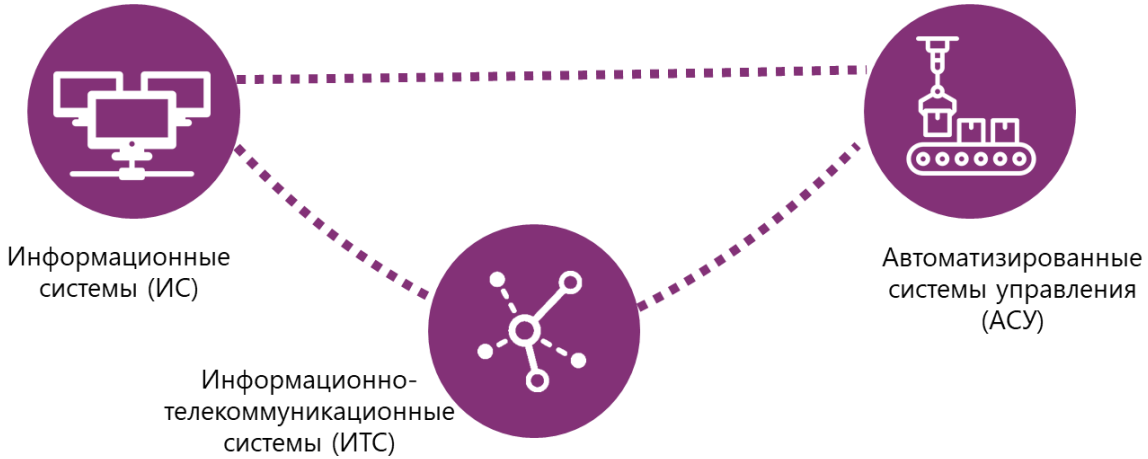

ТЕХНО 2019 infotecs ФЕСТ
ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ
12 09 2019
Защита КИИ.
Сетевые средства
информационной
безопасности для АСУ

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.)

Какие объекты АСУ защищать?

ТЕХНО infotecs ФЕСТ 2019

Информация о параметрах и объектах процесса АСУ

Входная и выходная информация, управляющая информация, контрольно-измерительная информация, иная критическая информация

Программные средства АСУ

Микропрограммное, общесистемное, прикладное программное обеспечение

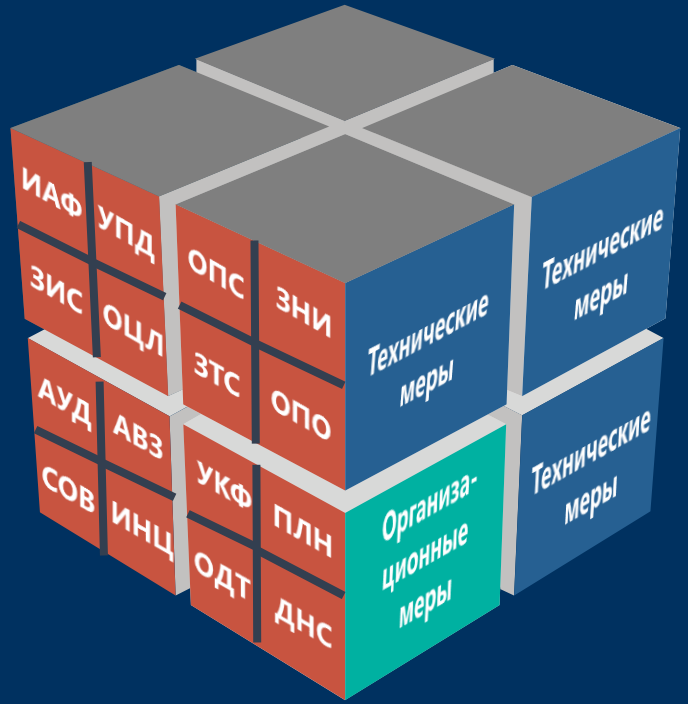
Программно-аппаратные средства АСУ

АРМ, промышленные серверы, телекоммуникационное оборудование, линии связи, ПЛК, производственное и технологическое оборудование, исполнительные устройства

