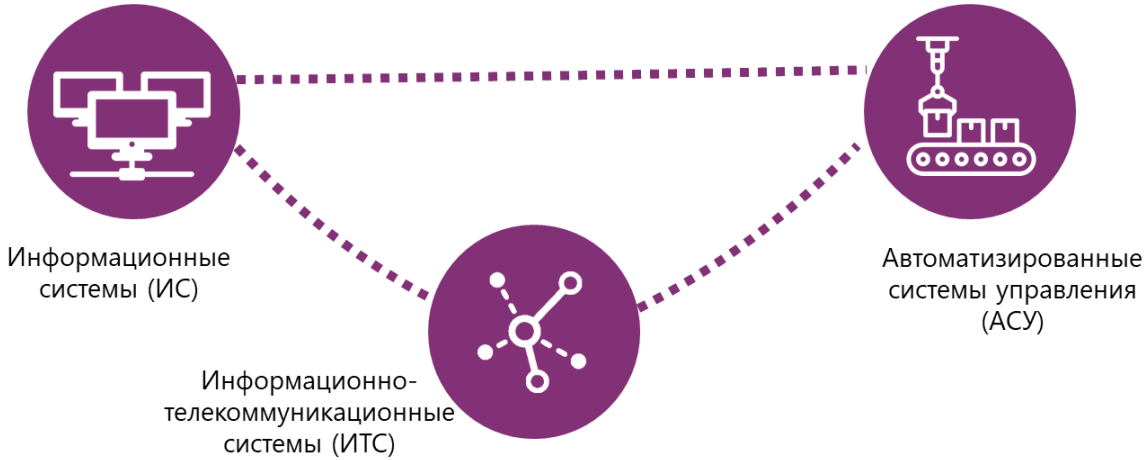
Промышленный шлюз безопасности ViPNet Coordinator IG

Безопасность КИИ РФ

Федеральный закон №187-ФЗ «О безопасности КИИ»

- Государственные органы
- Государственные учреждения
- Юридические лица
- ИП

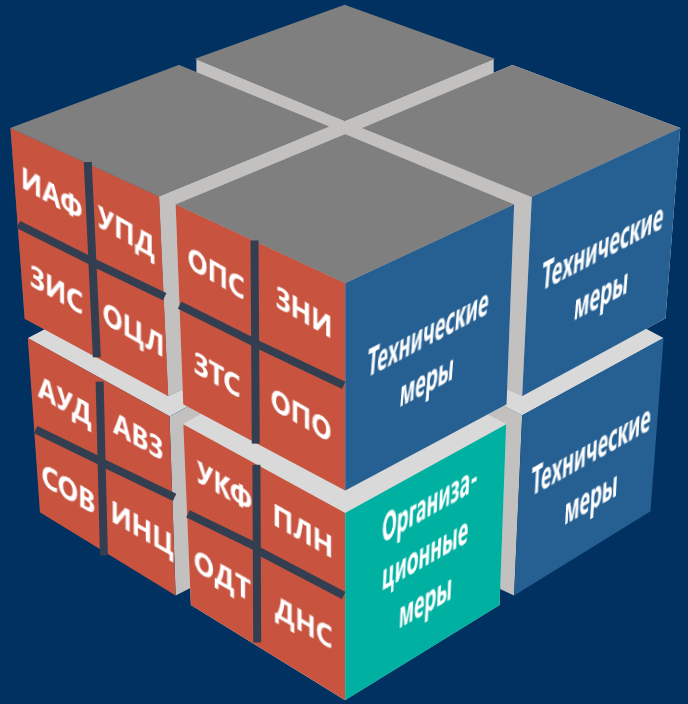


Объекты КИИ

- Требования к созданию систем безопасности объектов КИИ (Приказ ФСТЭК России N235 от 21.12.2017г.)
- Требования по обеспечению безопасности объектов КИИ (Приказ ФСТЭК России N239 от 25.12.2017 г.)

Состав мер по защите объектов КИИ согласно Приказу №239 ФСТЭК России

ТЕХНО 2020 infotecs фест



I. Идентификация и аутентификация (ИАФ)
II. Управление доступом (УПД)
III. Ограничение программной среды (ОПС)
IV. Защита машинных носителей информации (ЗНИ)
V. Аудит безопасности (АУД)
VI. Антивирусная защита (АВЗ)
VII. Предотвращение вторжений (компьютерных атак) (СОВ)
VIII. Обеспечение целостности (ОЦЛ)
IX. Обеспечение доступности (ОДТ)
X. Защита технических средств и систем (ЗТС)
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
XII. Планирование мероприятий по обеспечению безопасности (ПЛН)
XIII. Управление конфигурацией (УКФ)
XIV. Управление обновлениями программного обеспечения (ОПО)
XV. Реагирование на инциденты информационной безопасности (ИНЦ)
XVI. Обеспечение действий в нештатных ситуациях (ДНС)
XVII. Информирование и обучение персонала (ИПО)

всего 152 меры

ViPNet Coordinator IG

Промышленные шлюзы безопасности ViPNet Coordinator IG

Сценарии

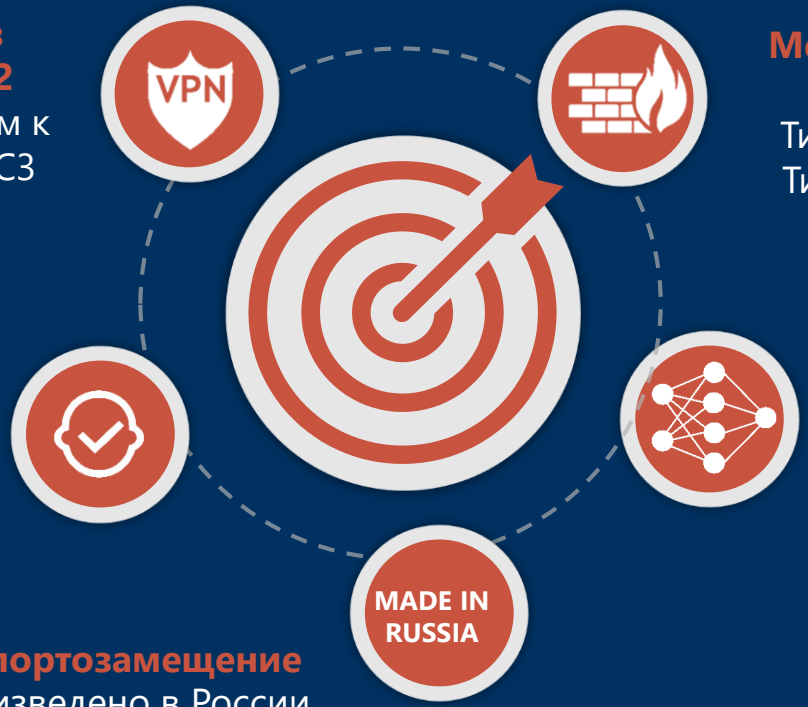
- защита периметра сети
- сегментирования сети и разграничения доступа к ее сегментам
- защиты проводных и беспроводных каналов связи сети
- организация ДМЗ
- управление сетевыми потоками
- сокрытие реальных адресов и архитектуры сети
- организации удаленного доступа для стационарных и мобильных пользователей,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

ViPNet Coordinator IG

ТЕХНО 2020 infotecs ФЕСТ

VPN – шлюз уровня L3, L2
По требованиям к СКЗИ класса КС3

Межсетевой экран SPI, DPI
Типа «Д» 4 класса
Типа «А» 4 класса



Доверенная платформа
Собственная схемотехника

Коммуникации
Проводные, 3G, Wi-fi

Импортозамещение
Произведено в России

Исполнения ViPNet Coordinator IG

ViPNet Coordiantor
IG10 I1

ViPNet Coordiantor
IG100 I1

ViPNet Coordiantor
IG10 I2*

* Планы Q4 2020

Исполнения ViPNet Coordinator IG

	ViPNet Coordinator IG10 I1	ViPNet Coordinator IG100 I1	ViPNet Coordinator IG10 I2
Производительность L3 VPN и L2 VPN	до 10 Мбит/с	до 60 Мбит/с	до 100 Мбит/с
Производительность МЭ	до 10 Мбит/с	до 60 Мбит/с	до 100 Мбит/с
Проводные интерфейсы	Ethernet 3xRJ45	Ethernet 3xRJ45	Ethernet 5xRJ45
Беспроводные модули	3G или LTE*, Wi-Fi 2,4 ГГц	3G или LTE*, Wi-Fi 2,4 ГГц	3G или LTE*, 2 Sim Wi-Fi 2,4 ГГц
Питание	12 - 24 В DC, 15 Вт	12 - 24 В DC, 10 Вт	2 входа питания: 12 - 24 В DC, 25 Вт
Рабочая температура	-20^{0}C (-40 ^{0}C)...+60^{0}C	-20^{0}C...+60^{0}C	-40^{0}C...+60^{0}C
ЭМС	ГОСТ Р51318-22 (СИСПР 22), ГОСТ CISPR 24 2013 (СИСПР 24)	ГОСТ Р51318-22 (СИСПР 22), ГОСТ CISPR 24 2013 (СИСПР 24)	ГОСТ Р51318-22 (СИСПР 22), ГОСТ CISPR 24 2013 (СИСПР 24), ГОСТ Р 51317.6.5-2006 (МЭК 61000-6-5:2001)

