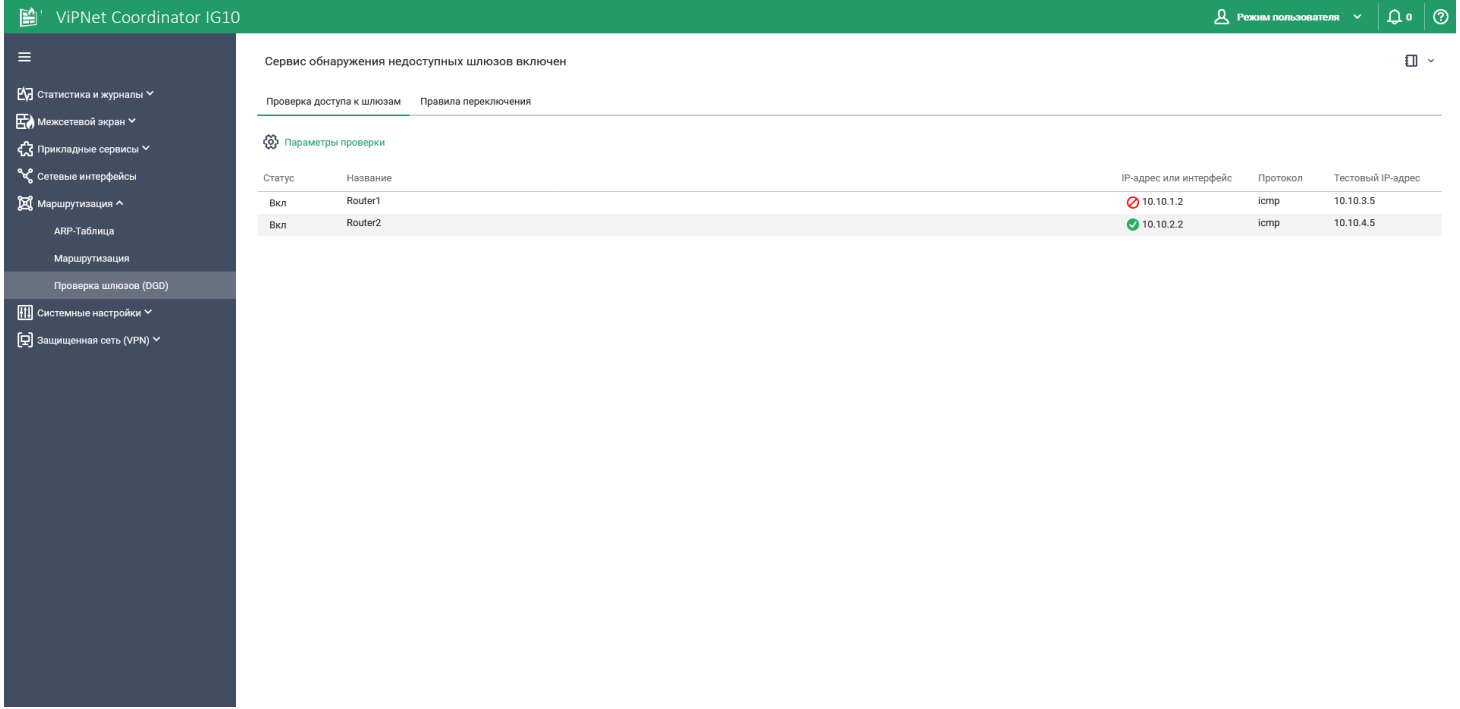


Условия:

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

MultiWAN: резервирование каналов WAN-WAN

Политики маршрутизации



infotecs

MultiWAN: резервирование каналов WAN-WAN

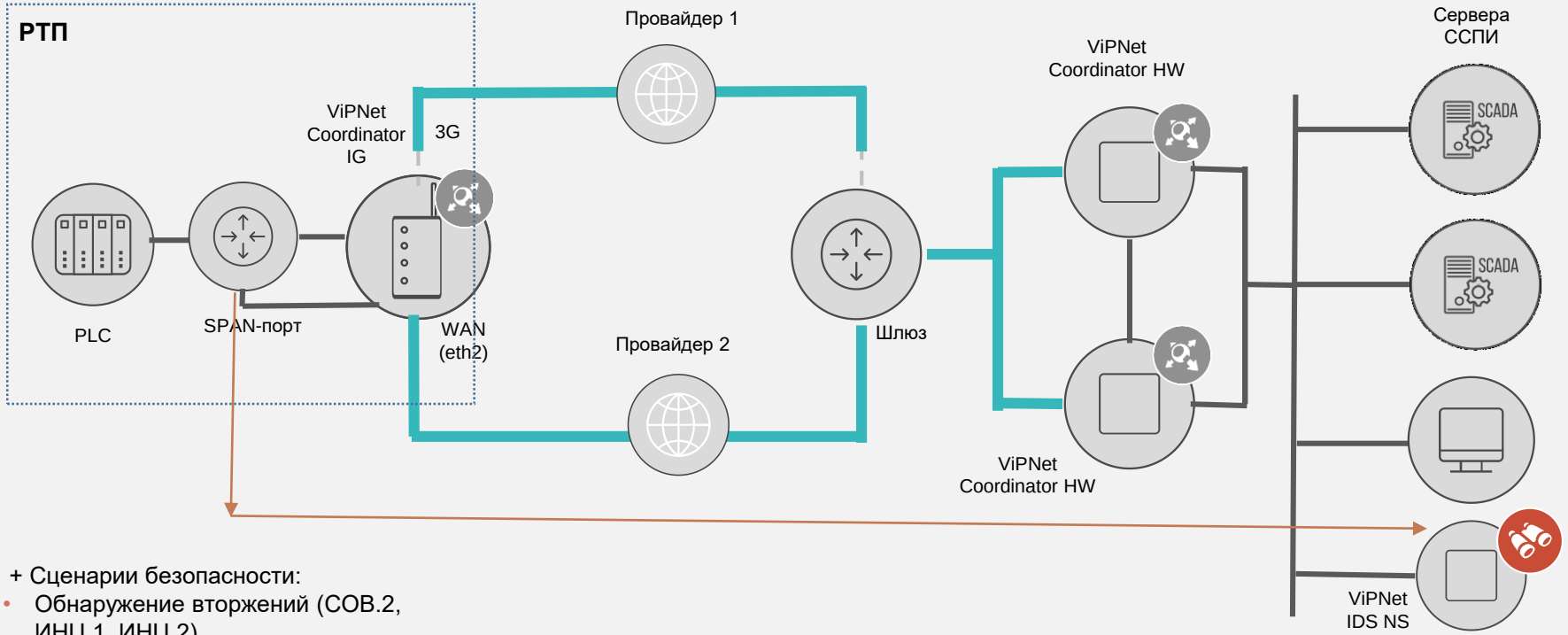
Проверка состояния шлюзов (DGD)

