Индустриальный шлюз безопасности: работа с промышленными протоколами

Андрей Иванов
Иван Герасименко

infotecs

ViPNet Coordinator IG

- Защищенная сеть ViPNet
- Wi-Fi-модуль
- GSM-модуль
- Межсетевой экран + DPI протоколов Modbus и IEC 104
- Шлюз Modbus RTU-TCP
- Коммутатор и маршрутизатор
- Отказоустойчивость
- Мониторинг состояния

Каналы передачи данных

Wi-Fi, GSM

Wi-Fi модуль:

- Клиент
- Точка доступа

GSM-модуль:

- LTE-модуль

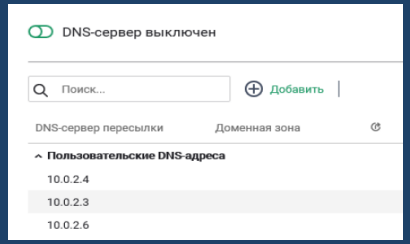
В комплекты модулей входят внешние антенны.

Возможно использование выносных антенн.

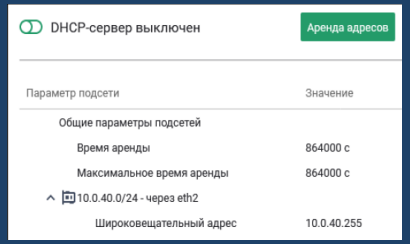
Внимание! Wi-Fi и GSM-модули устанавливается только на производстве!

Сетевые сервисы

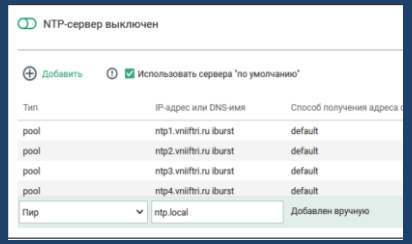
DNS (client/server)



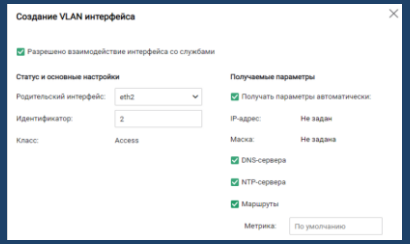
DHCP (server/relay)



NTP (client/server)

