

Индустриальный шлюз безопасности: работа с промышленными протоколами

Андрей Иванов
Иван Герасименко

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 устанавливаются только на производстве!



Интерфейс Wi-Fi
Режим клиента

Доступные сети Wi-Fi

Сеть	Тип безопасности
Infotecs	[WPA-PSK-CCMP+TKIP][WPA-PSK-CCMP+TKIP]
testSSID	[WPA2-PSK-CCMP][WPS][ESS]
office202_1	[WPA-PSK-CCMP+TKIP][WPA-PSK-CCMP+TKIP]
TP-LINK_2.4GHz_BE6AB1	[WPA-PSK-CCMP][WPA2-PSK-CCMP]
Diagnost	[WPA2-PSK-CCMP][ESS]

Получаемые параметры
Получать параметры автоматически:

IP-адрес: Не задан
Маска подсети: Не задана
 DNS-серверы

USB-модем подключен

Получаемые настройки
 DNS-сервера
 Маршруты
Метрика: По умолчанию (60)

Параметры подключения

Метод настройки:	
Оператор (MNC):	N/A (0)
Страна (MCC):	N/A
DNS-адрес APN:	N/A
Имя пользователя:	N/A
Пароль:	N/A
Набираемый номер:	N/A

Информация о модеме:
Модель: RS-232 RS-485
Производитель: RS-232 RS-485
Уровень сигнала: RS-232 RS-485
SIM-карта: RS-232 RS-485
PIN-код: RS-232 RS-485

Настройка модема:
 Wi-Fi
 Cell
 STAT
 VPN
 P1
 P2

Кнопки: Переключить в режим точки доступа, Операторы, Сохранить, Отмена

Сетевые сервисы

DNS (client/server)

DNS-сервер выключен

Поиск...

DNS-сервер пересылки Доменная зона

Пользовательские DNS-адреса

- 10.0.2.4
- 10.0.2.3
- 10.0.2.6

DHCP (server/relay)

DHCP-сервер выключен Аренда адреса

Параметр подсети	Значение
Общие параметры подсетей	
Время аренды	864000 с
Максимальное время аренды	864000 с
10.0.40.0/24 - через eth2	
Широковещательный адрес	10.0.40.255

NTP (client/server)

NTP-сервер выключен

Использовать сервера "по умолчанию"

Тип	IP-адрес или DNS-имя	Способ получения адреса
pool	ntp1.vniifri.ru iburst	default
pool	ntp2.vniifri.ru iburst	default
pool	ntp3.vniifri.ru iburst	default
pool	ntp4.vniifri.ru iburst	default
Пир	ntp.local	Добавлен вручную

VLAN

Создание VLAN интерфейса

Разрешено взаимодействие интерфейса со службами

Статус и основные настройки

Родительский интерфейс: eth2

Идентификатор: 2

Класс: Access

Получаемые параметры

Получать параметры автоматически

IP-адрес: Не задан

Маска: Не задана

DNS-сервера

NTP-сервера

Маршруты

Метрика: По умолчанию

Обработка сетевого трафика в соответствии с приоритетом

В VIPNet Coordinator IG реализована поддержка протокола классификации сетевого трафика DiffServ. Использование этого протокола предполагает, что в заголовке каждого IP-пакета может быть добавлена DSCP-метка, задающая приоритет обработки пакета.

Когда на VIPNet Coordinator IG поступает IP-пакеты с DSCP-метками, по значению метки определяется принадлежность каждого IP-пакета к одному из 8 классов приоритета. IP-пакеты, принадлежащие к классу с более высоким приоритетом, всегда обрабатываются раньше пакетов, принадлежащих к менее приоритетным классам.

При зашифровании и расшифровании (инкапсуляции и деинкапсуляции) IP-пакета DSCP-метка переносится из заголовка в открытую или закрытую часть IP-пакета. Поэтому, когда на VIPNet Coordinator IG приходит открытый IP-пакет с DSCP-меткой, VIPNet Coordinator IG его шифрует и отправляет далее получателю. По пути следования IP-пакета его DSCP-метка может быть снята или изменена и будет актуальной после расшифрования пакета.

VIPNet Coordinator IG поддерживает следующие политики обработки трафика с учетом приоритета в соответствии с RFC 2474 и RFC 2475:

Создание bond интерфейса

Разрешено взаимодействие интерфейса со службами

Статус и основные настройки

Идентификатор: 2

Класс: Access

Режим: balance-rr

Сетевые интерфейсы: eth2, eth3

Частота опроса: 100 мс

Получаемые параметры

Получать параметры автоматически

IP-адрес: Не задан

Маска: Не задана

DNS-сервера

NTP-сервера

Маршруты

Маршрутизация

Сводная таблица Статическая Политики маршрутизации DHCP OSPF

Сервис OSPF включен

Маршруты

Распространять маршруты

DHCP

Статические

Настройки на первом узле	Настройки на втором узле
<pre>[network] checktime = 10 timeout = 2 activertries = 3 channelretries = 3 synctime = 5 fastdown = yes virtualmacprefix = 39</pre>	<pre>[network] checktime = 10 timeout = 2 activertries = 3 channelretries = 3 synctime = 5 fastdown = yes virtualmacprefix = 39</pre>
<pre>[channel] device = eth0 activeip = 80.251.137.40/24</pre>	<pre>[channel] device = eth0 activeip = 80.251.137.40/24</pre>