Метод проверки: ICMP, TCP:80, TCP:443

Работает для проводных и беспроводных каналов

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

Защита информации для распределительной электроподстанция (классический вариант)



+ Сценарии безопасности:

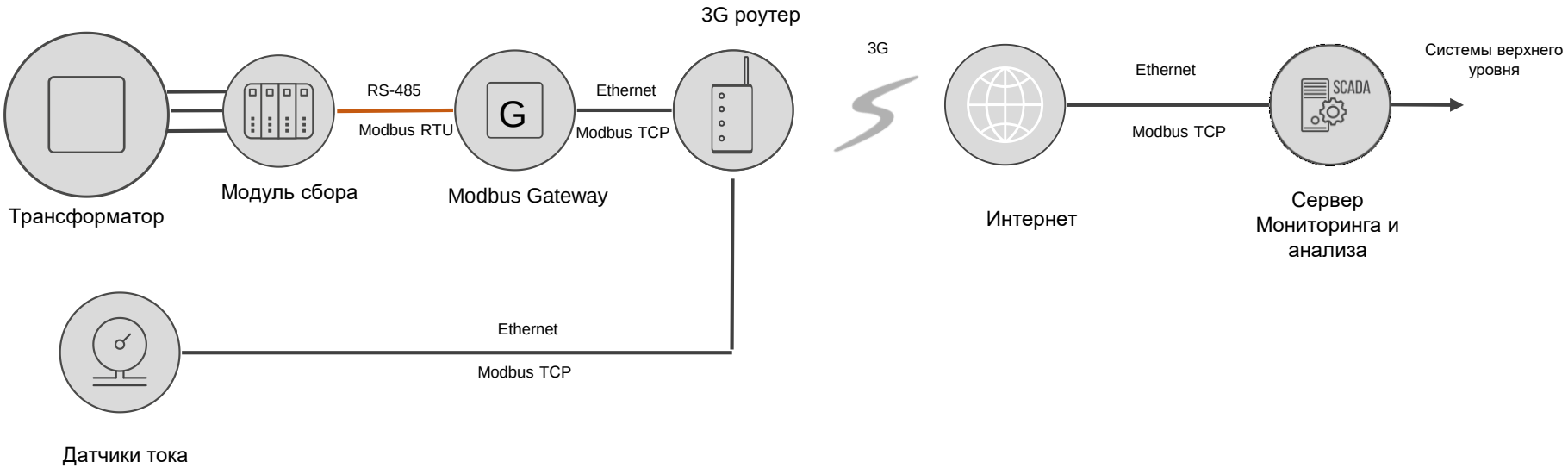
- Обнаружение вторжений (СОВ.2, ИНЦ.1, ИНЦ.2)

Контроль за производственным оборудованием

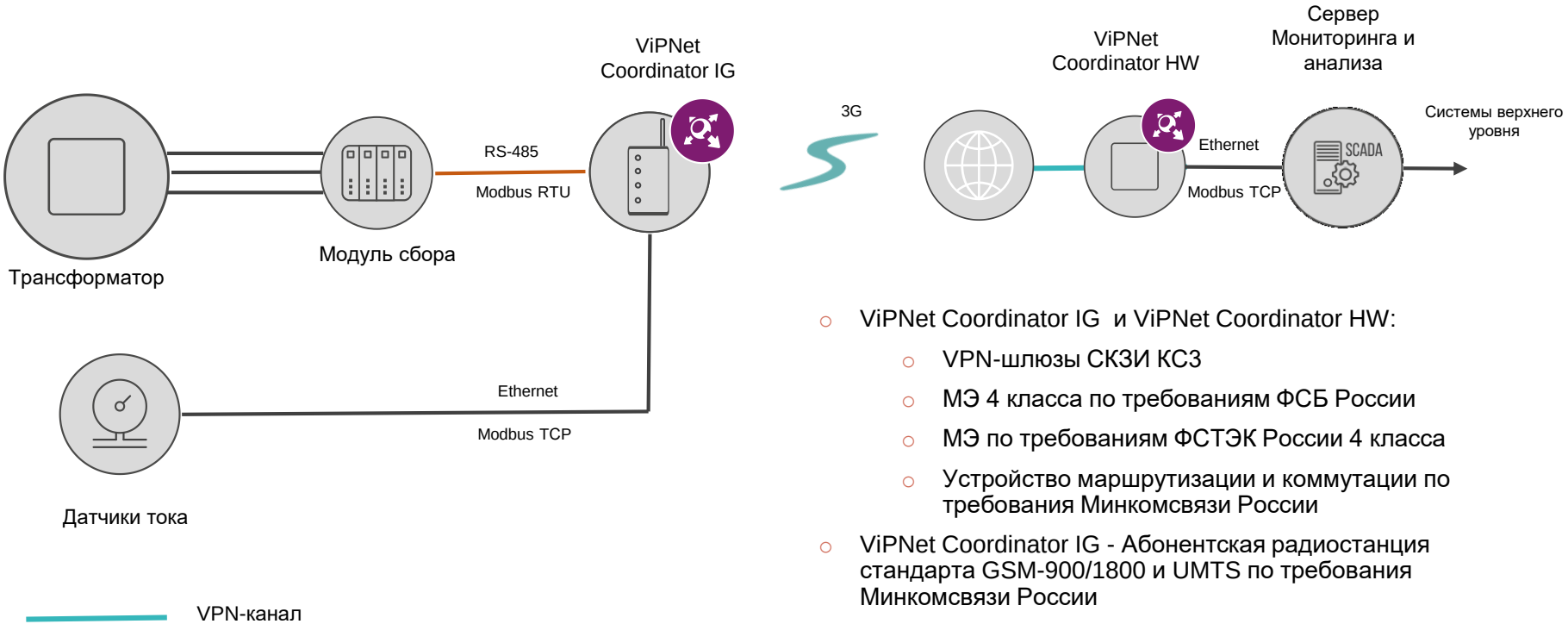
Системы мониторинга высоковольтного оборудования