Средства защиты информации

Архитектура и конфигурация АСУ

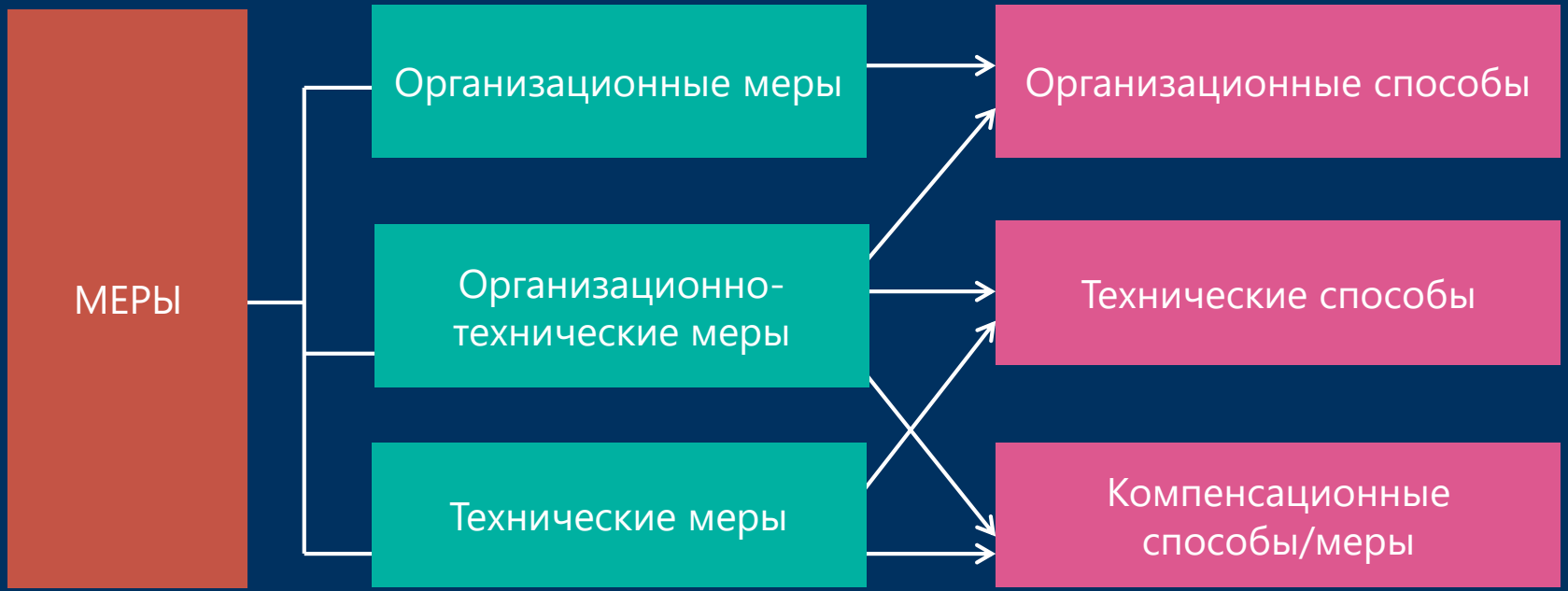
Состав мер по защите объектов КИИ согласно Приказу №239 ФСТЭК России



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

Меры защиты объектов КИИ



Технические меры защиты объектов КИИ

ТЕХНО 2019 infotecs ФЕСТ

Сетевые средства ИнфоТеКС для защиты АСУ КИИ

Продукты ИнфоТеКС для защиты АСУ КИИ

ViPNet Coordinator HW

ViPNet Client

ViPNet Coordinator IG

ViPNet Coordinator IG

ViPNet Coordinator IG

ViPNet Coordinator IG10

ViPNet Coordinator IG100

Сценарии

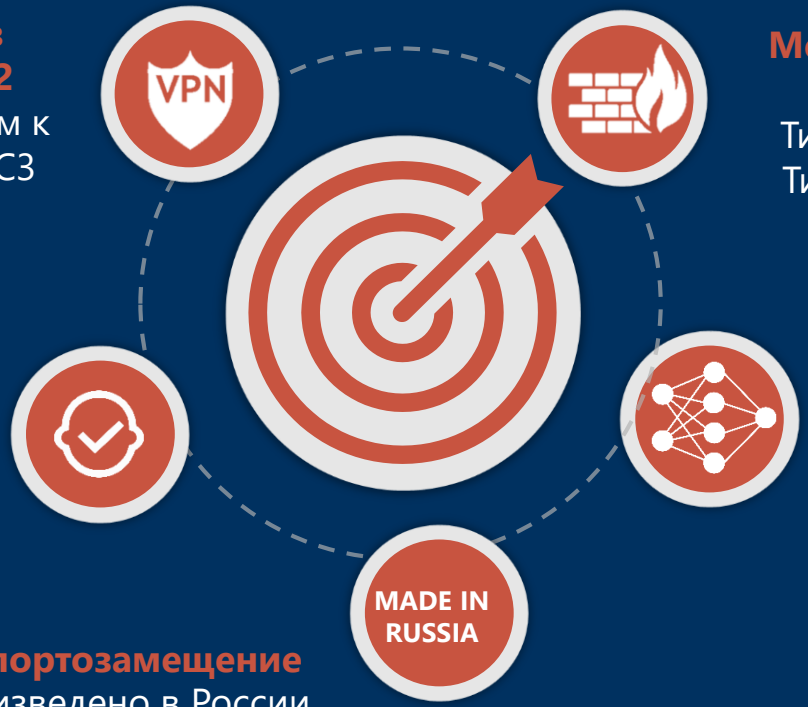
- защита периметра сети
- сегментирования сети и разграничения доступа к ее сегментам
- защиты проводных и беспроводных каналов связи сети
- организация ДМЗ
- управление сетевыми потоками
- сокрытие реальных адресов и архитектуры сети
- организации удаленного доступа для стационарных и мобильных пользователей,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