* Планы Q4 2020

ViPNet Coordinator IG: характеристики

ТЕХНО 2020 infotecs ФЕСТ

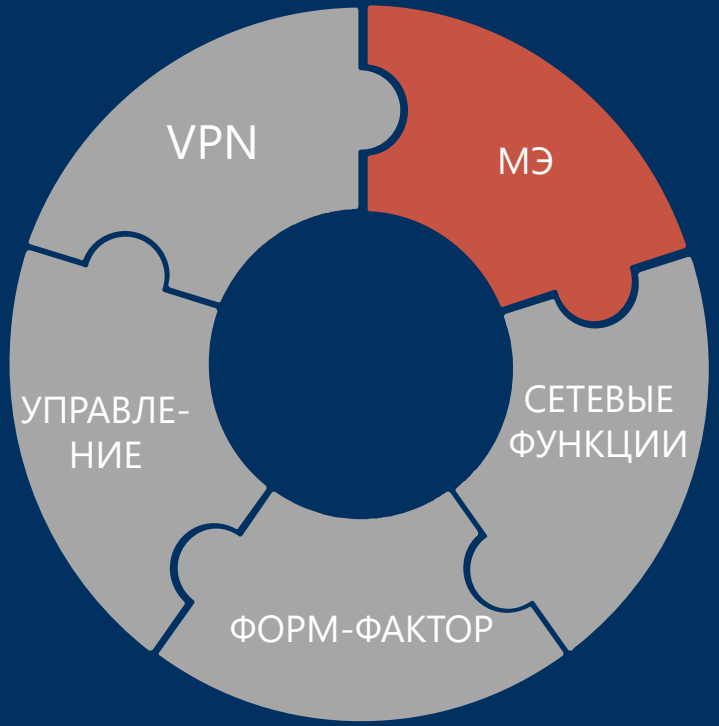
VPN

- ViPNet VPN-шлюз сетевого уровня L3
- ViPNet VPN-шлюз сетевого уровня L2 (L2OverIP)
- VPN-сервер
- 10 и 60 Мбит/с
- Аутентификация для каждого зашифрованного IP-пакета
- СКЗИ класса КС3 по требованиям ФСБ России

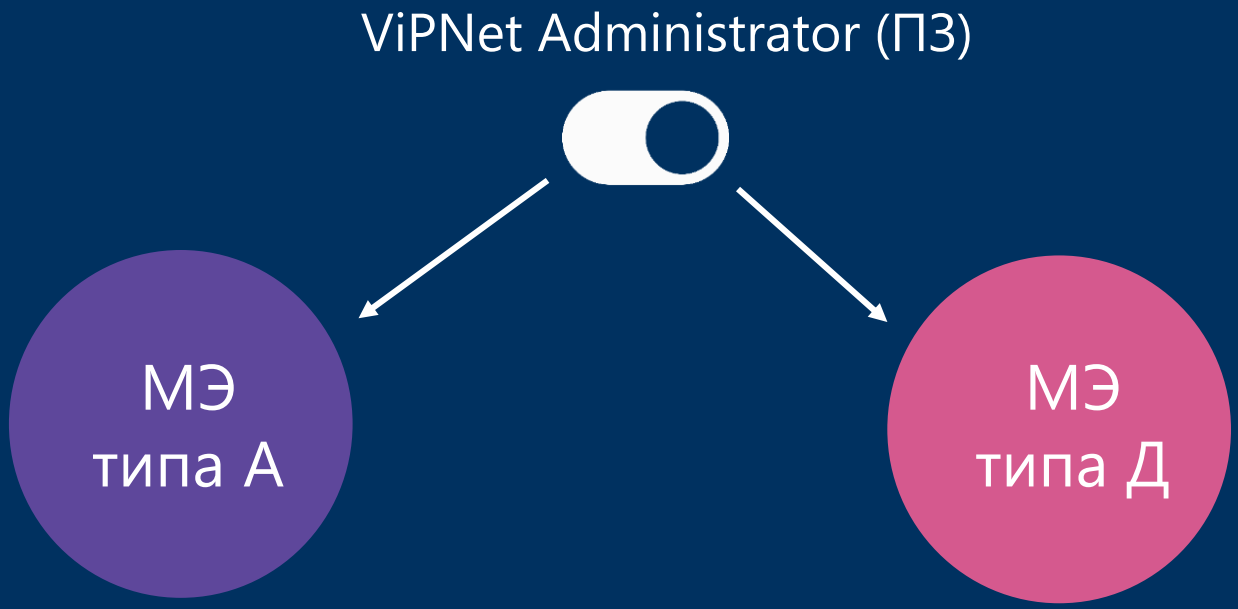
ViPNet Coordinator IG: характеристики

МЕЖСЕТЕВОЙ ЭКРАН

- NAT,
- Антиспуффинг
- Фильтрация по портам, адресам и типам протоколов
- Раздельные наборы фильтров для разных режимов работы
- DPI для Modbus TCP/RTU
- МЭ 4 класса защищенности по требованиям ФСБ России
- Сертификат МЭ типа А.4 и Д.4 4 квартал 2020 г.



Межсетевой экран



Правила МЭ для разных режимов работы ViPNet Coordinator IG

Промышленный межсетевой экран

ТЕХНО 2020 infotecs ФЕСТ

Фильтрация по сетевым адресам отправителя и получателя

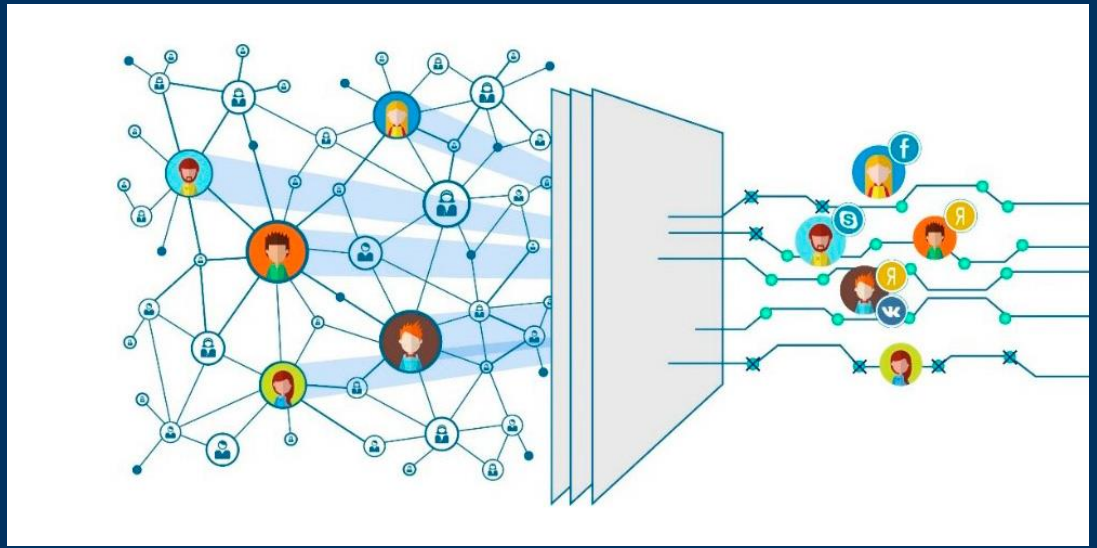
Фильтрация по протоколам сетевого и транспортного уровня