- 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

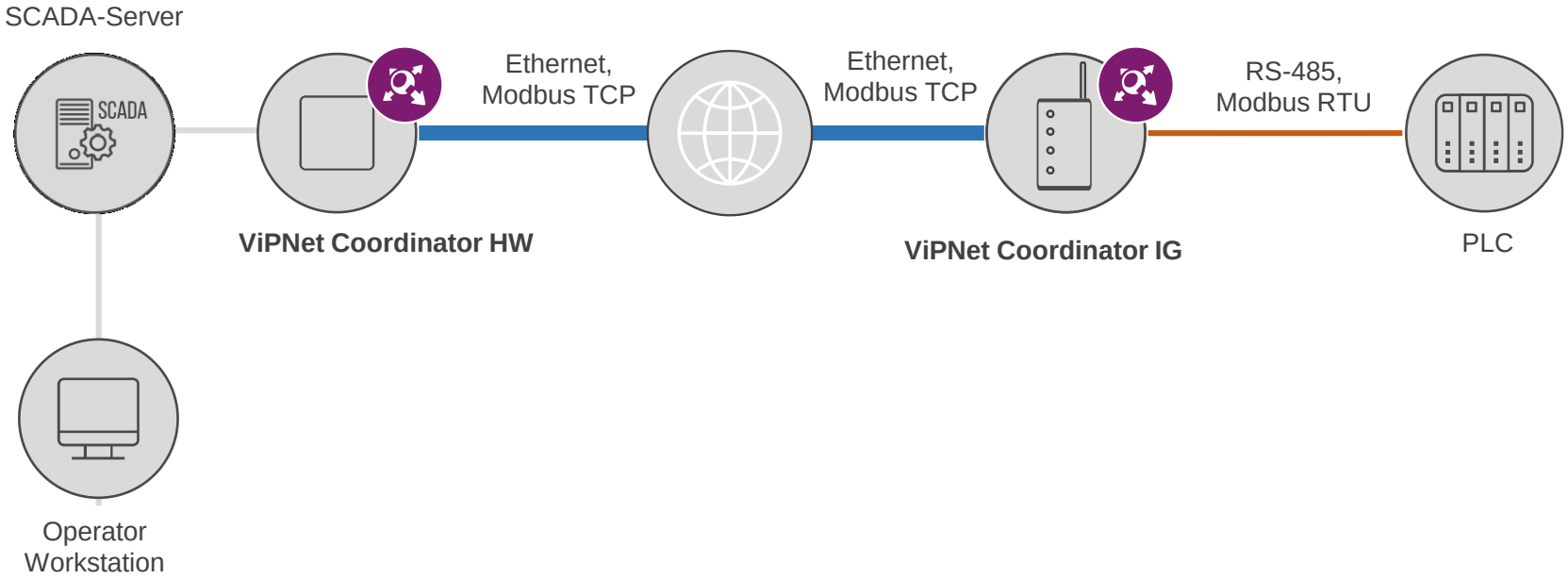


Защита системы мониторинга высоковольтного оборудования (минимальный вариант)

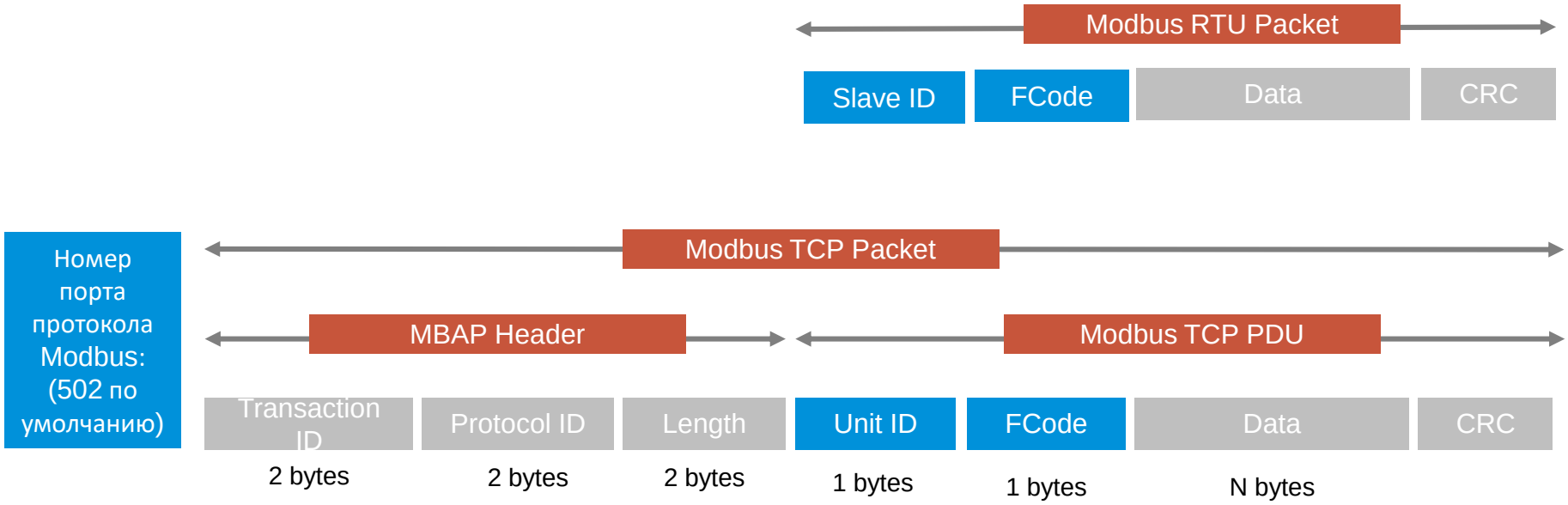


- ViPNet Coordinator IG и ViPNet Coordinator HW:
  - VPN-шлюзы СКЗИ КС3
  - МЭ 4 класса по требованиям ФСБ России
  - МЭ по требованиям ФСТЭК России 4 класса
  - Устройство маршрутизации и коммутации по требования Минкомсвязи России
- ViPNet Coordinator IG - Абонентская радиостанция стандарта GSM-900/1800 и UMTS по требования Минкомсвязи России
- ViPNet Coordinator HW имеет поточный антивирус