ViPNet Coordinator IG

ТЕХНО 2019 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

ViPNet Coordinator IG: характеристики

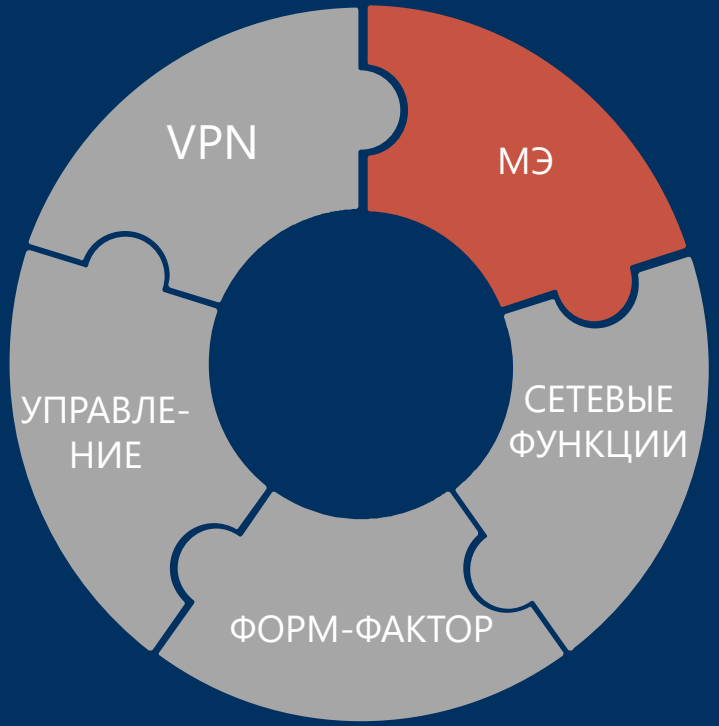
VPN

- 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

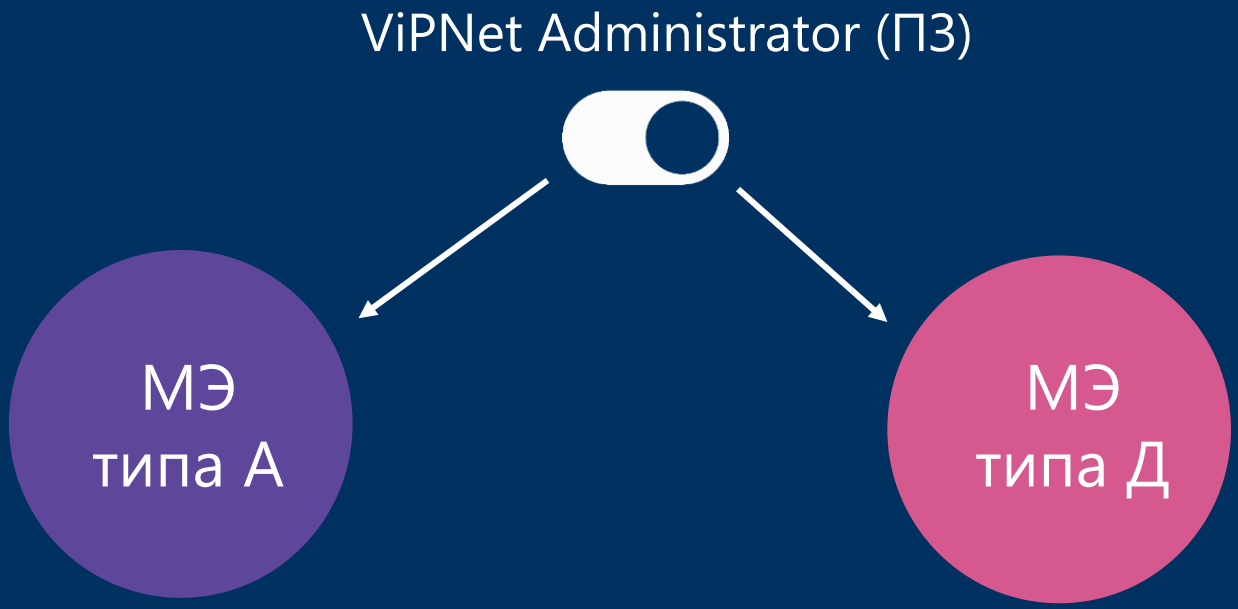
ViPNet Coordinator IG: характеристики

МЕЖСЕТЕВОЙ ЭКРАН

- NAT
- Антиспуффинг
- Фильтрация по IP источника и назначения, портам и типам протоколов
- Раздельной фильтрации для открытого IP-трафика и шифруемого IP-трафика
- Раздельные наборы фильтров для разных режимов
- Поддержка промышленных протоколов: EtherNet/IP, Modbus TCP, PROFINET, DNP, IEC 60870-104, MMS, OPC
- DPI для Modbus TCP/RTU