Фильтрация по портам источника и получателя в рамках сессии

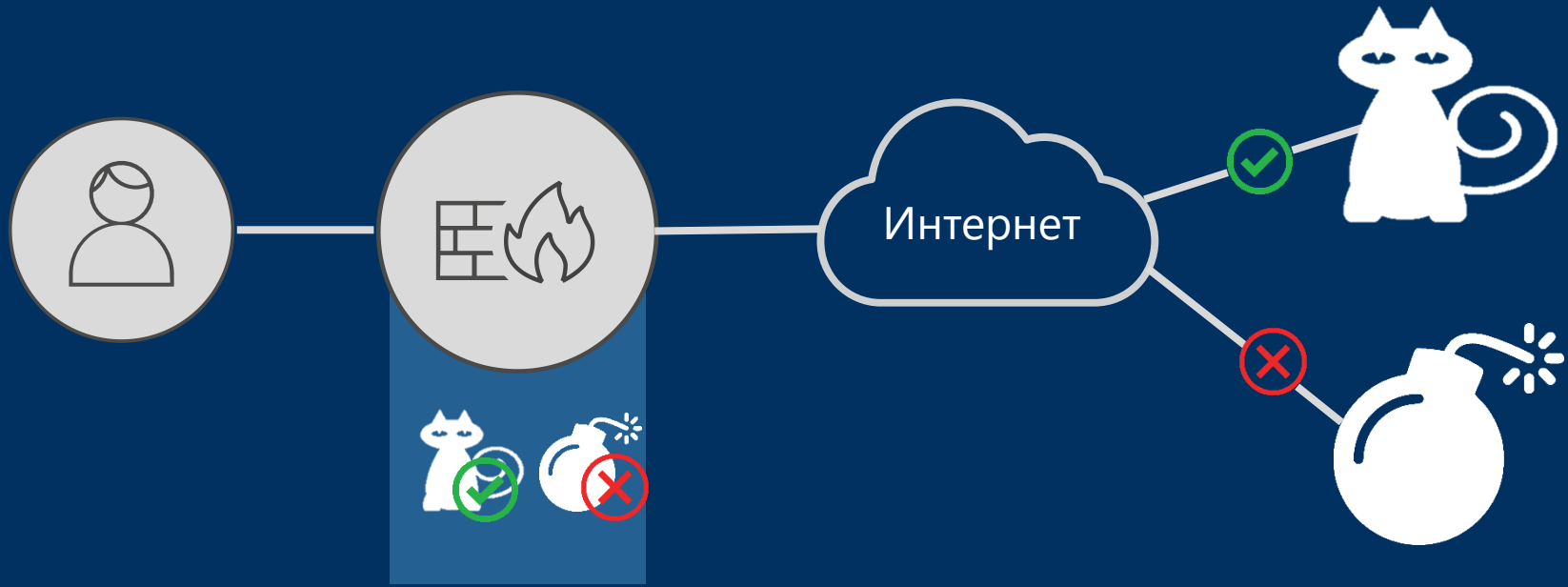
Фильтрация по протоколам прикладного уровня Разрешенные и запрещенные команды

Фильтрация по протоколам прикладного уровня

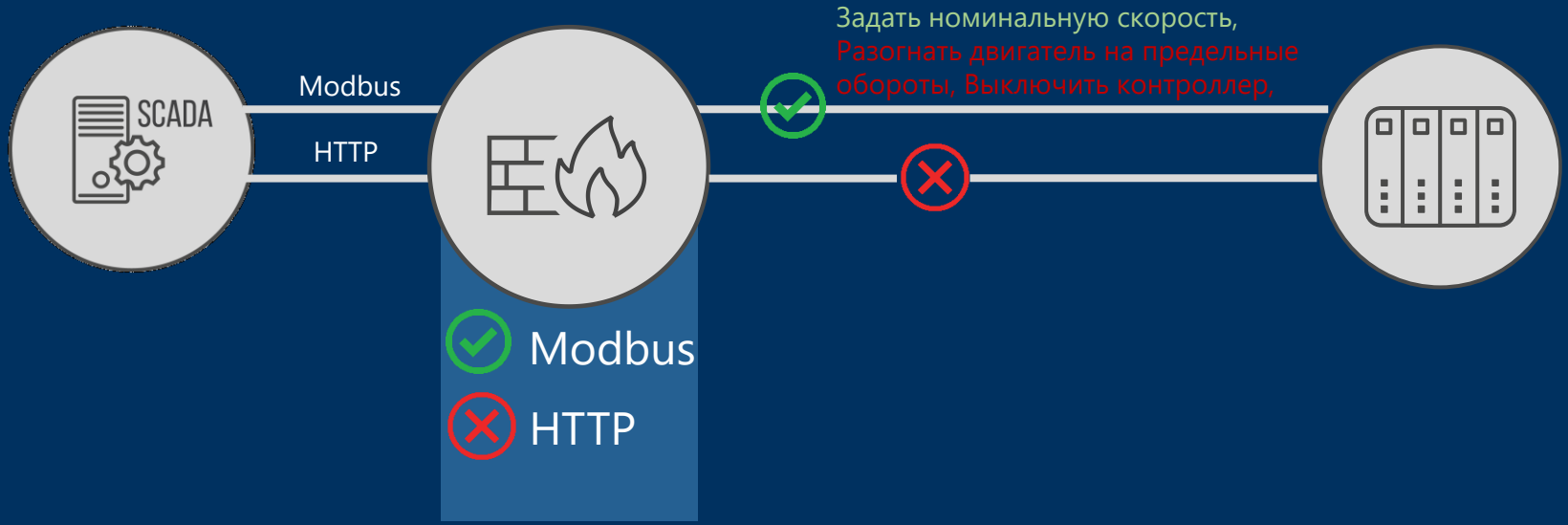
В чем разница между фильтрацией по протоколам прикладного уровня для корпоративных систем (IT) и Автоматизированных систем управления (OT)?



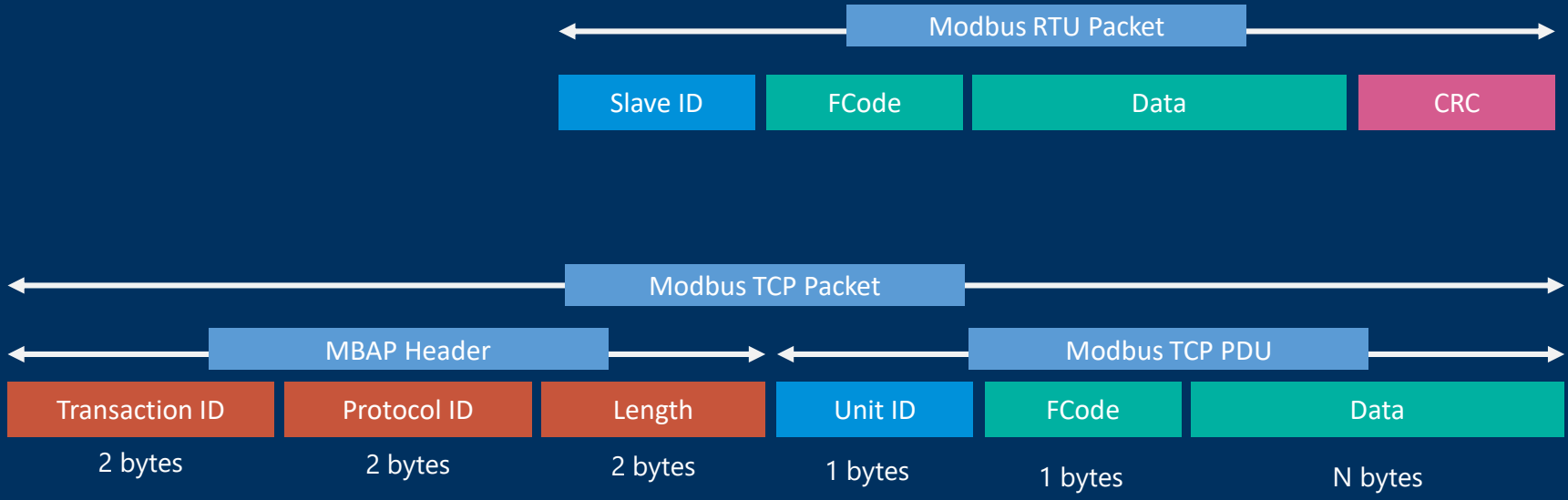
Фильтрация по протоколам прикладного уровня для корпоративных систем



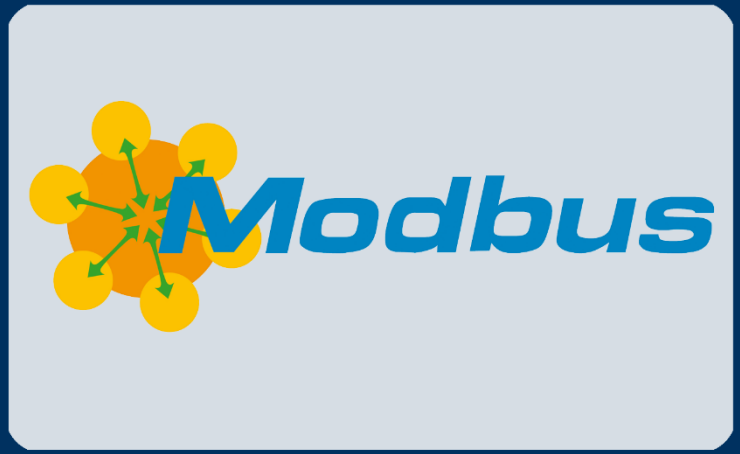
Фильтрация по протоколам прикладного уровня на уровне определения протокола в АСУ