Конвертер протоколов Modbus TCP-RTU и RTU-TCP в ViPNet Coordinator IG



Глубокая фильтрация протокола Modbus



Глубокая фильтрация протокола Modbus

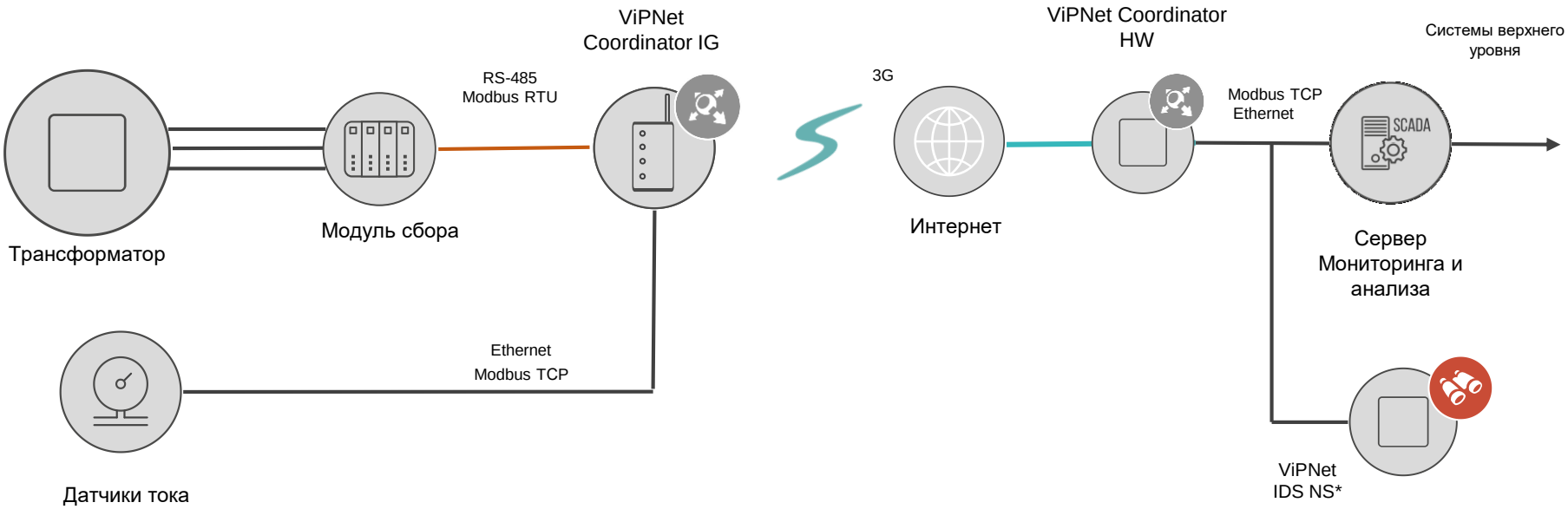
Фильтрация:

- 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

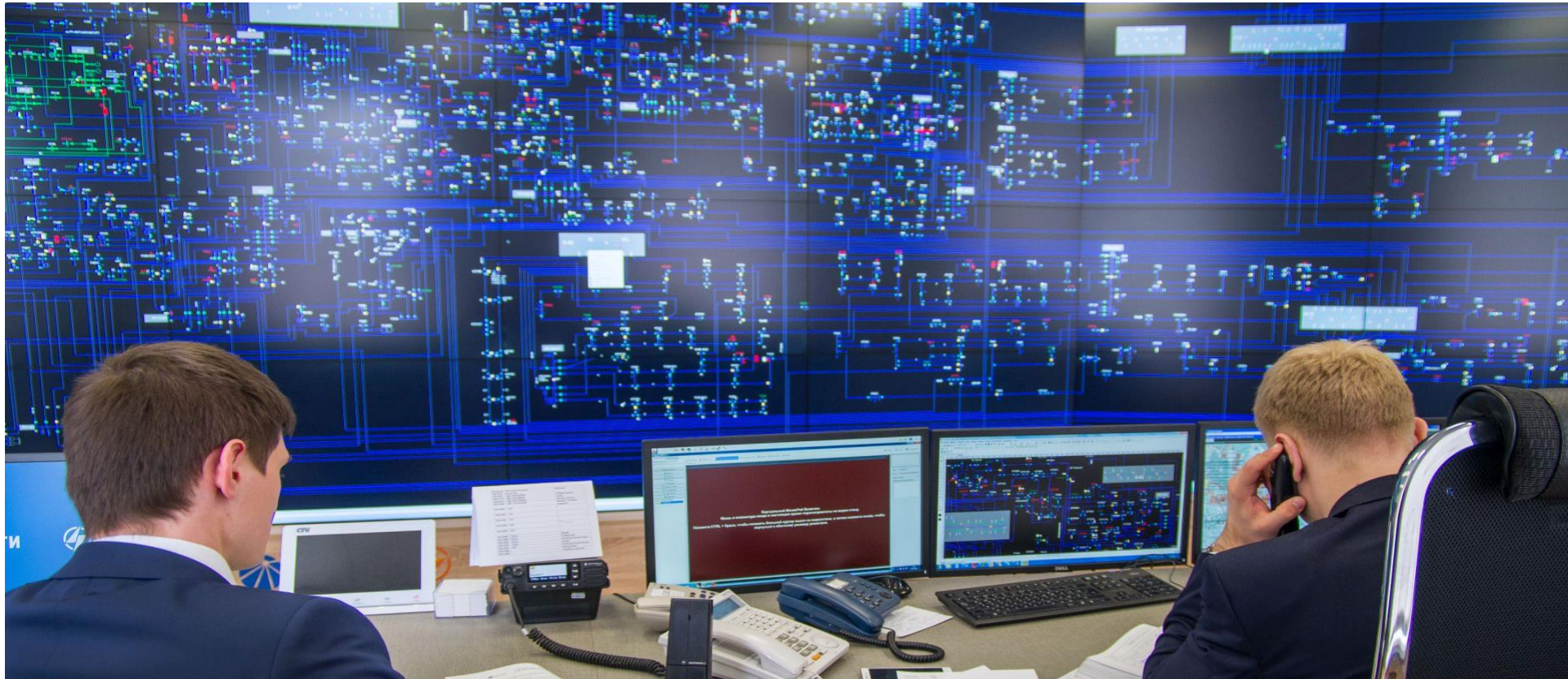
Защита системы мониторинга высоковольтного оборудования (классический вариант)