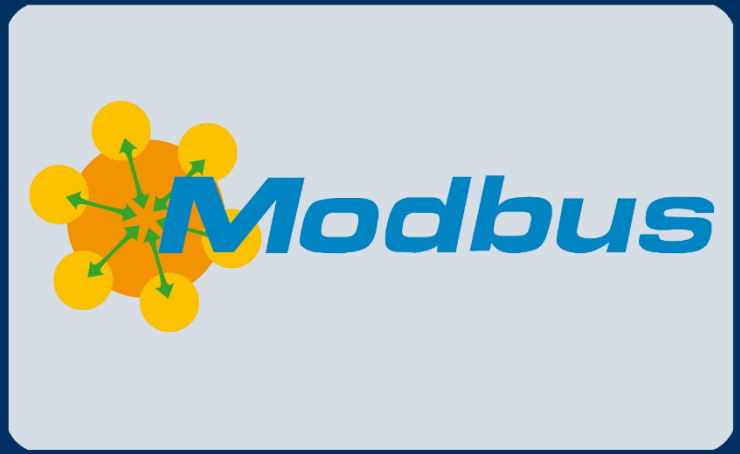


Межсетевой экран



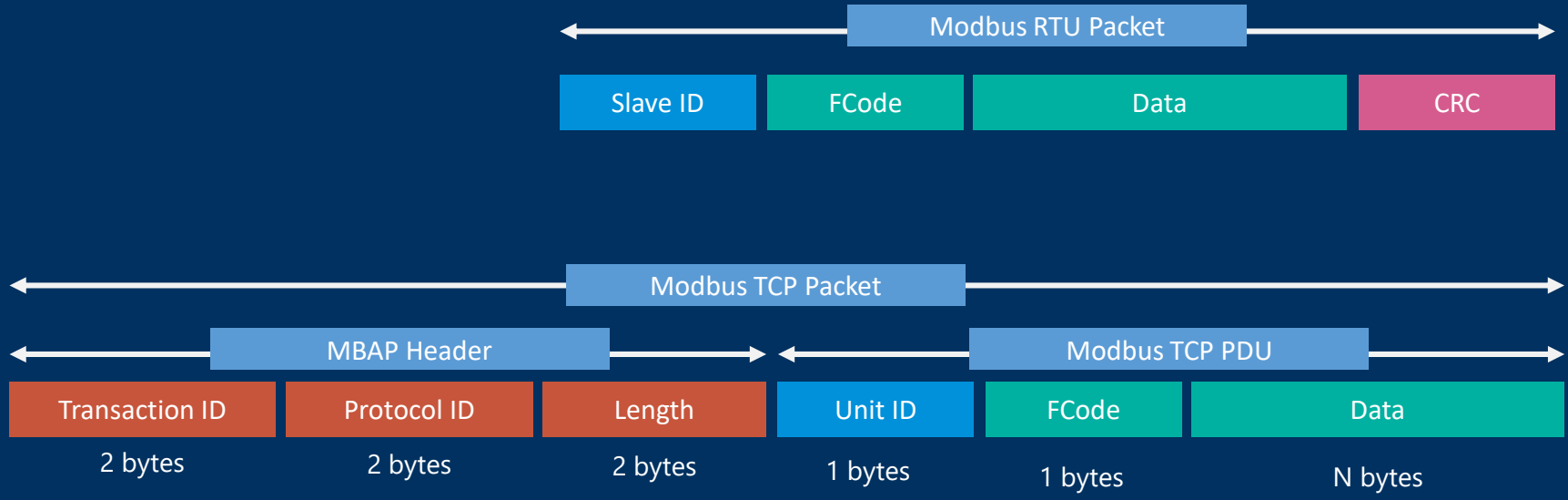
Правила МЭ для разных режимов работы ViPNet Coordinator IG