Фильтрация по протоколам прикладного уровня на уровне полей протокола



Фильтрация на прикладном уровне в ViPNet Coordinator IG

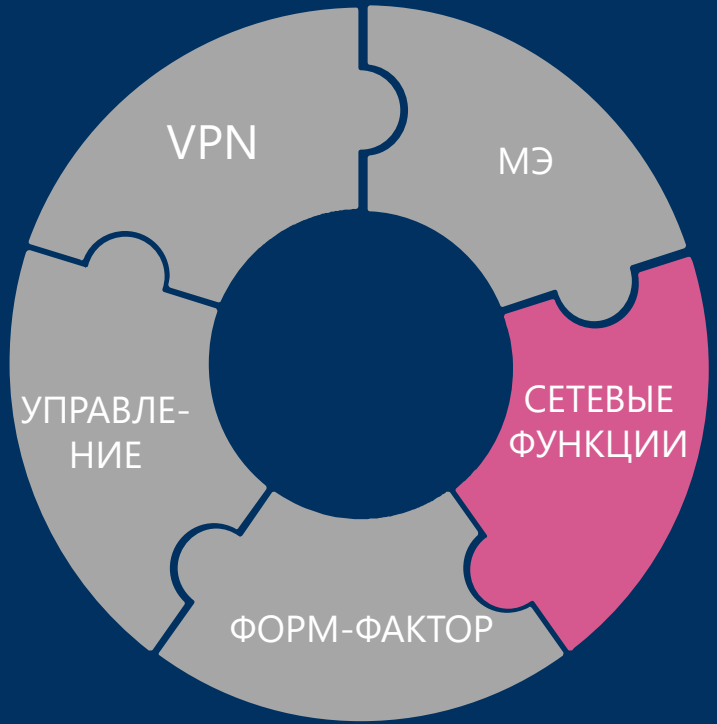


- Контроль пакетов на аномалии
- Возможность разрешения/запрета сообщений от конкретных адресов
- Возможность разрешения/запрета сообщений с конкретными командами

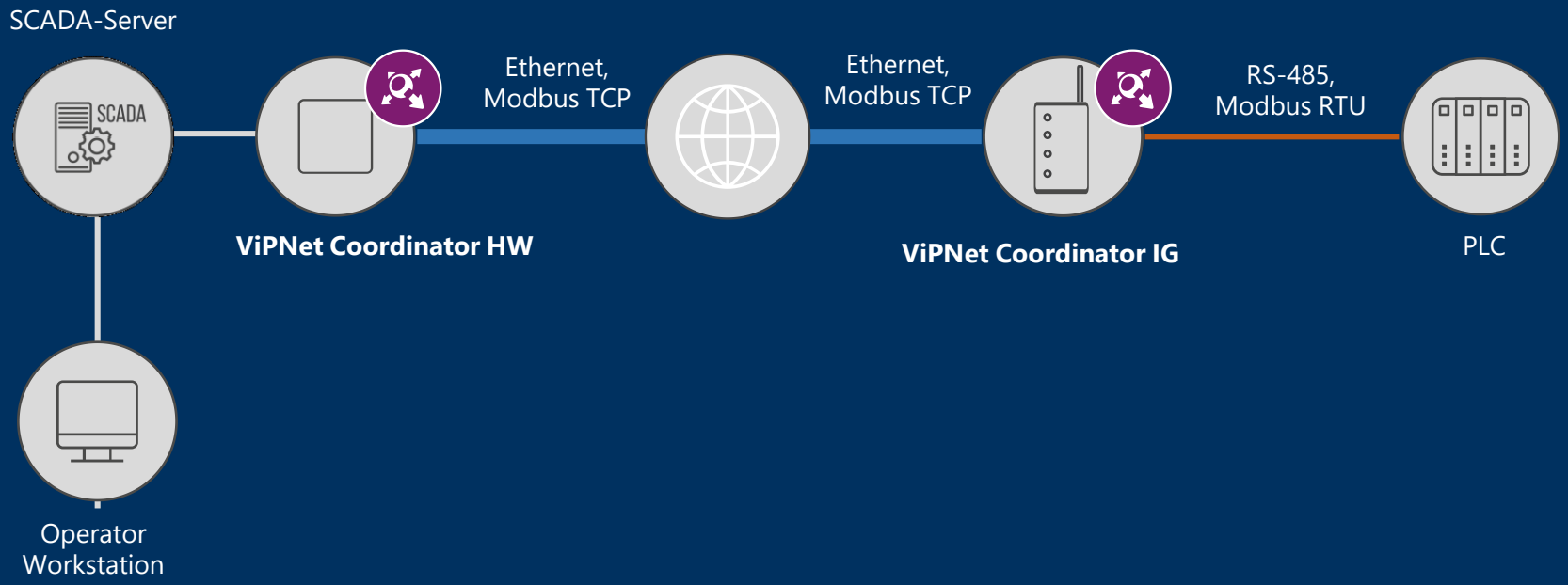
ViPNet Coordinator IG: характеристики

СЕТЕВЫЕ ФУНКЦИИ

- Статическая и динамическая маршрутизация
- DNS-сервер, DHCP-сервер, DHCP-relay
- VLAN, QoS, Etherchannel
- NTP-сервер
- Wi-Fi: IEEE 802.11 b/g,
- UMTS/HSPA, GSM/GPRS/EDGE
- Шлюза Modbus TCP/RTU
- GPIO



Шлюз Modbus TCP-RTU и RTU-TCP



GPIO

Входной сигнал

- Датчик вскрытия внешнего шкафа
- Переключение режима работы МЭ типа Д

- Сигнал с пользовательского устройства

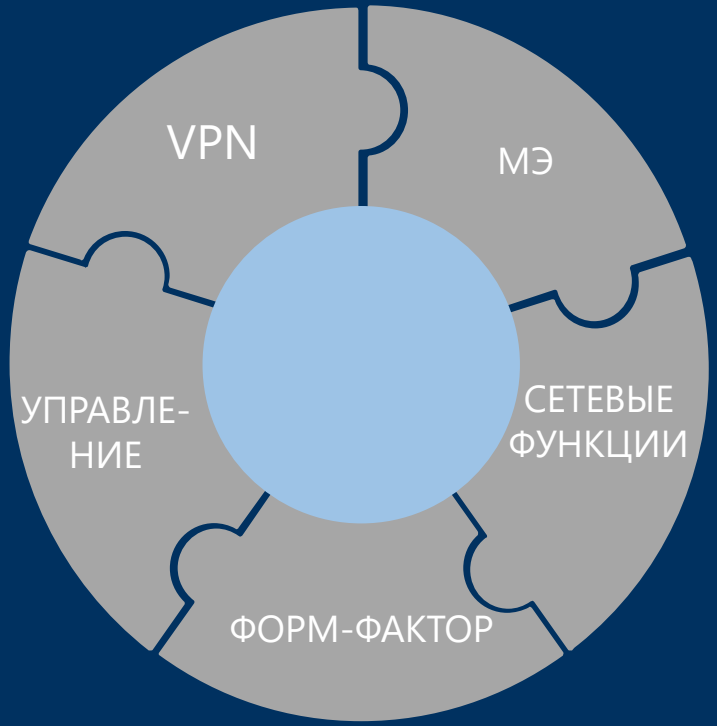
Выходной сигнал

- Кластер с шлюзом Modbus TCP-RTU
- Индикатор событий
  - Работа в регламентом обслуживании
  - Работа в штатном режиме
  - Работа в специальном режиме
  - Вскрыт шкаф
  - Сигнал с пользовательского устройства