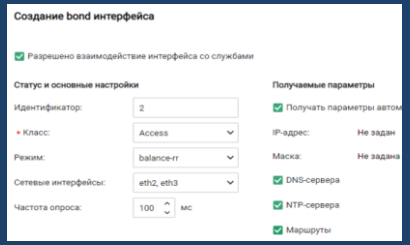


VLAN

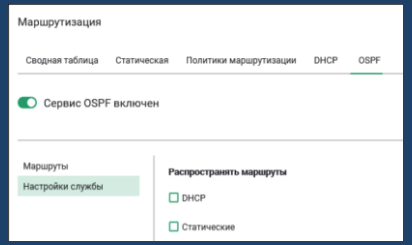


QoS

MultiWAN



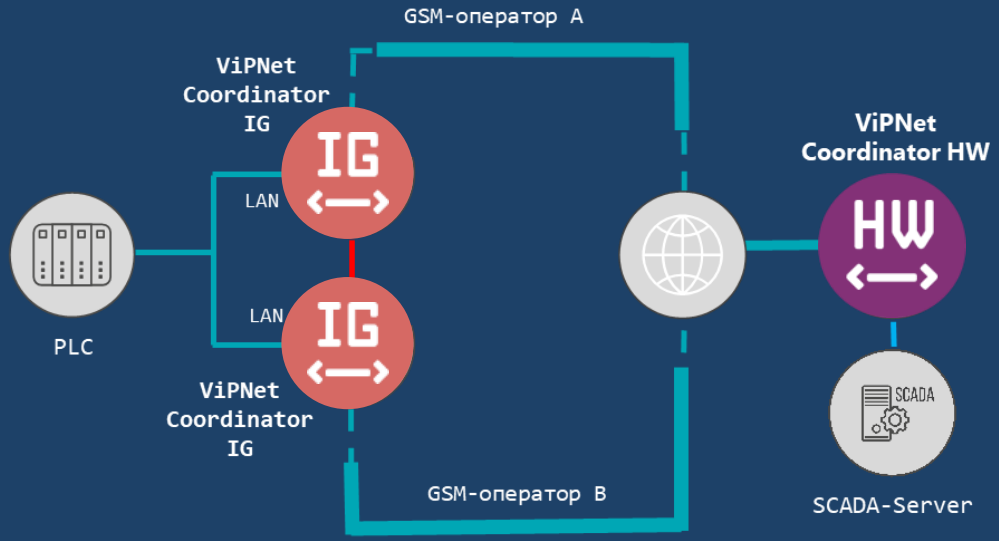
OSPF



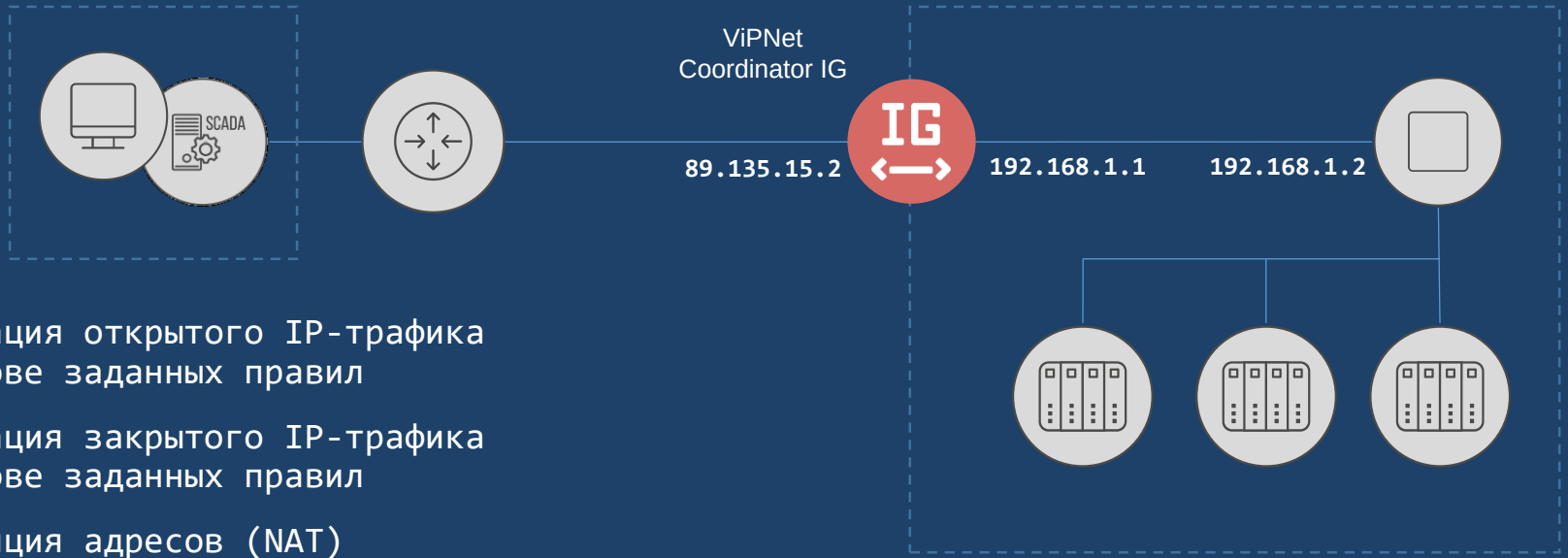
Cluster

Отказоустойчивость

- Защита от программных 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

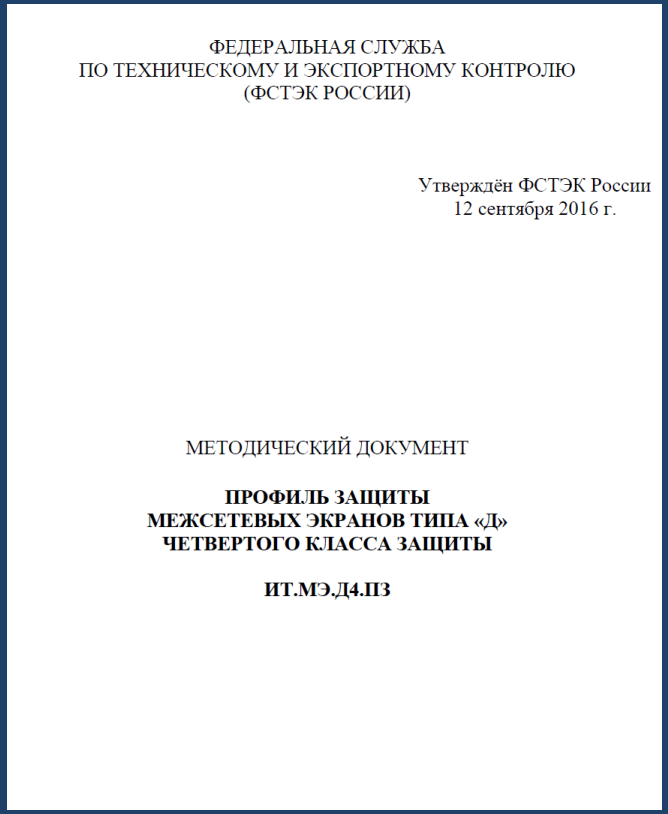


Межсетевой экран



- 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

ViPNet Coordinator IG: межсетевой экран типа «Д»