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

Фильтрация по протоколам прикладного уровня на уровне полей протокола

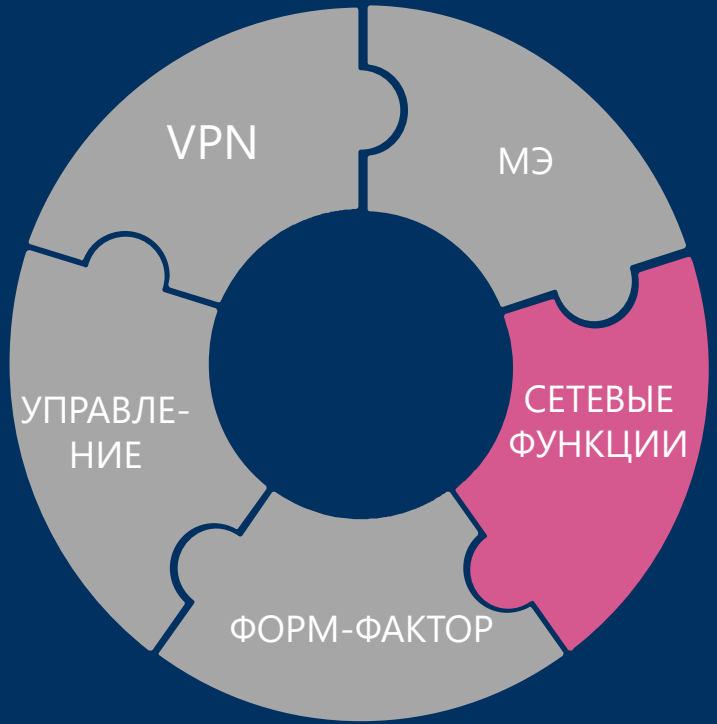


ViPNet Coordinator IG: характеристики

ТЕХНО 2019 infotecs ФЕСТ

СЕТЕВЫЕ ФУНКЦИИ

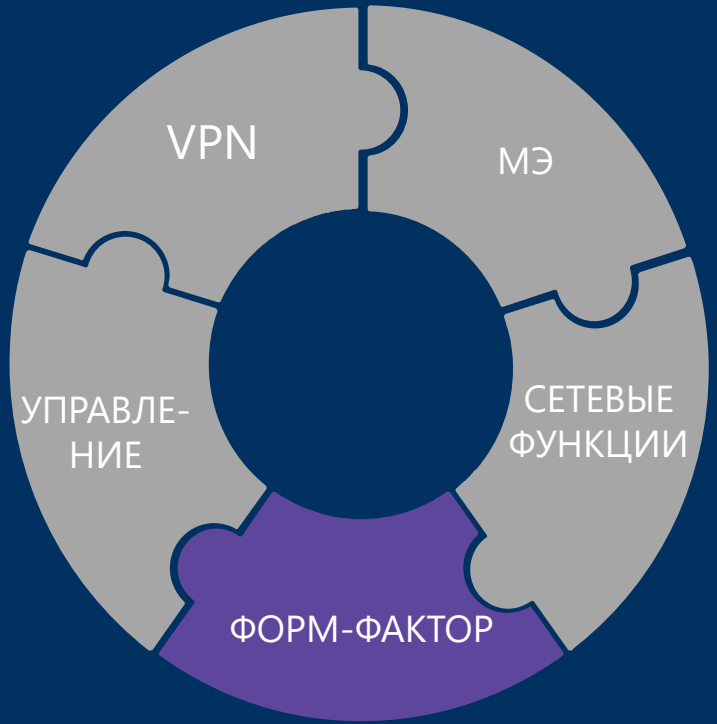
- Статическая и динамическая маршрутизация
- DNS-сервер, DHCP-сервер, DHCP-relay
- VLAN, QoS, Etherchannel
- NTP-сервер
- WAN: 1xRJ45 10/100
- LAN: 2xRJ45 10/100
- Wi-Fi: IEEE 802.11 b/g,
- UMTS/HSPA, GSM/GPRS/EDGE
- Шлюза Modbus TCP/RTU
- GPIO