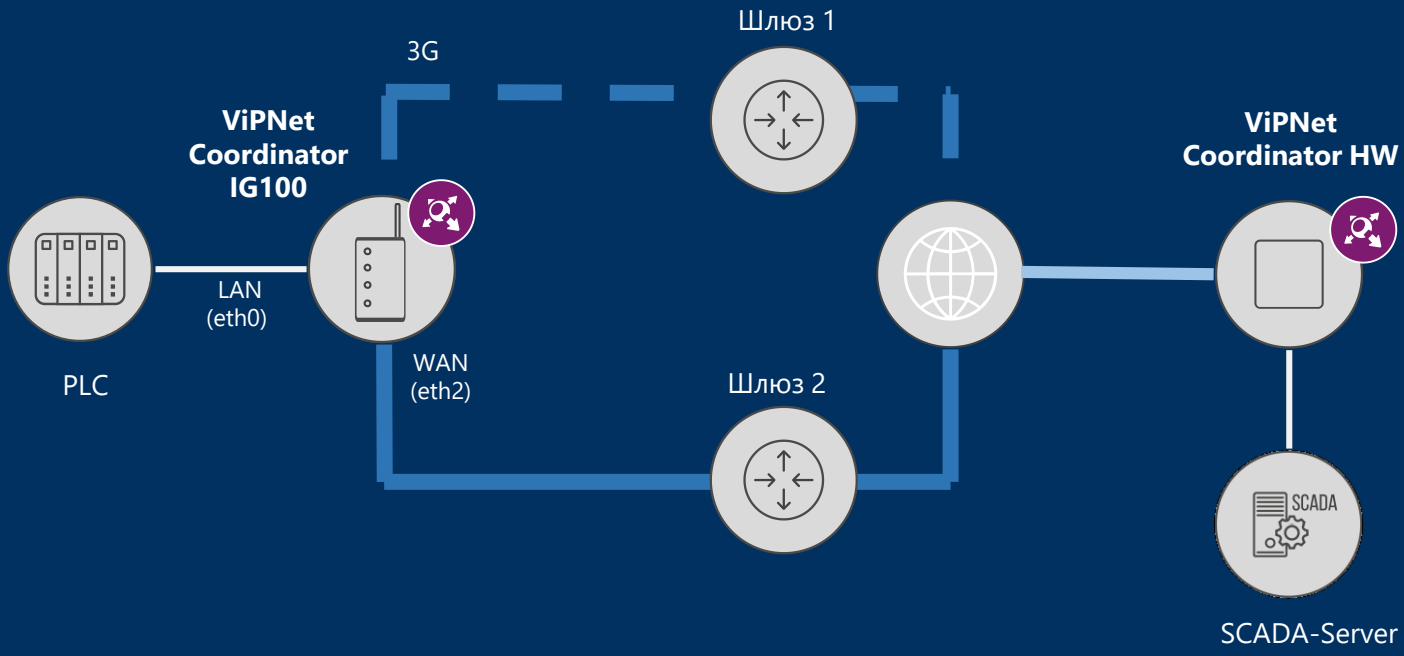
ViPNet Coordinator IG: характеристики

Надежность

- Кластер горячего резервирования (Failover)
- MultiWAN
- 24/7/235 режим работы
- 350 тыс. часов наработки на отказ

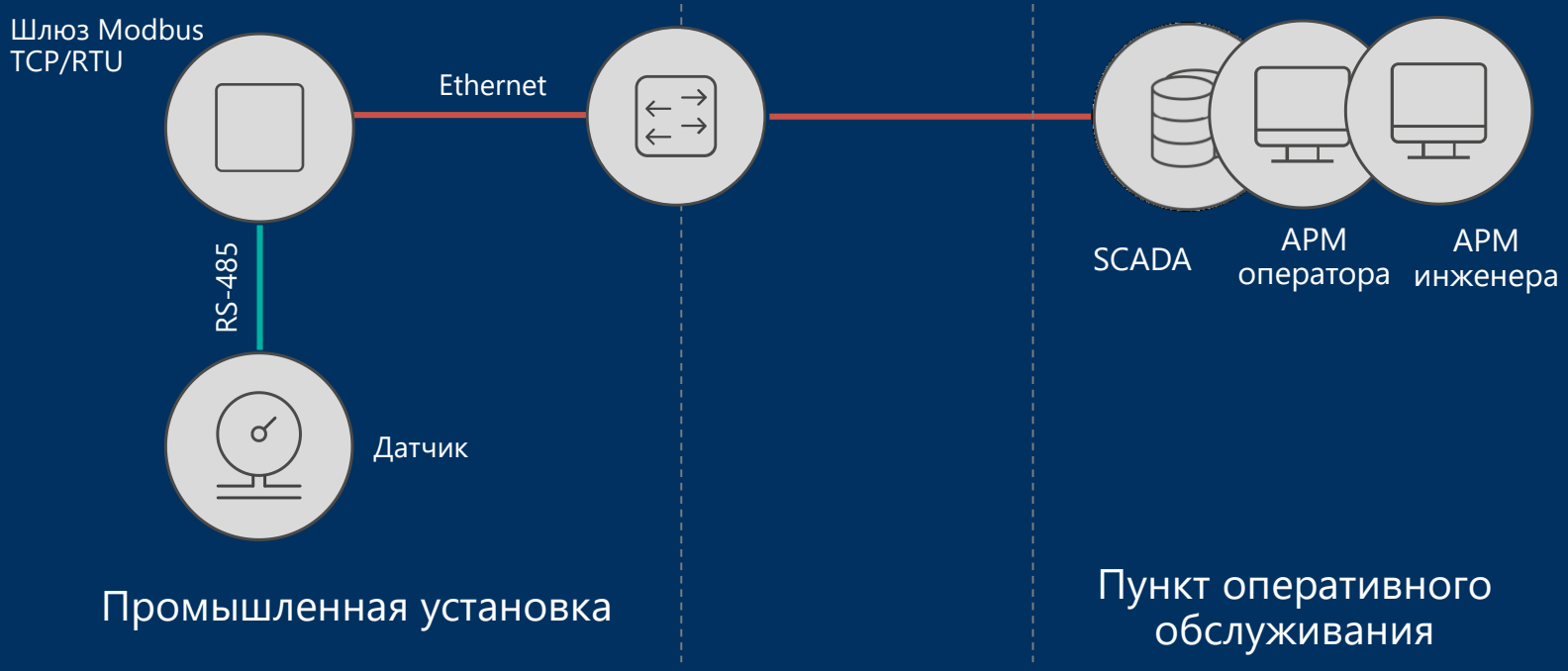


MultiWAN: резервирование каналов



Практика

Система мониторинга климатических параметров



Многофункциональный датчик

Модель: Датчик температуры и влажности EnergoM-3001-T-H

Интерфейс: RS-485

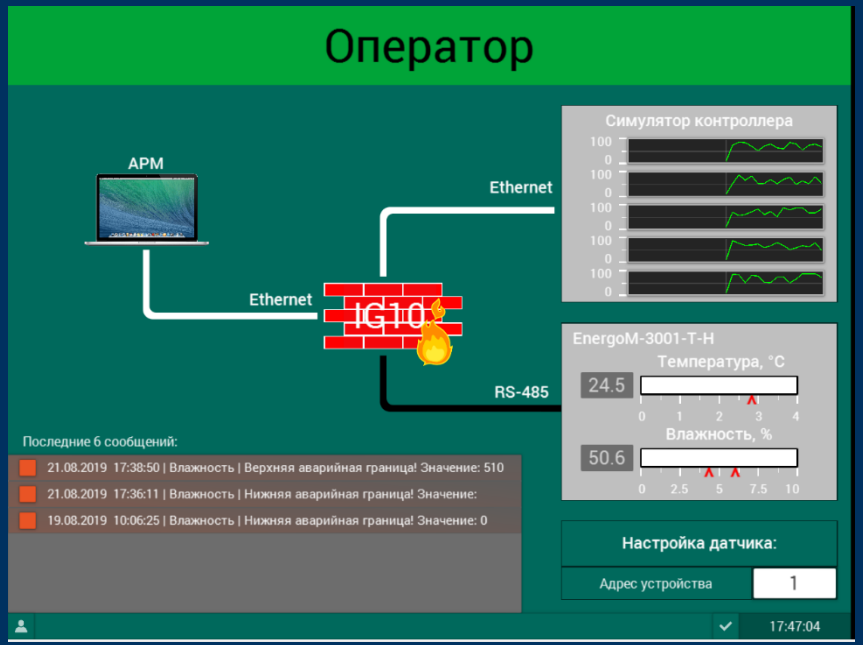
Протокол: Modbus RTU

Технические характеристики EnergoM-3001-T-H

ТЕХНО 2020 infotecs ФЕСТ

Register address

Register	Configuration address	Content	Operating
0000H	4001	Humidity (unit:0,1%)	Read only
0001H	4002	Temperature (unit: 0,1 0C)	Read only
0100H	40101	Device address (0-252)	Read and Write
0101H	40102	Baud rate (2400/4800/9600)	Read and Write
1000H	400001	Temperature T1(unit: 0,1 0C)	Read only
1001H	400002	Temperature T2(unit: 0,1 0C)	Read only
1010H	400003	Temperature T3(unit: 0,1 0C)	Read only
1100H	400004	Temperature T2(unit: 0,1 0C)	Read only



SCADA

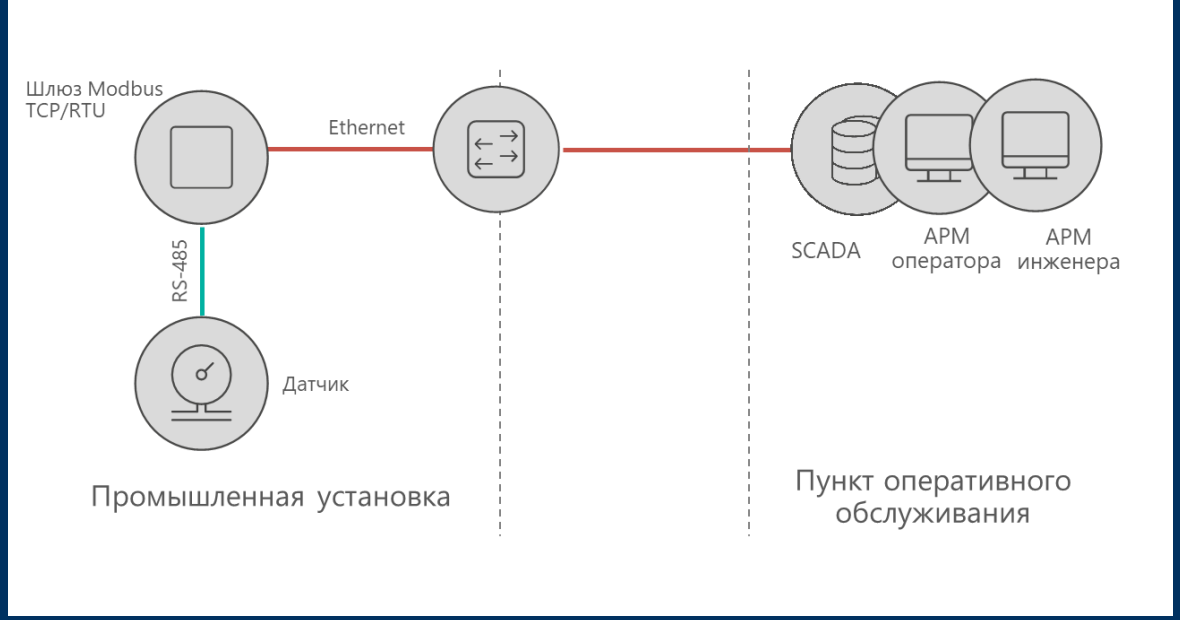
Пакет: Simple-scada

Системные требования:

ОС - Windows XP/7/8/10 x86 или x64, Windows Embedded Standard 7 и выше, Windows Server 2008 R2 и выше

Процессор — Intel Atom D2550 и выше;

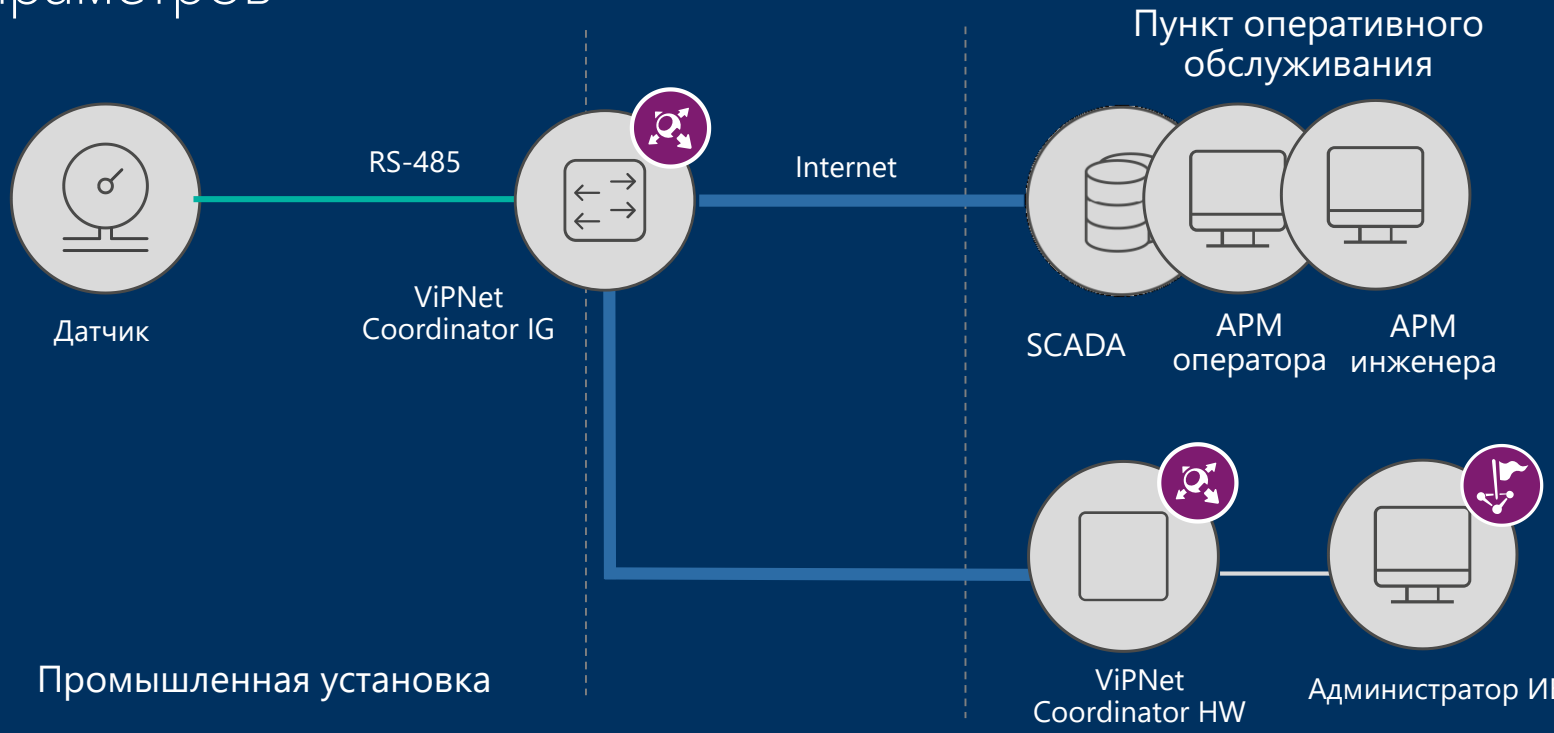
Видеокарта — Intel GMA 3650 и выше;



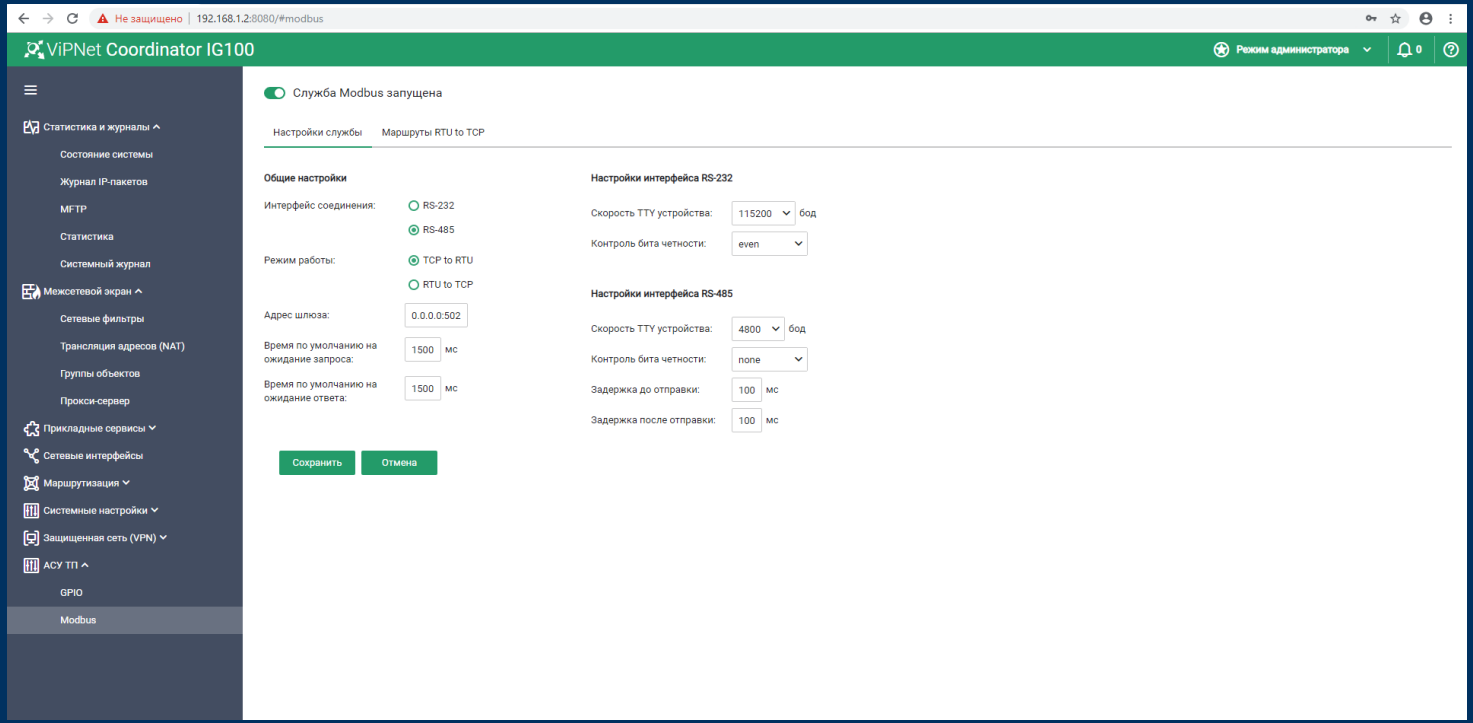
Система с точки зрения модели угроз

- Подмена значений температуры и влажности (подмена ответа на запрос к датчику)
- Несанкционированное изменение конфигурации датчика
- Физический доступ к датчику и конвертеру