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утверждён ФСТЭК России
12 сентября 2016 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**ПРОФИЛЬ ЗАЩИТЫ
МЕЖСЕТЕВЫХ ЭКРАНОВ ТИПА «Д»
ЧЕТВЕРТОГО КЛАССА ЗАЩИТЫ**

ИТ.МЭ.Д4.ПЗ

МЭ уровня промышленной сети (тип «Д») – это МЭ, применяемый в автоматизированной системе управления технологическими или производственными процессами. МЭ типа «Д» может иметь программное или программно-техническое исполнение и должен обеспечивать контроль и фильтрацию промышленных протоколов передачи данных (Modbus, Profibus, CAN, HART, Industrial Ethernet и (или) иные протоколы).

МЭ типа «Д»: режимы работы

GPIO

General-Purpose Input/Output – интерфейс ввода/вывода общего назначения

Входной сигнал

- Датчик вскрытия шкафа
- Переключение в специальный режим работы (для типа «Д»)
- Сигнал с пользовательского устройства

Выходной сигнал

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

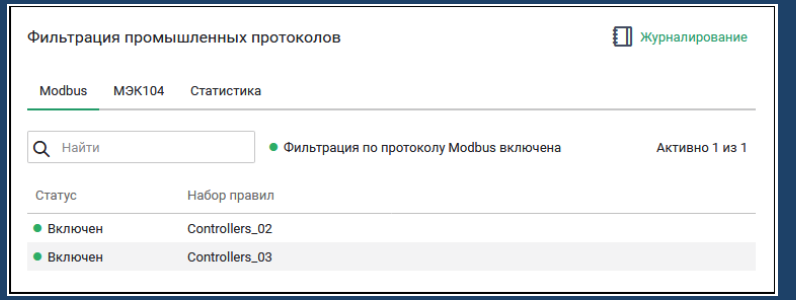
Фильтрация промышленных протоколов

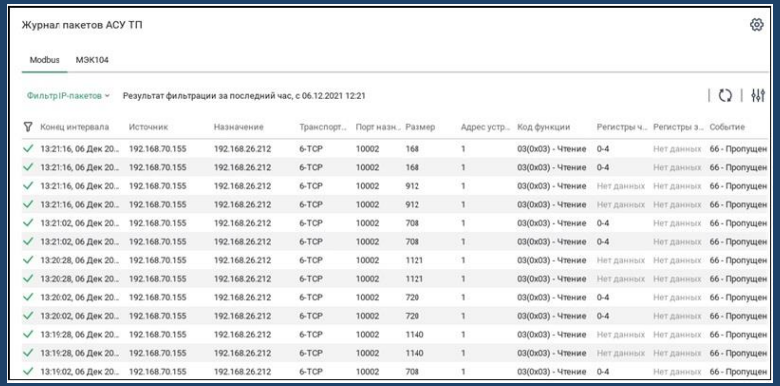
- Настройка межсетевого экрана
  - Настройка сетевых фильтров
  - Настройка фильтрации промышленных протоколов
    - Общие сведения о фильтрации промышленных протоколов
    - Основные принципы фильтрации промышленных протоколов
      - Принципы фильтрации протокола Modbus на прикладном уровне
      - Принципы фильтрации протокола МЭК 60870-5-104 на прикладном уровне
    - Создание и изменение наборов правил фильтрации промышленного протокола
    - Просмотр наборов правил промышленного протокола