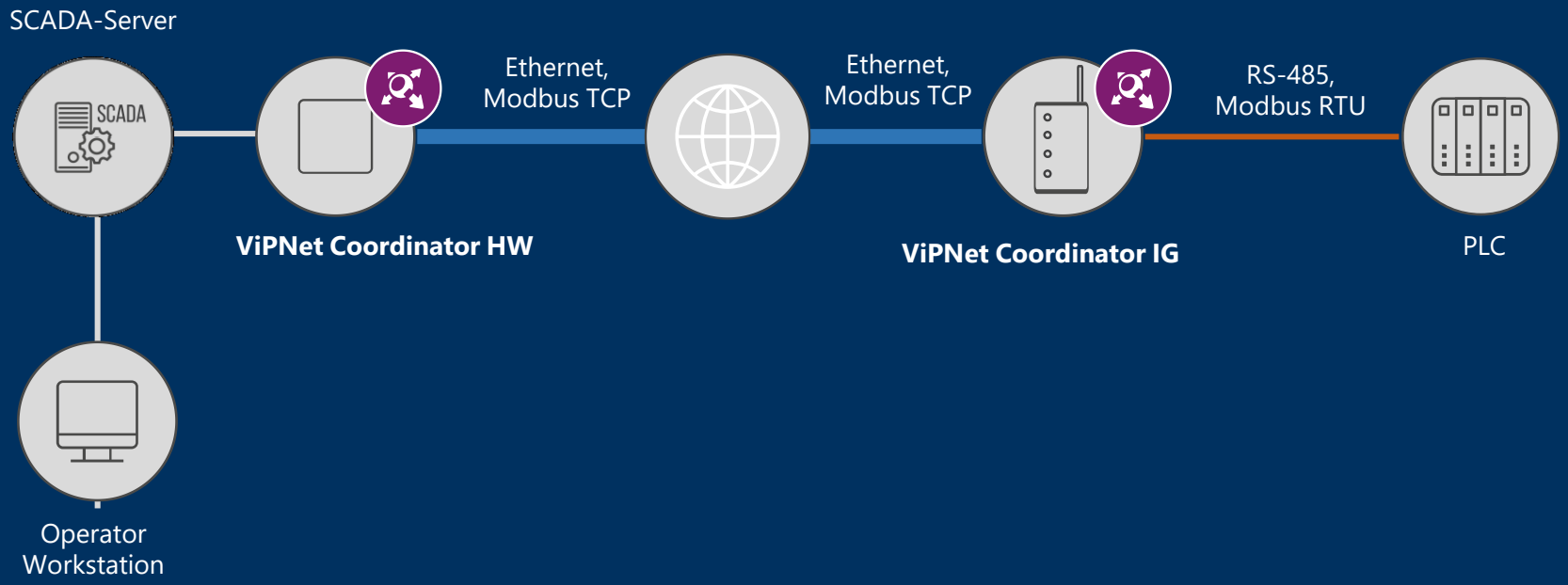
ViPNet Coordinator IG: характеристики

ФОРМ-ФАКТОР

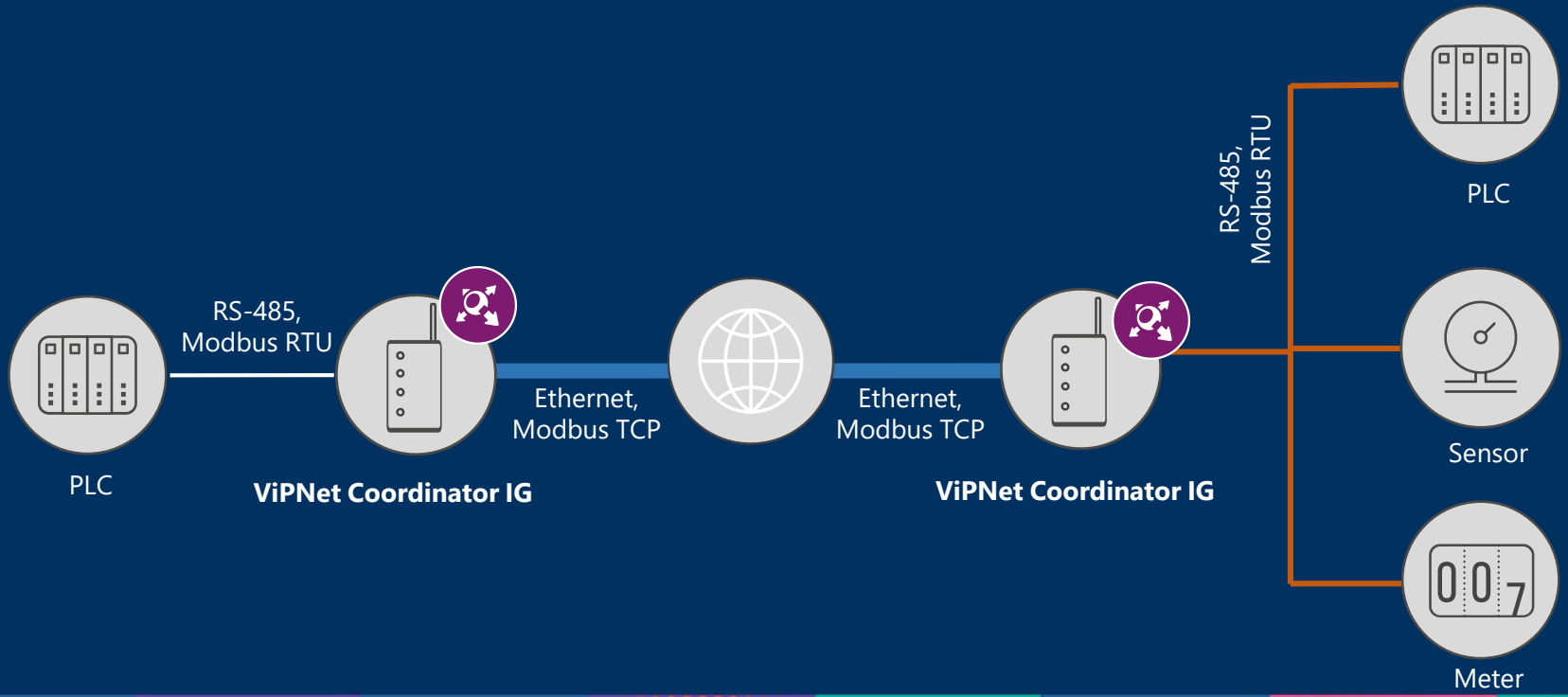
- ARM-платформа
- Безвентиляторный дизайн
- Рабочая температура: 20^0C(-40^0C) … $+60^0$C
- IP30 и бокс IP65 для кластера
- Напряжение питания: 12…24 В DC
- Крепление на din-рейку
- 50x120x120 мм, 0.6 кг
- ЭМС: ГОСТ 51318.22/CISPR22, ГОСТ CISPR 24