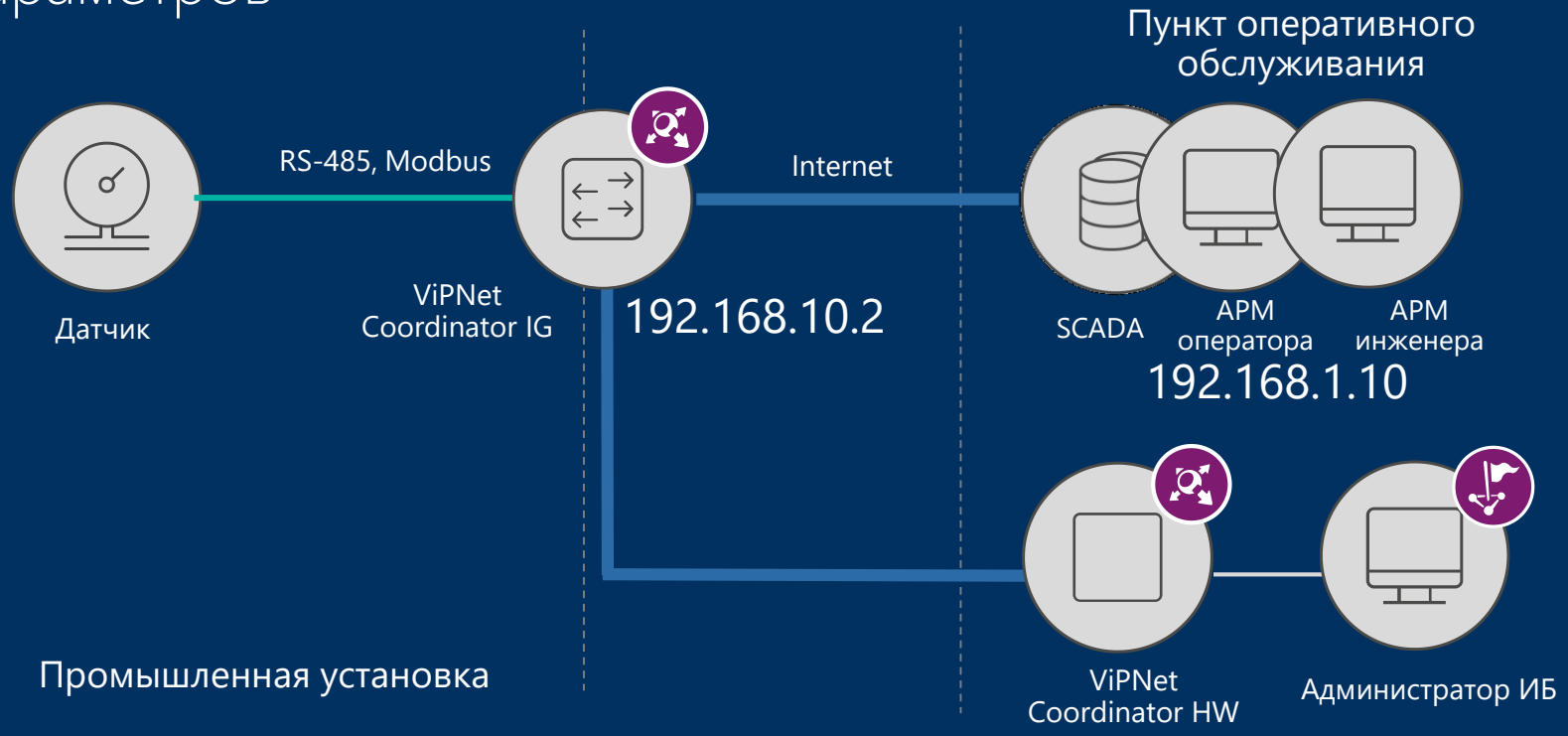
Система мониторинга климатических параметров