Фильтрация промышленных протоколов

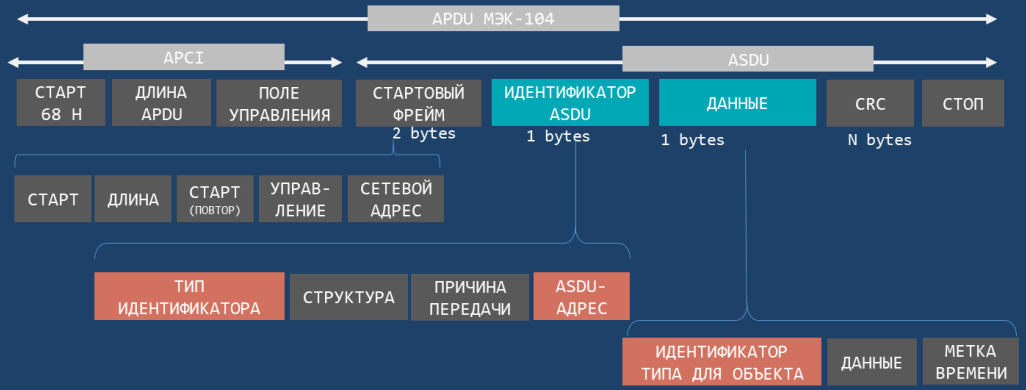
Версия 4.5.1:

- Фильтрация промышленных протоколов настраивается отдельно от сетевых фильтров
- Отдельный журнал пакетов промышленных протоколов
- Фильтрация на прикладном уровне протоколов Modbus и МЭК 60870-5-104
  - Правила транспортного уровня
  - Правила прикладного уровня





Протокол МЭК 60870-5-104



ГОСТ Р МЭК 60870-5-104-2004

Группа П77

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

УСТРОЙСТВА И СИСТЕМЫ ТЕЛЕМЕХАНИКИ

Часть 5. Протоколы передачи

Раздел 104. Доступ к сети для ГОСТ Р МЭК 870-5-101 с использованием стандартных транспортных профилей

Telecontrol equipment and systems. Part 5. Transmission protocols. Section 104. Network access for IEC 60870-5-101 using standard transport profiles

ОКС 33.200
ОКП 42 3200

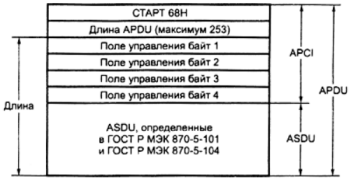


Рисунок 4 - APDU определяемого обобщающего телемеханического стандарта

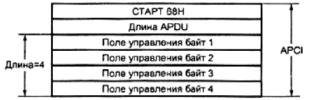
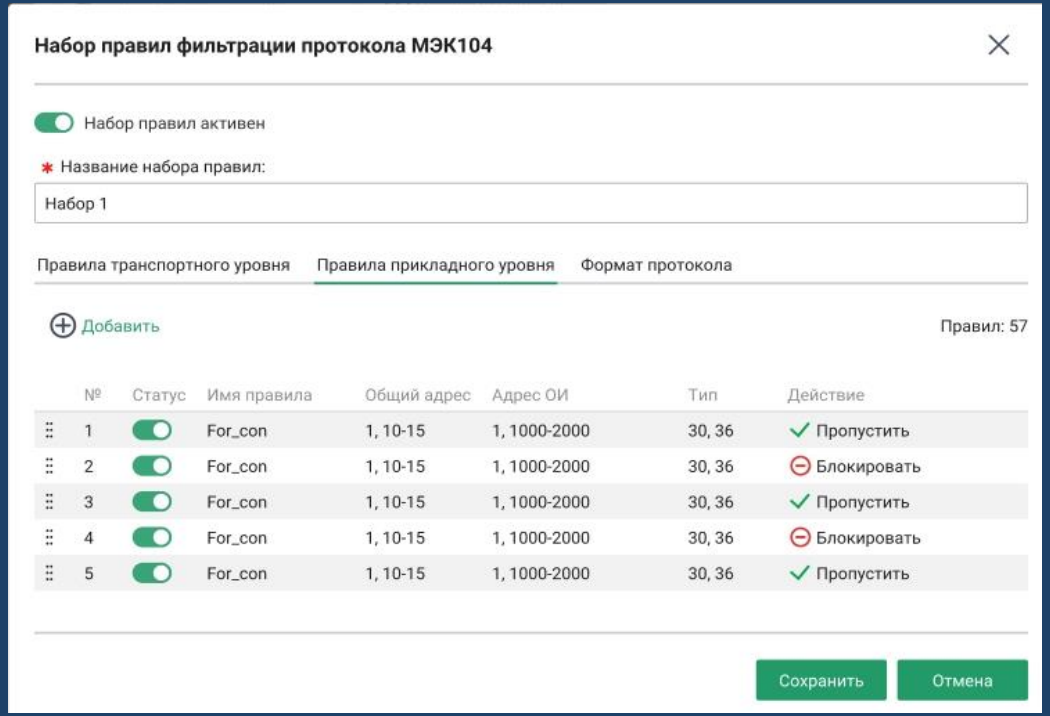