Шлюз Modbus TCP-RTU и RTU-TCP: пример №1



Шлюз Modbus TCP-RTU и RTU-TCP: пример №2



GPIO

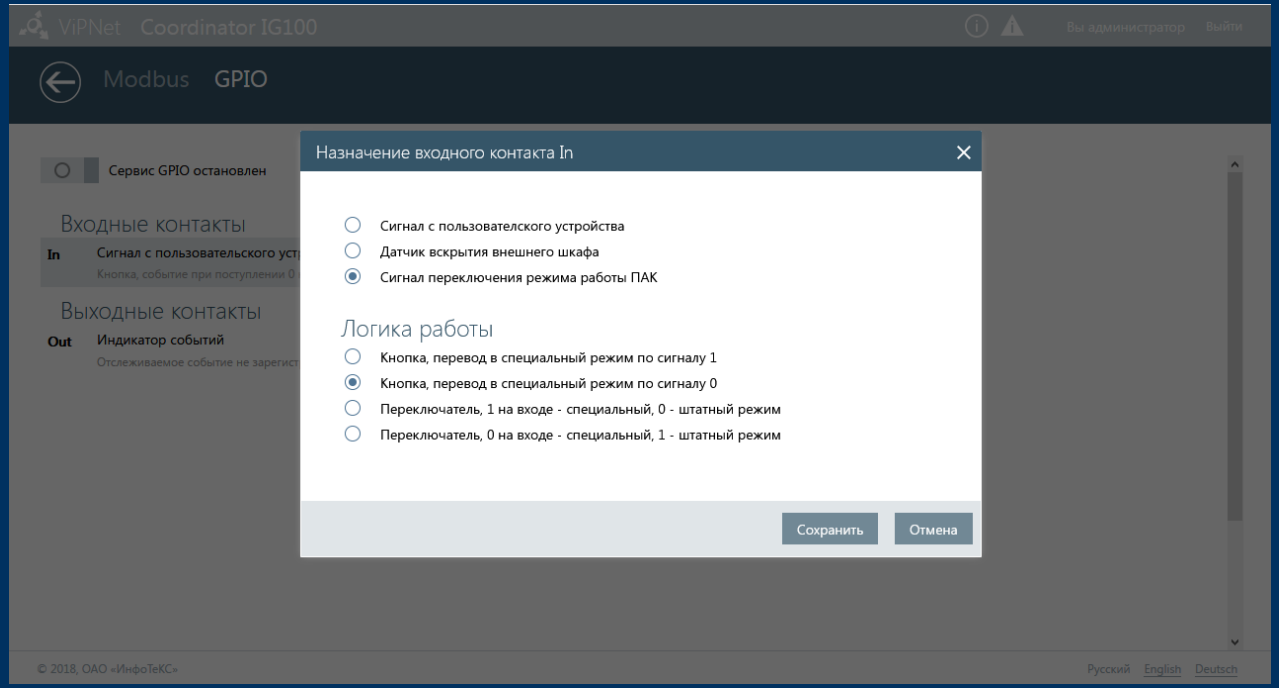
Входной сигнал

- 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

GPIO


ViPNet Coordinator IG100
Вы администратор
Выйти
Modbus GPIO
Сервис GPIO остановлен
Входные контакты
In
Сигнал с пользовательского уст
Кнопка, событие при поступлении 0
Выходные контакты
Out
Индикатор событий
Отслеживаемое событие не зарегист
Назначение входного контакта In
Сигнал с пользовательского устройства
Датчик вскрытия внешнего шкафа
Сигнал переключения режима работы ПАК
Логика работы
Кнопка, перевод в специальный режим по сигналу 1
Кнопка, перевод в специальный режим по сигналу 0
Переключатель, 1 на входе - специальный, 0 - штатный режим
Переключатель, 0 на входе - специальный, 1 - штатный режим
Сохранить
Отмена
© 2018, ОАО «ИнфоТеКС»
Русский English Deutsch