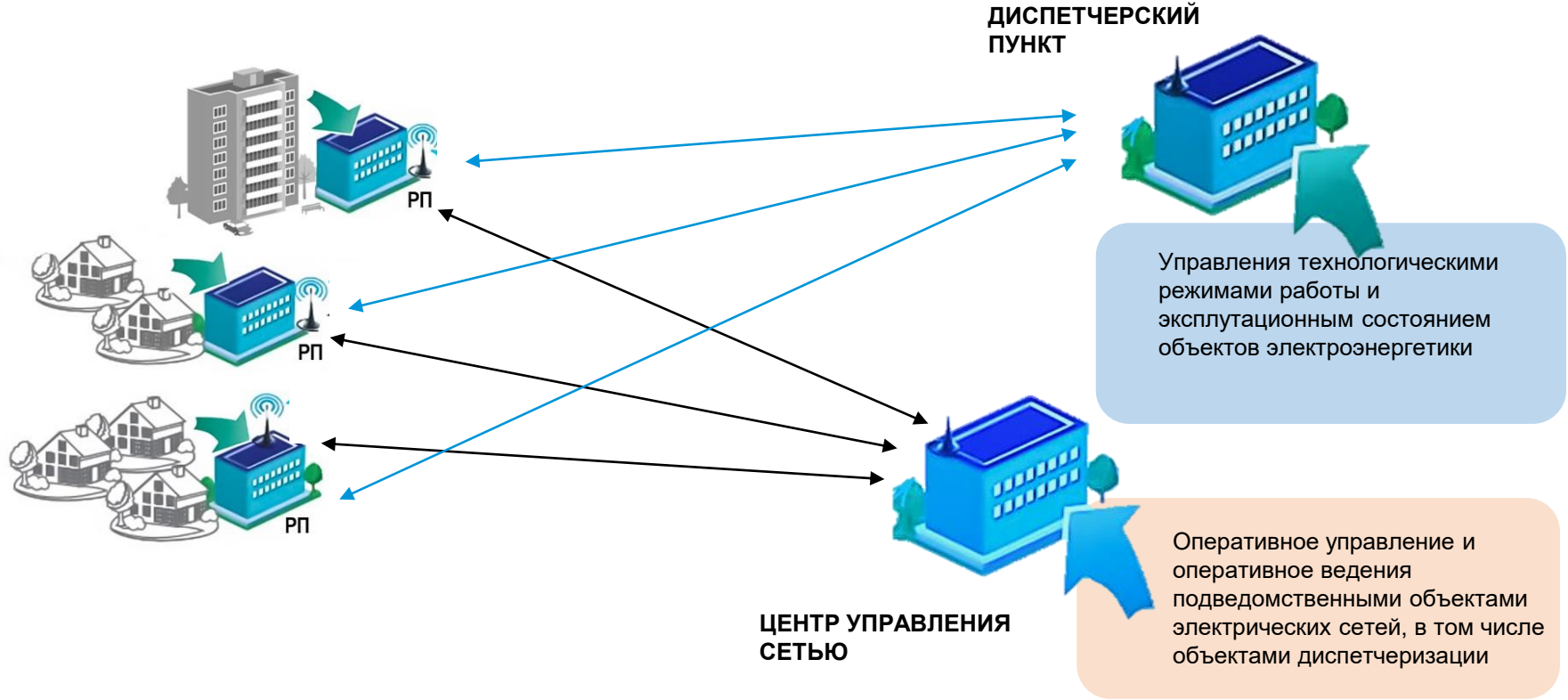
* СОВ уровня сети

Взаимодействие с другими сетями

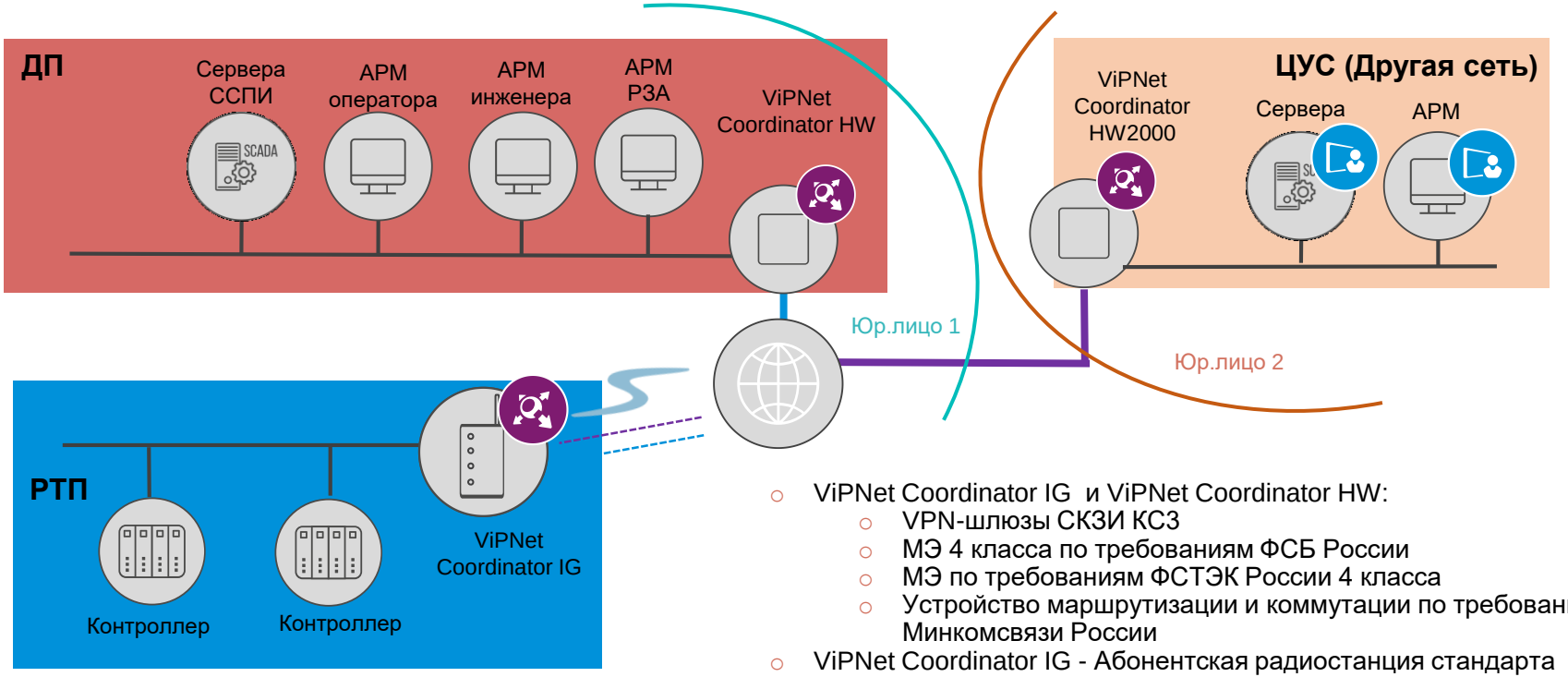
Передача информации в Центр управления сетью