Рисунок 5 - APCI определяемого обобщающего телемеханического стандарта

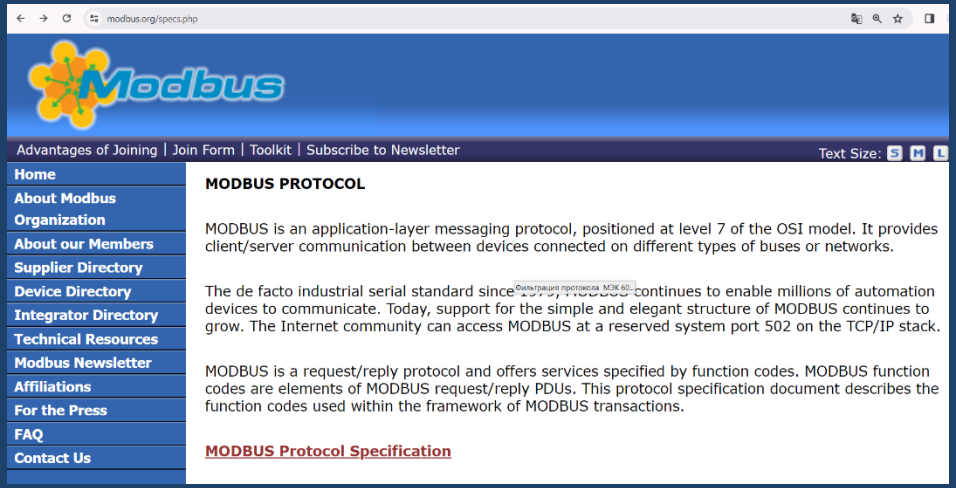
Фильтрация протокола МЭК 60870-5-104 (4.5.1)

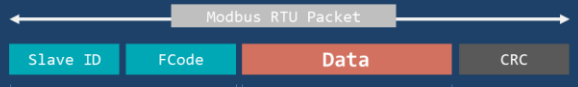
- Номер порта
- Общий адрес (ASDU)
- Адрес объекта информации (Information Object Address)
- Идентификатор типа (Type Identifier)