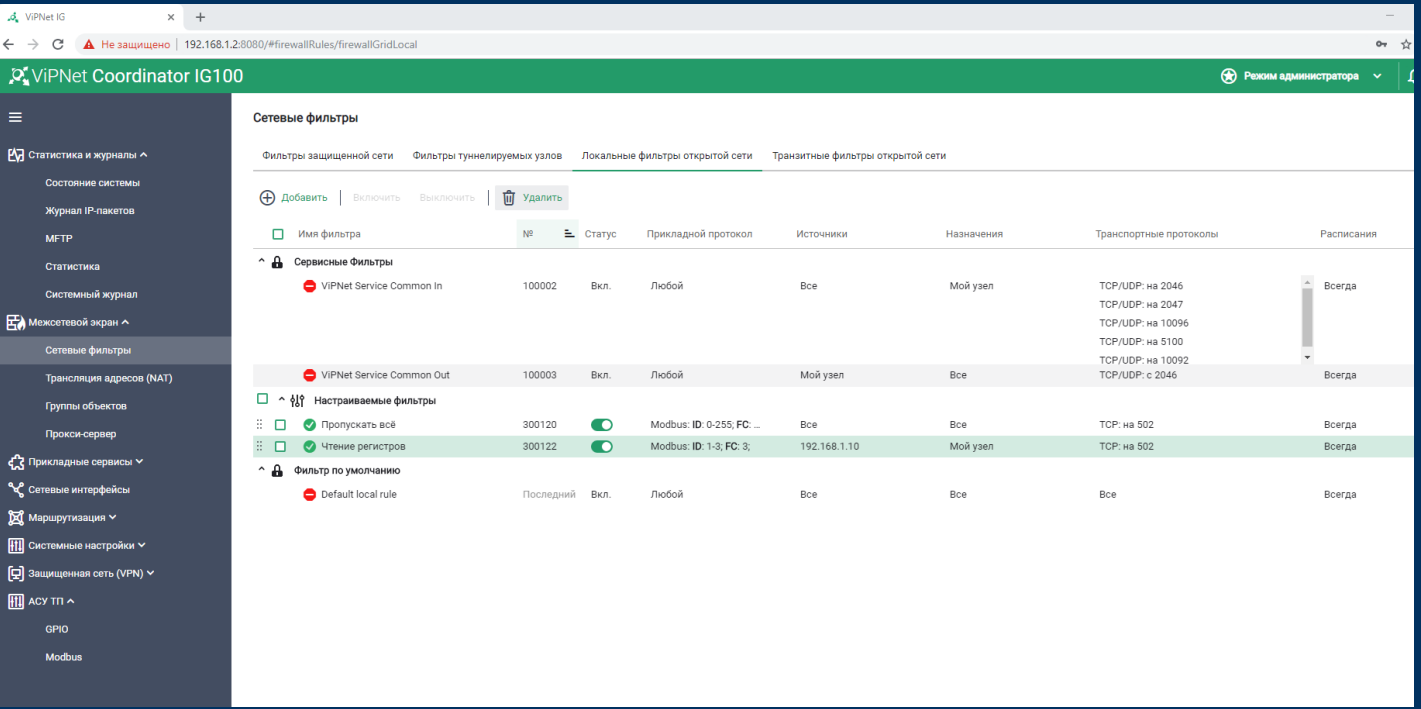
Шлюз Modbus TCP/RTU



Система мониторинга климатических параметров

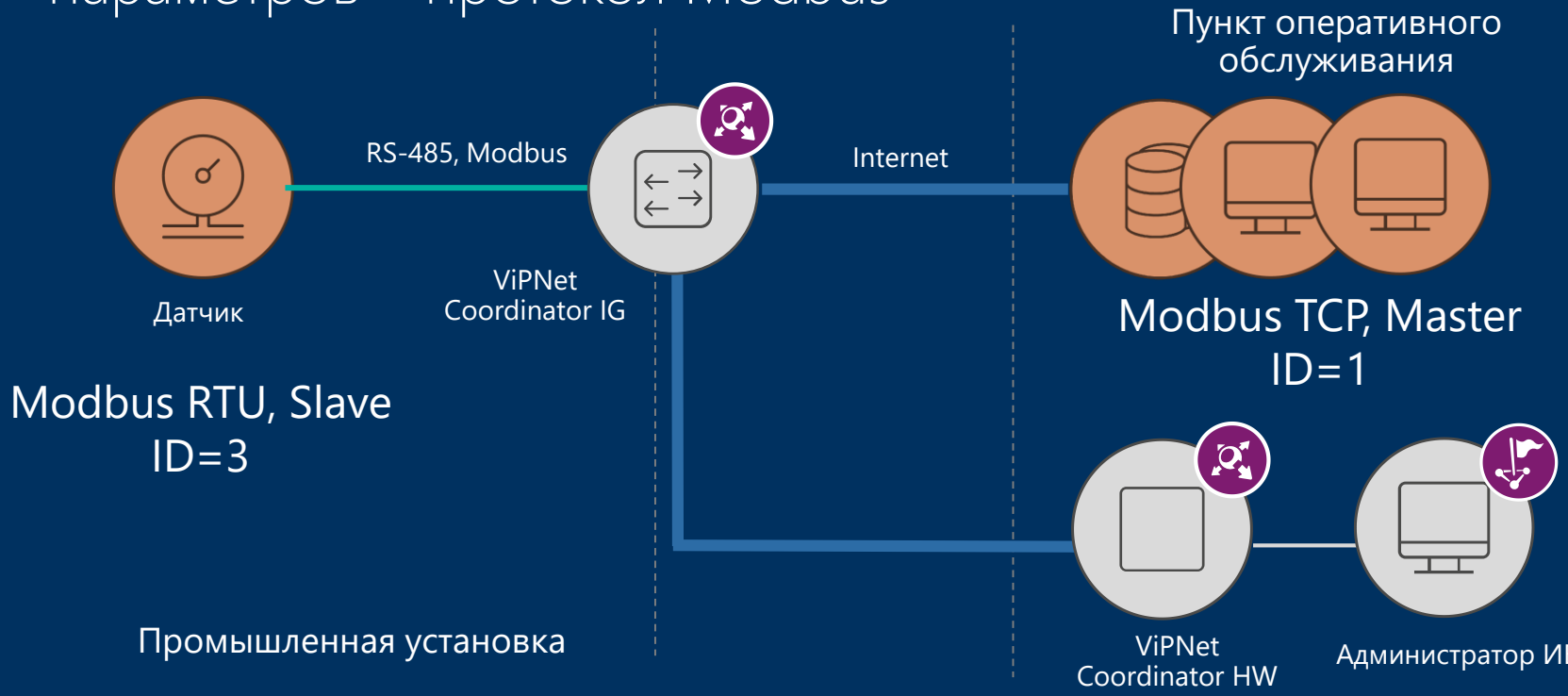


Классический подход с МЭ: Разрешающие правила для устройств в сети

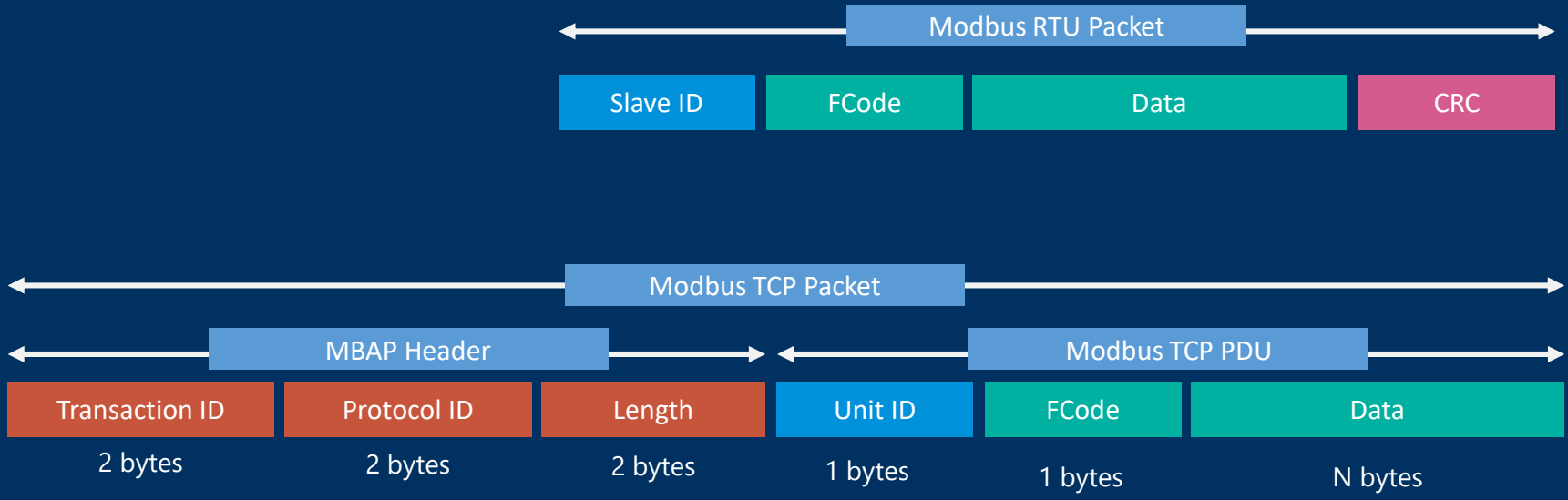


- Разрешаем трафик только с устройства с IP 192.168.1.10
- Разрешаем трафик с АРМ Администратора безопасности

Система мониторинга климатических параметров – протокол Modbus



Фильтрация по протоколам прикладного уровня на уровне полей протокола

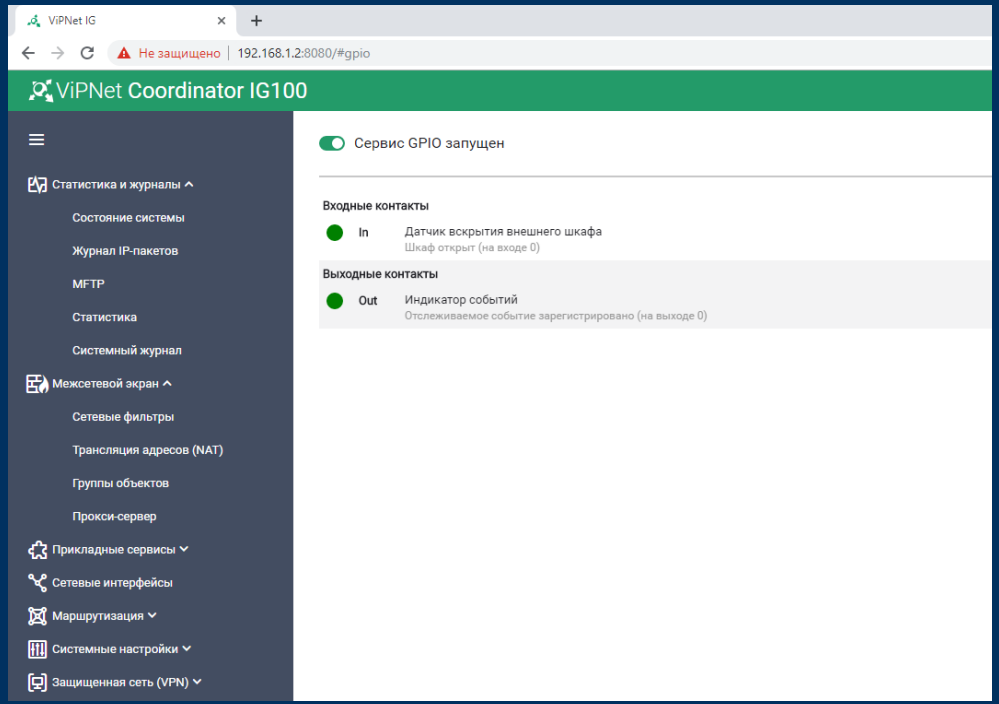


Сужение поверхности для атаки – Настройка межсетевого экрана (DPI)

Имя фильтра	Статус	Действие	Транспортные протоколы	Прикладные протоколы	Источники	Назначения	Расписани
Фильтры политик безопасности							
ViPNet Service Common In		Блокирует	TCP/UDP: на 2046, TCP/UDP: на 2047, TCP/UDP: на 10096, TCP/UDP: на 5100, TCP/UDP: на 10092	Любые	Все	Мой узел	Всегда
ViPNet Service Common Out		Блокирует	TCP/UDP: с 2046	Любые	Мой узел	Все	Всегда
Фильтры политик безопасности из Policy Manager							
Общее правило ОС		Разрешает	UDP: с 67-68 на 67-68, UDP: с 138 на 138	Любые	Все	Все	Всегда
Широковещательные фильтры<Все IP-адреса>		Разрешает	UDP: с 67-68 на 67-68, UDP: с 137 на 137, UDP: с 138 на 138	Любые	Все	Широковещательные адреса	Всегда
Настраиваемые фильтры							
Оператор может только читать регистры		Разрешает	TCP: на 502	Modbus: **ID**: 1-3; **FC**: 3;	192.168.1.10	Мой узел	Всегда
Все остальные не могут читать\записывать регистры		Блокирует	TCP: на 502	Modbus: **ID**: 0-255; **FC**: 1-127, 129-255;	Все	Мой узел	Всегда
Фильтр		Разрешает	Все	Любые	192.168.1.10	Мой узел	Всегда
Фильтры по умолчанию							
Default rule		Блокирует	Все	Любые	Все	Все	Всегда

Разрешаем действия только тем устройствам, что работают в сети – с ID 1-3

Разрешаем устройствам только те команды, которые они выполняют - чтение регистров Modbus (команда 3) для устройства с ID=1 и чтение/запись для ID=3



Про физическую безопасность - наблюдение за контролируемым периметром:

Установка датчика вскрытия шкафа

Настройка GPIO для отслеживания вскрытия шкафа

ТЕХНО 2020 infotecs Фест

Спасибо за внимание!