Передача информации в Центр управления сетью



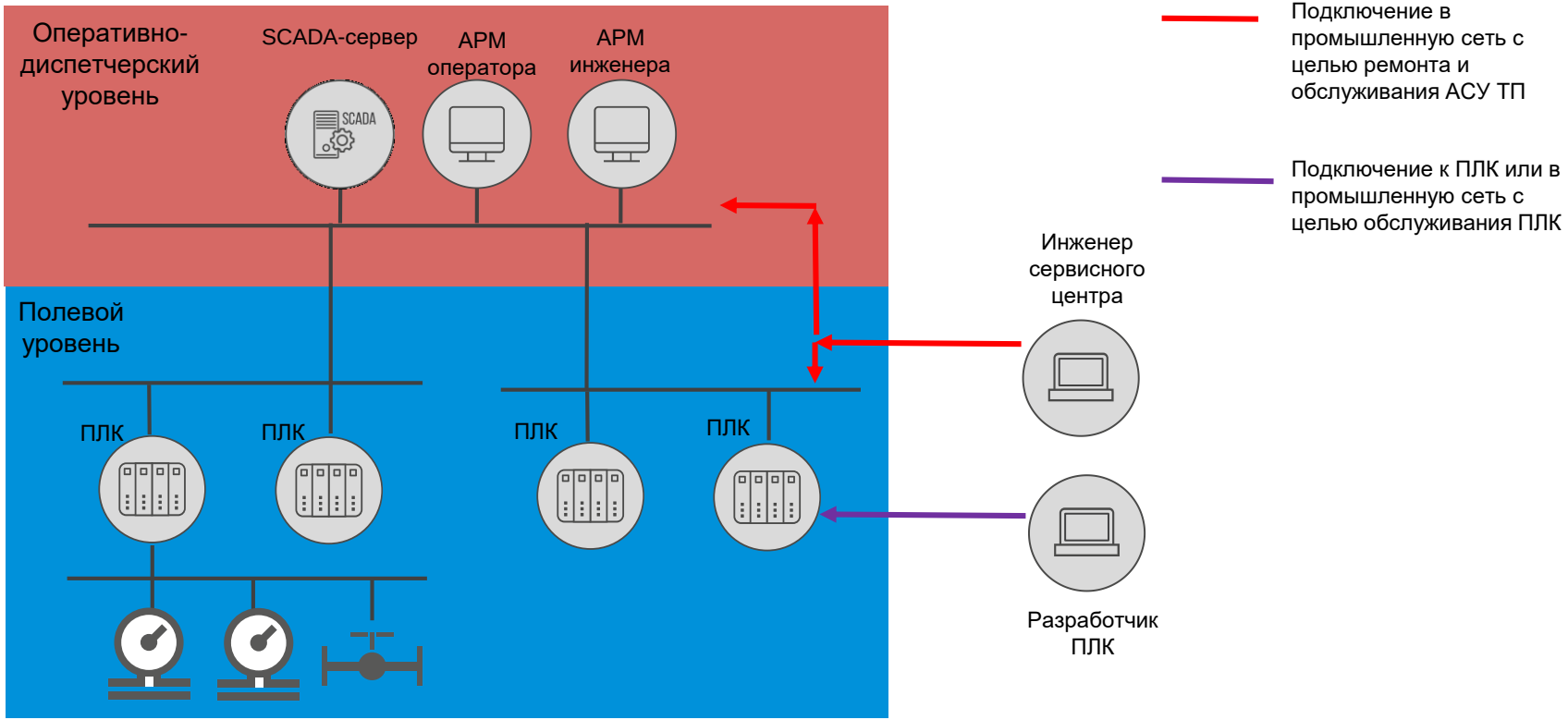
Защита каналов для центра управления сетями электроподстанций (минимальный вариант)



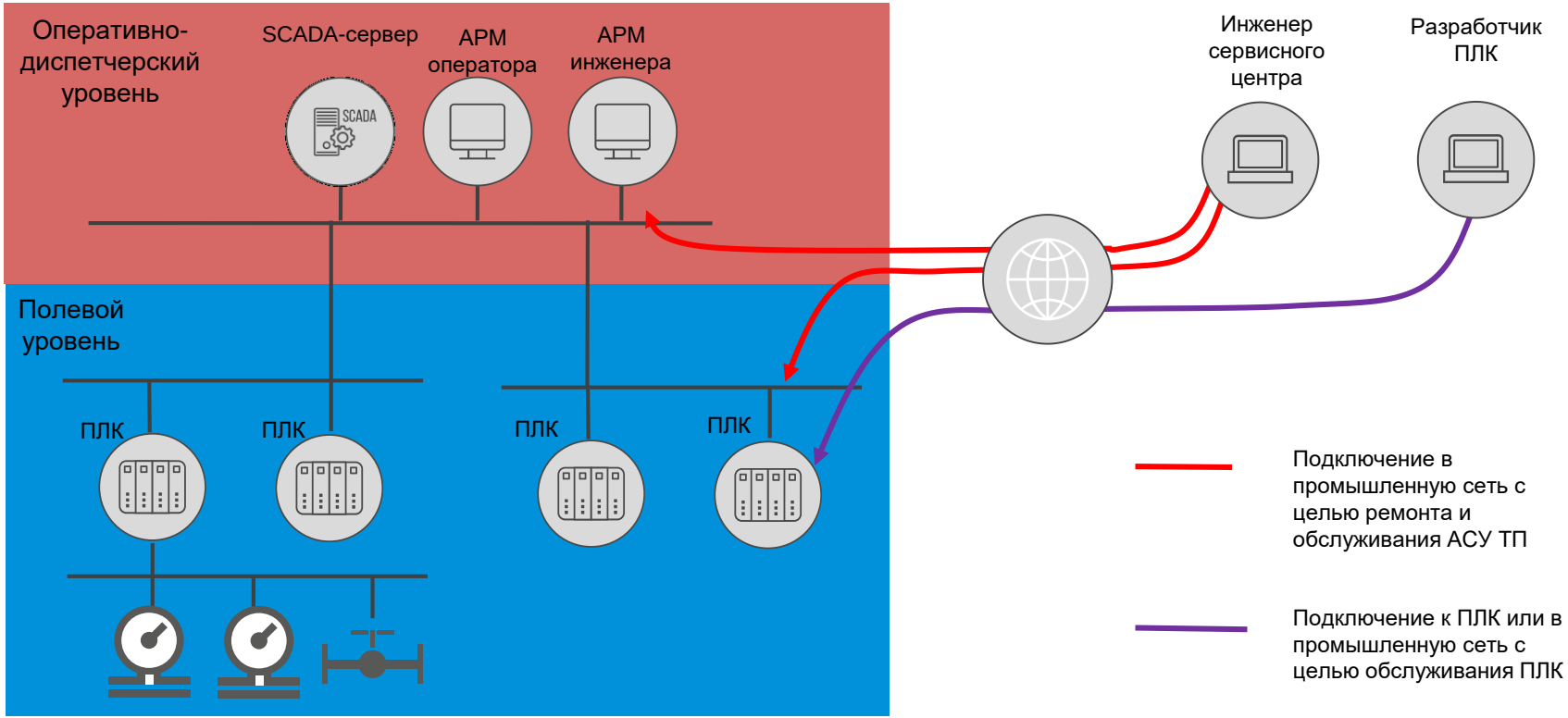
- ViPNet Coordinator IG и ViPNet Coordinator HW:
  - VPN-шлюзы СКЗИ КС3
  - МЭ 4 класса по требованиям ФСБ России
  - МЭ по требованиям ФСТЭК России 4 класса
  - Устройство маршрутизации и коммутации по требования Минкомсвязи России
- ViPNet Coordinator IG - Абонентская радиостанция стандарта GSM-900/1800 и UMTS по требования Минкомсвязи России
- ViPNet Coordinator HW имеет поточный антивирус