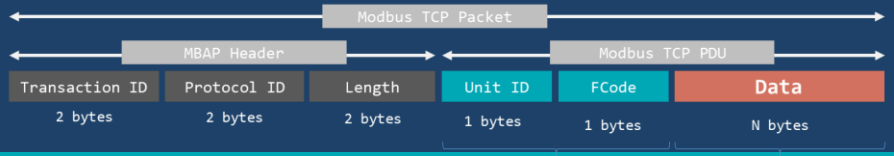


Протокол Modbus

https://modbus.org/specs.php







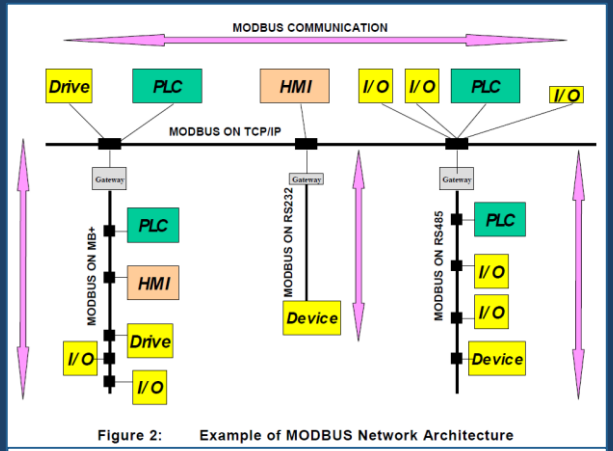


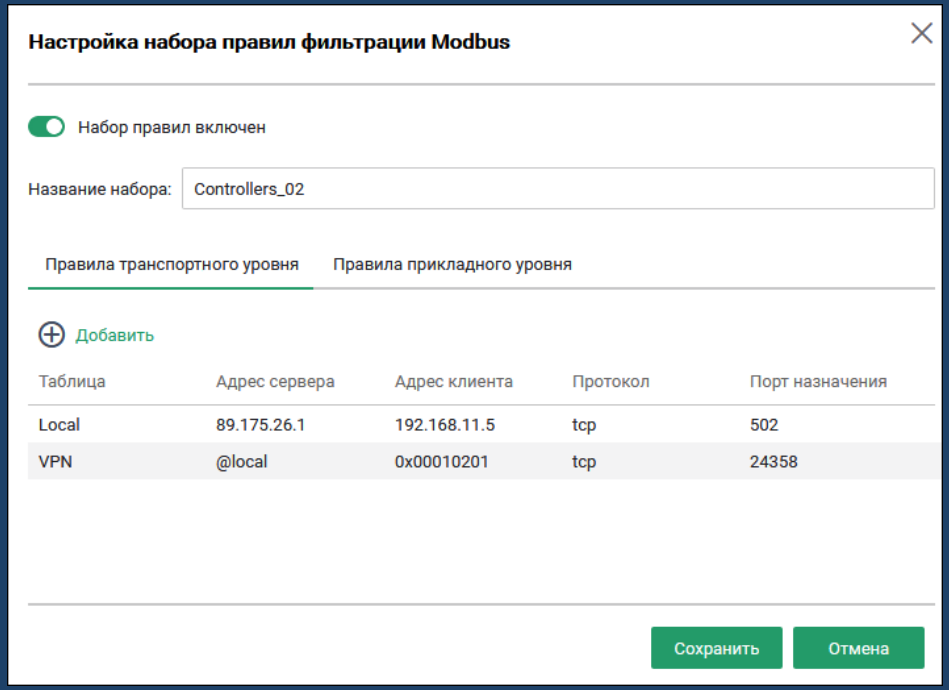
Figure 2: Example of MODBUS Network Architecture

5.1 Public Function Code Definition

				Function Codes code	Sub code	(hex)	Section
Data Access	Bit access	Physical Discrete Inputs	Read Discrete Inputs	02		02	6.2
		Internal Bits Or Physical coils	Read Coils	01		01	6.1
			Write Single Coil	05		05	6.5
			Write Multiple Coils	15		0F	6.11
	16 bits access	Physical Input Registers	Read Input Register	04		04	6.4
		Internal Registers Or Physical Output Registers	Read Holding Registers	03		03	6.3
			Write Single Register	06		06	6.6
			Write Multiple Registers	16		10	6.12
			Read/Write Multiple Registers	23		17	6.17
			Mask Write Register	22		16	6.16
			Read FIFO queue	24		18	6.18
	File record access		Read File record	20		14	6.14
			Write File record	21		15	6.15
	Diagnostics		Read Exception status	07		07	6.7
			Diagnostic	08	00-18,20	08	6.8
			Get Com event counter	11		0B	6.9
			Get Com Event Log	12		0C	6.10
			Report Server ID	17		11	6.13
			Read device Identification	43	14	2B	6.21
	Other		Encapsulated Interface Transport	43	13,14	2B	6.19
			CANopen General Reference	43	13	2B	6.20