ViPNet Coordinator IG: характеристики

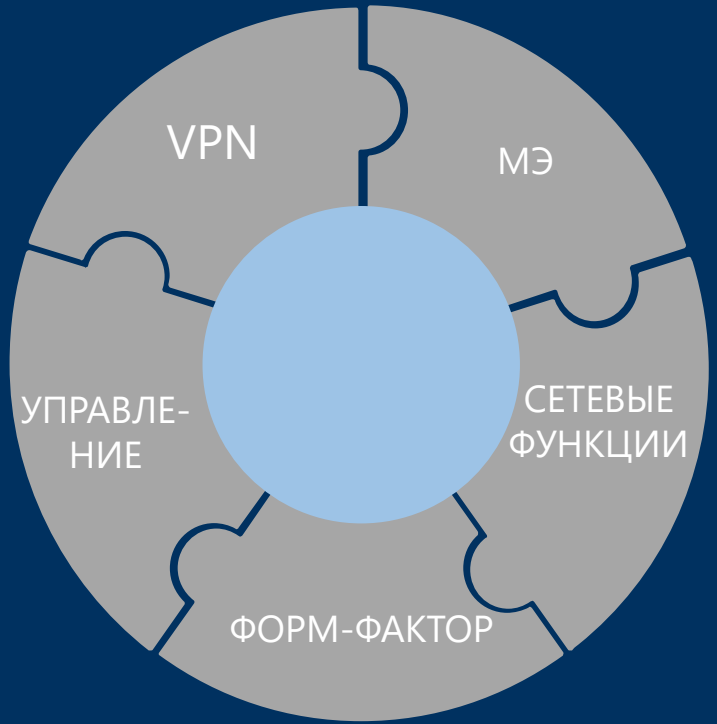
УПРАВЛЕНИЕ

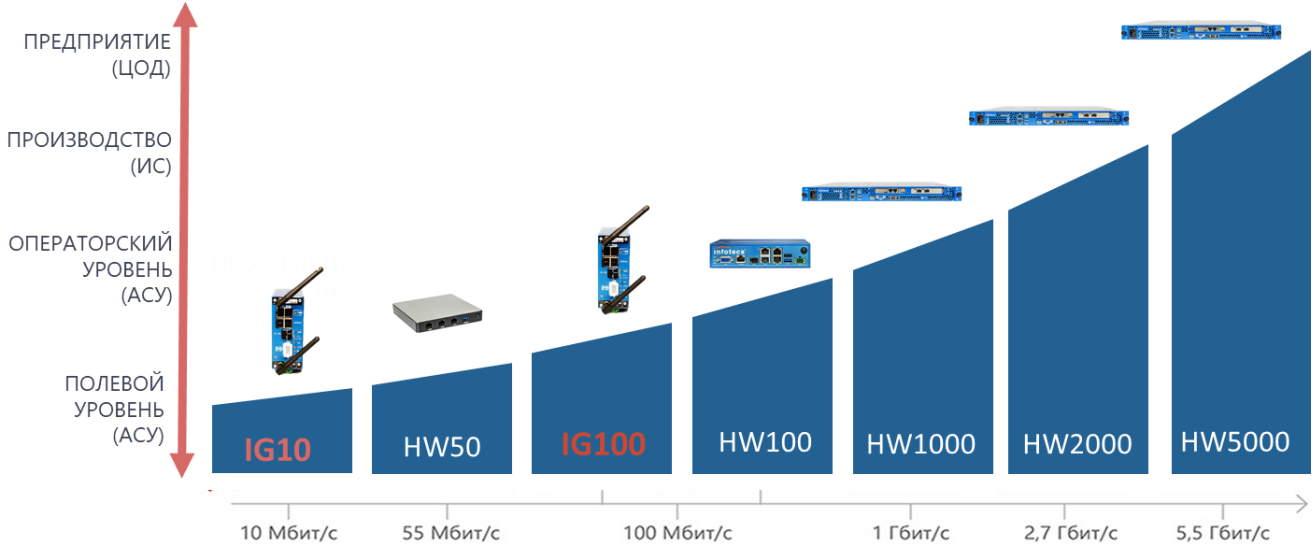
- Настройка: Web-интерфейс, консоль, SSH
- Обновления: локально, ViPNet Administrator
- Удаленное управление : ViPNet Administrator, ViPNet Policy Manager
- Удаленный мониторинг: ViPNet StateWatcher, SNMP, Syslog
- Event log: Firewall Event, System Security Event

ViPNet Coordinator IG: характеристики

Надежность

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





Непрерывная безопасность от ЦОД до контроллера

- Встречная работа
- Единое управление

Сертификация

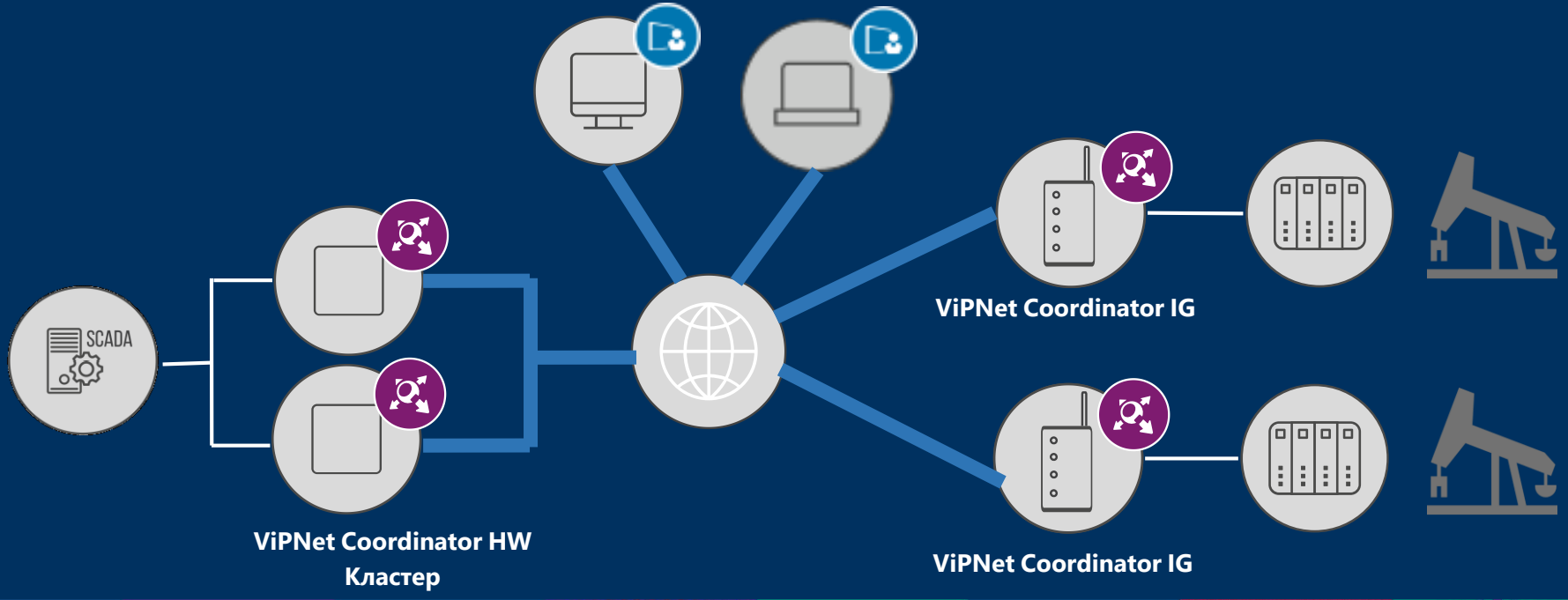
ViPNet Coordinator IG10

- Сертификат СКЗИ класса КС3
- Сертификат МЭ 4 класса защищенности

ViPNet Coordinator IG10 и ViPNet Coordinator IG100

- Отчетные материалы на СКЗИ класса КС3 и МЭ 4 класса защищенности отправлены регулятору
- Заключительная стадия подготовки отчетных материалов по МЭ типа А.4 и Д.4

Примеры защиты объектов КИИ: Защита системы управления нефтяными кустами



ТЕХНО 2019 infotecs Фест

Спасибо
за внимание!