Дистанционное сервисное обслуживание/ оказание услуг

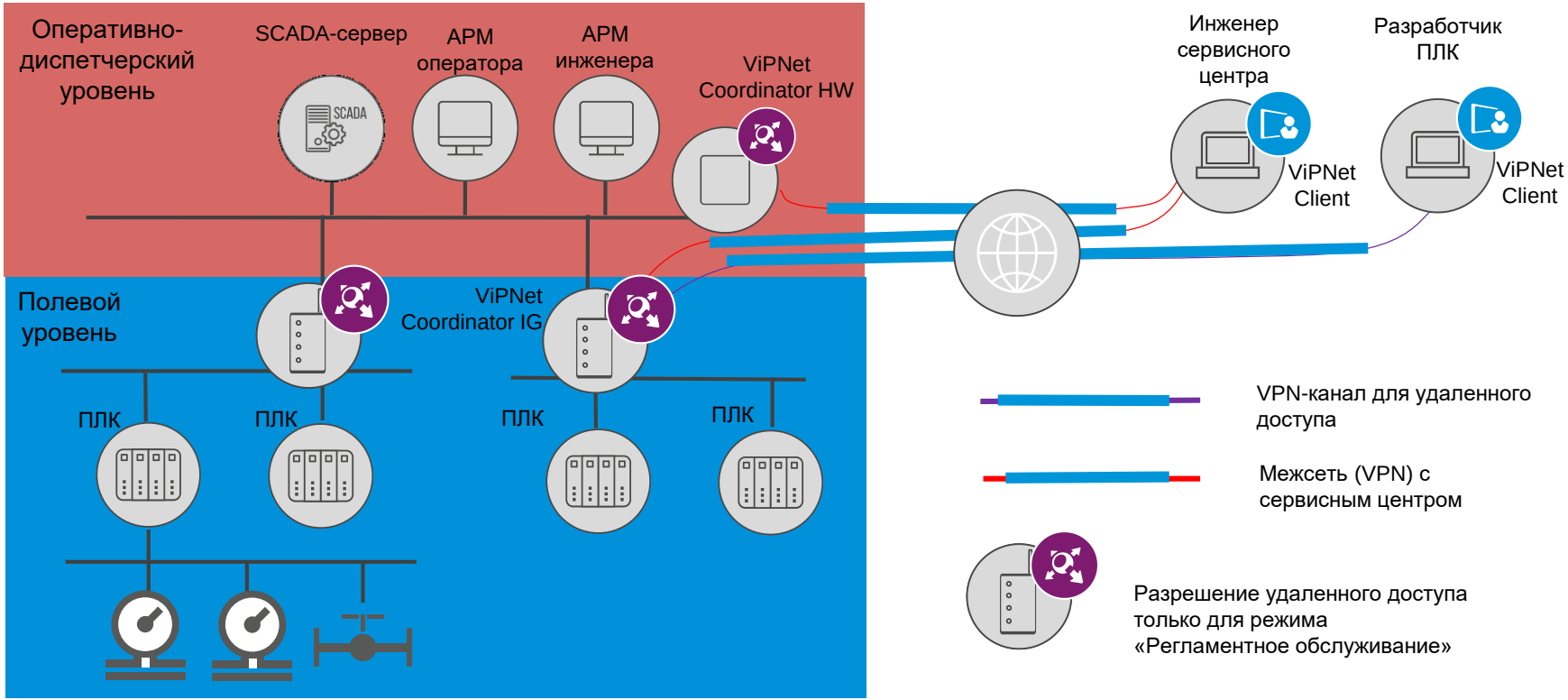
АСУ ТП химического завода



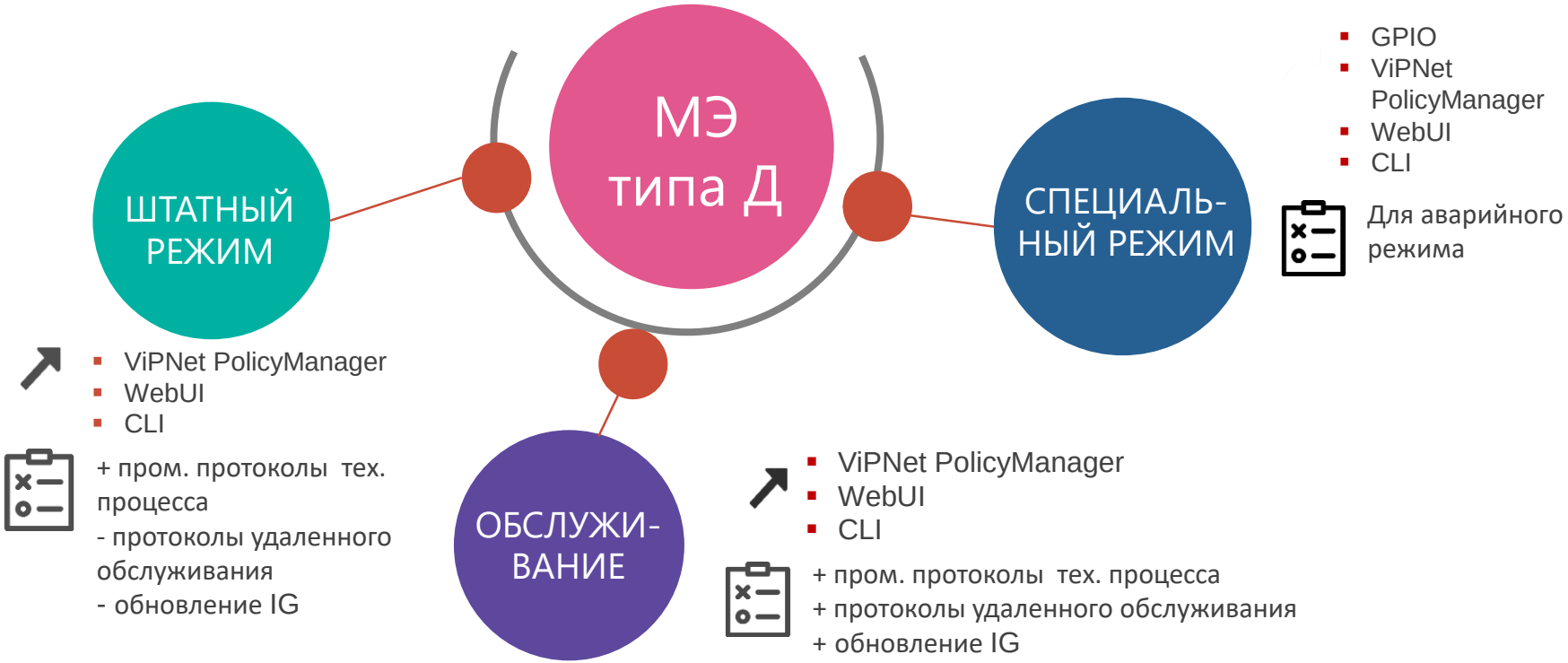
Современная реальность в АСУ ТП химического завода



Защита информации при удаленном подключении к АСУ ТП (часть 1)



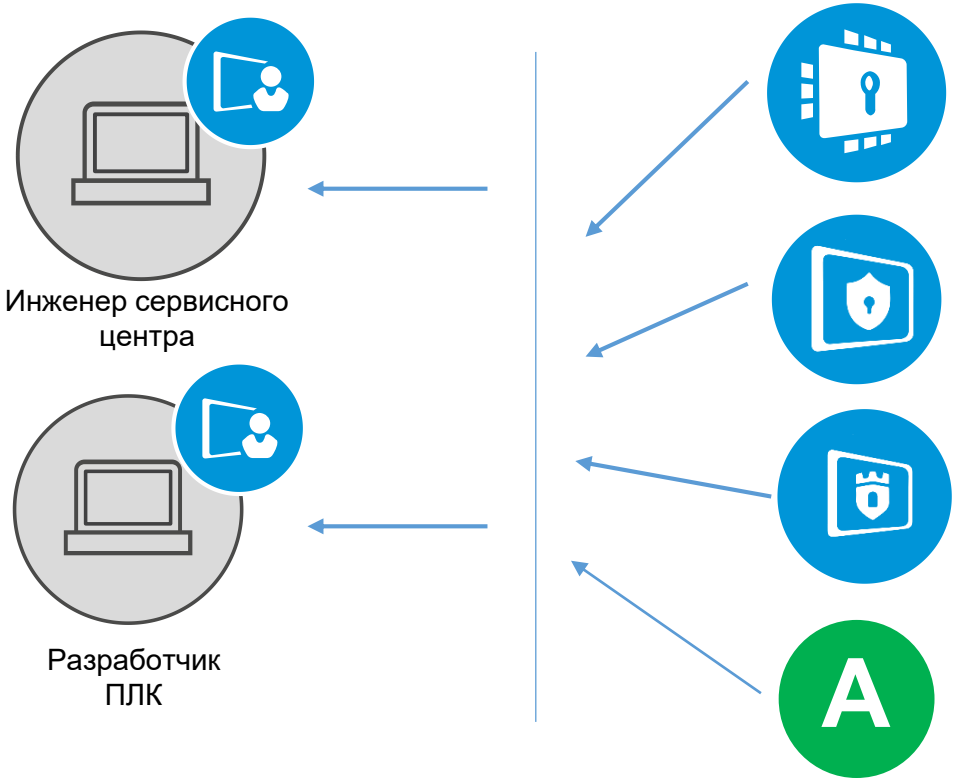
Правила МЭ для разных режимов работы ViPNet Coordinator IG



ViPNet Coordinator HW и ViPNet Coordinator IG

- VPN-шлюз СКЗИ КС3
- МЭ 4 класса по требованиям ФСБ России
- МЭ по требованиям ФСТЭК России ИТ.МЭ.А4.ПЗ
- Устройство маршрутизации и коммутации по требования Минкомсвязи России

Защита информации при удаленном подключении к АСУ ТП (часть 2)



ViPNet SafeBoot

Доверие к платформе и обеспечение доверенной загрузки ОС

ViPNet SafePoint

Разграничение доступа и защита данных

ViPNet EndPoint Protection

Защита от внешних атак и угроз

Антивирус

Защита от внешних атак и угроз

Основные выводы по анализу Приказа №75 ФСТЭК России от 28.05.2020 г

- Приказ не содержит дополнительных требований по защите КИИ
- Все применяемые СЗИ должны соответствовать Приказам ФСТЭК России №239 от 25.12.2017 г. и №235 от 21.12.2017 г.
- Проект Приказа показал «эталонный» вариант реализации требований от ФСТЭК России

Ответы на вопросы

Marina.Sorokina@infotecs.ru
Марина Сорокина

infotecs

Спасибо
за внимание!