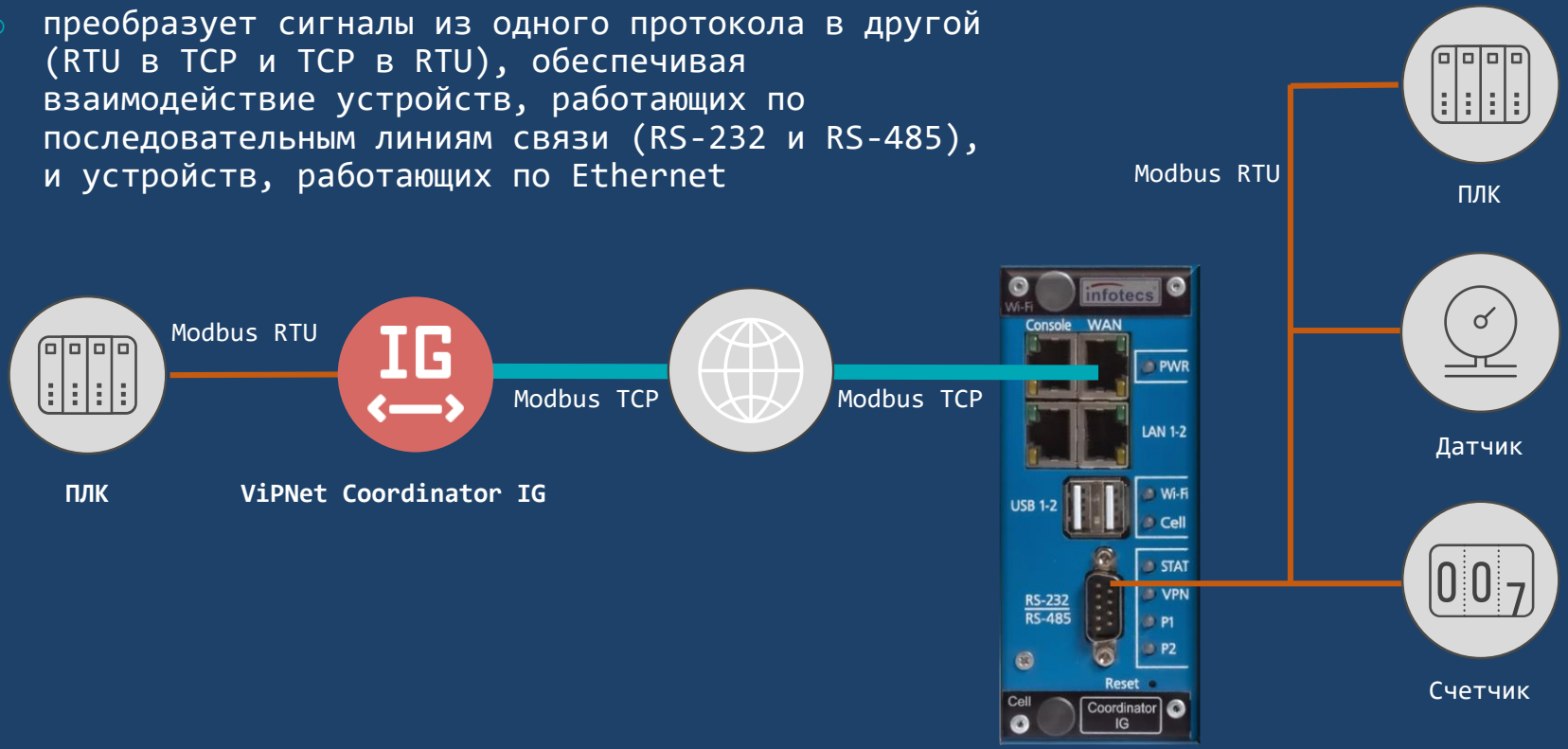
Фильтрация протокола Modbus TCP

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



Шлюз Modbus TCP-RTU и RTU-TCP

- преобразует сигналы из одного протокола в другой (RTU в TCP и TCP в RTU), обеспечивая взаимодействие устройств, работающих по последовательным линиям связи (RS-232 и RS-485), и устройств, работающих по Ethernet



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: 502

Время по умолчанию на ожидание запроса: 1500 мс

Время по умолчанию на ожидание ответа: 1500 мс

Настройки интерфейса RS-232

Скорость TTY устройства: 115200 бод

Контроль бита четности: even

Настройки интерфейса RS-485

Скорость TTY устройства: 115200 бод

Контроль бита четности: even

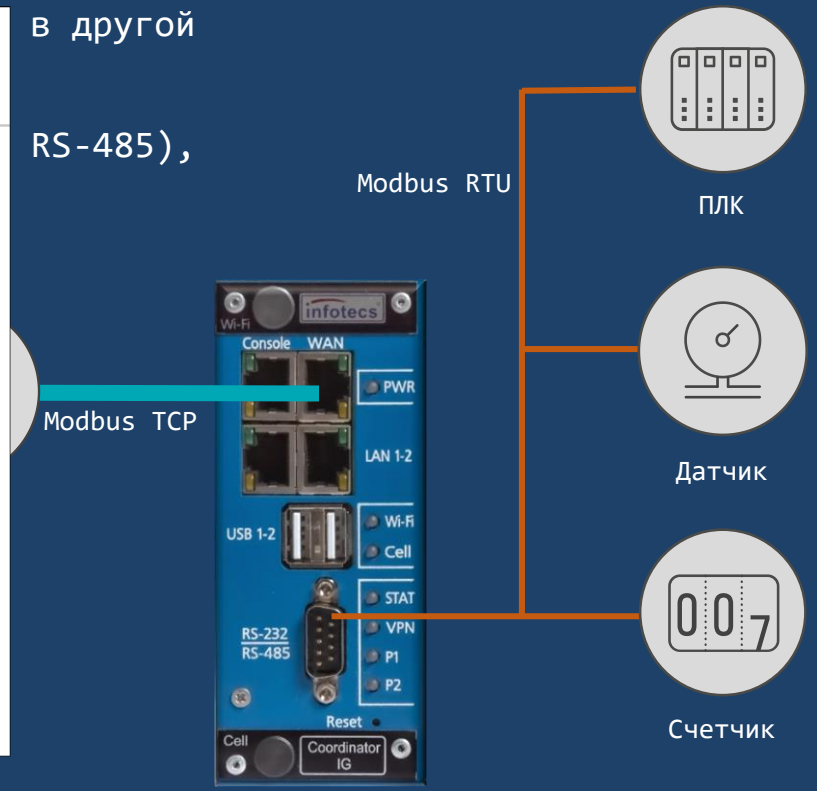
Задержка до отправки: 100 мс

Задержка после отправки: 100 мс

Сохранить | Отмена

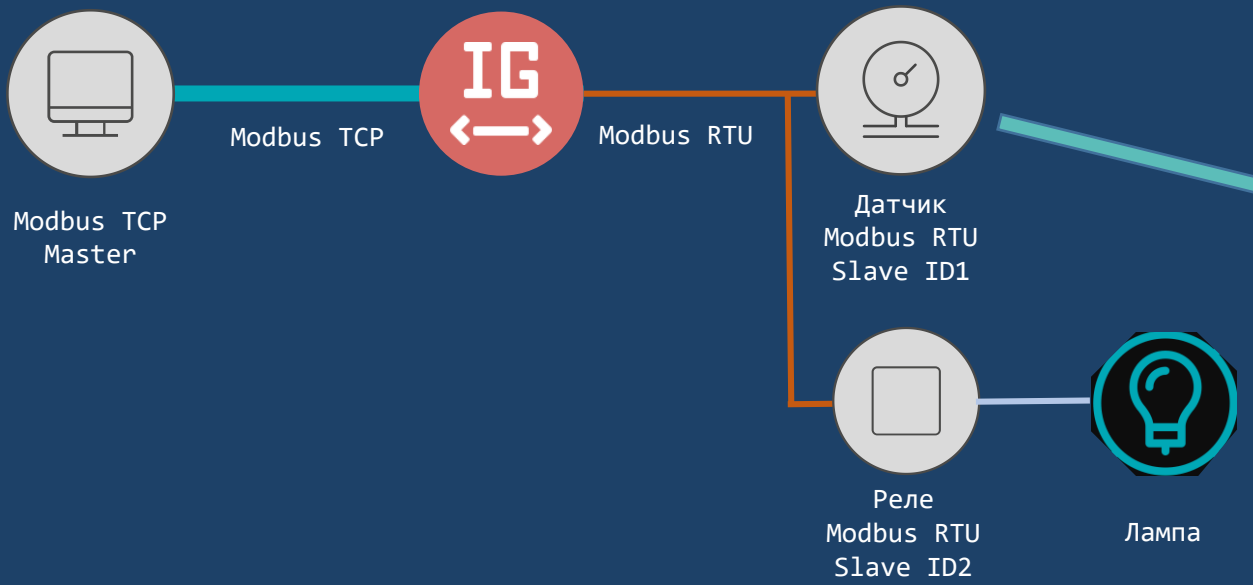
в другой

RS-485),

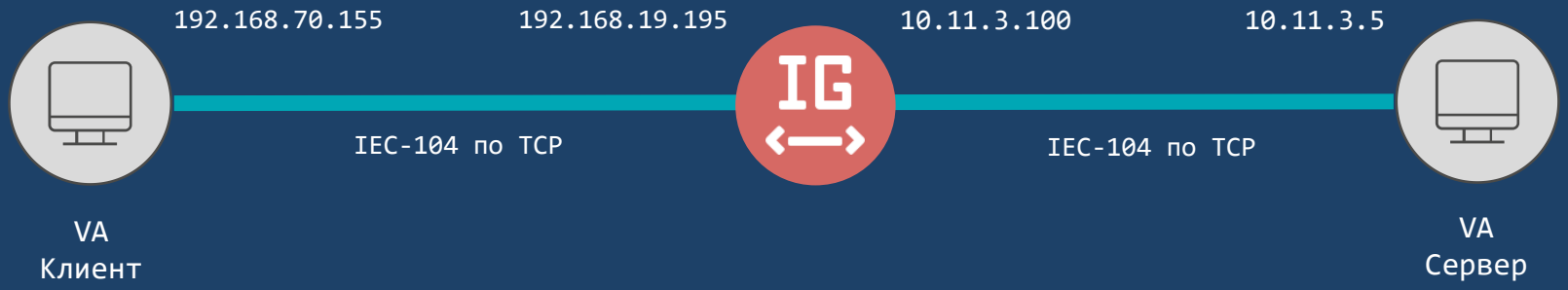


Мастер-класс

Modbus – схема стенда



МЭК-104 – схема стенда



Подписывайтесь
на наши соцсети,
там много интересного

Андрей Иванов
Andrey.Ivanov2@infotecs.ru

Иван Герасименко
Ivan.Gerasimenko@infotecs.ru