QoS

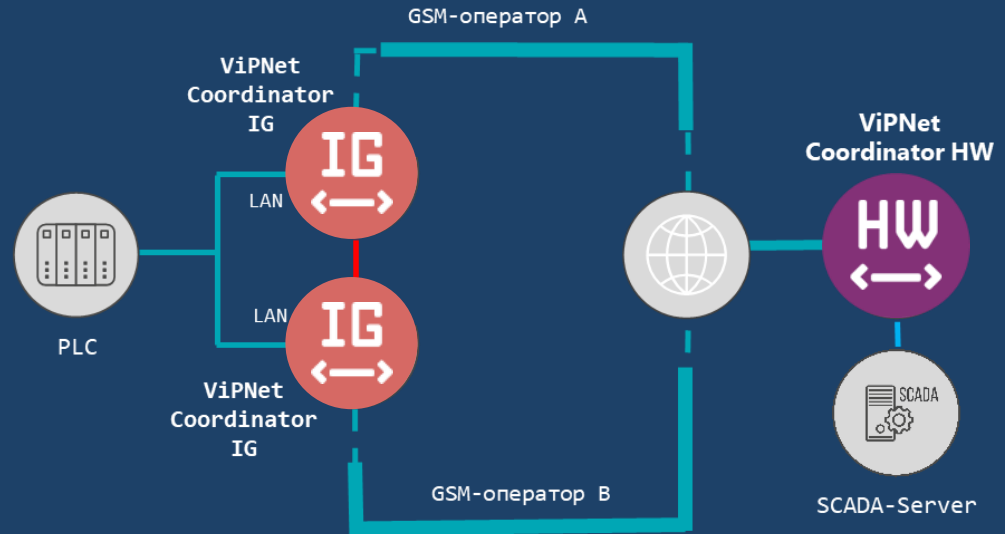
MultiWAN

OSPF

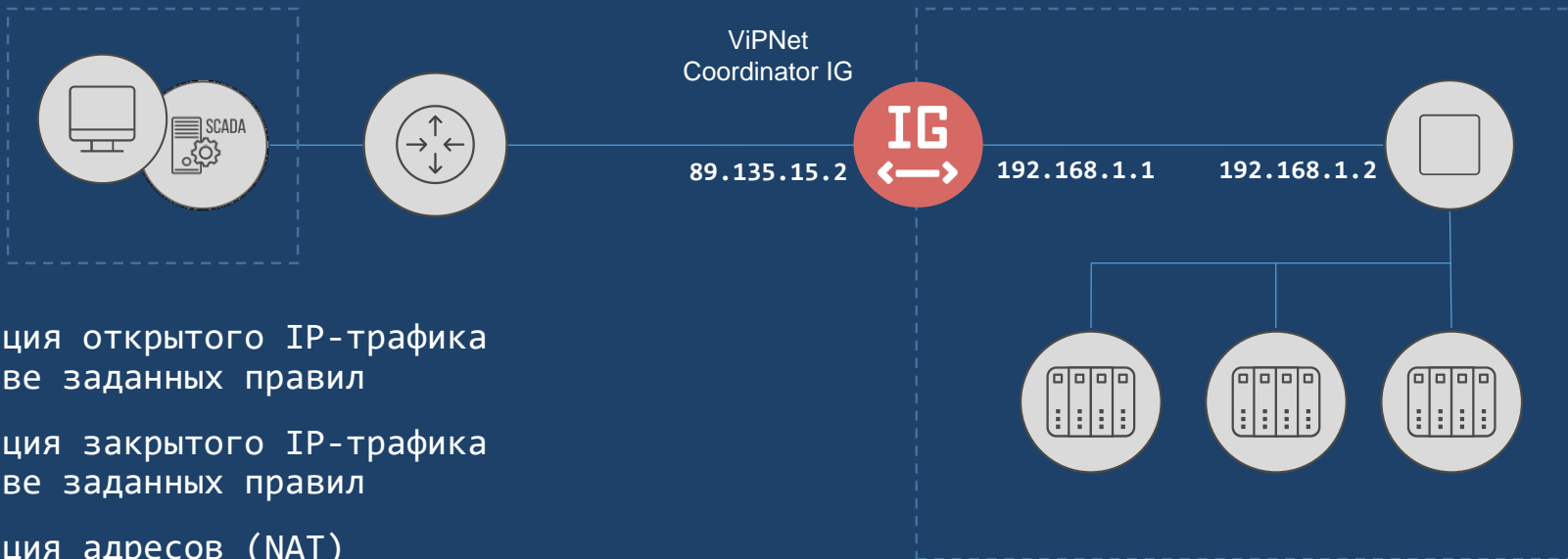
Cluster

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

Фильтрация промышленных протоколов Журналирование

Modbus МЭК104 Статистика

Найти ● Фильтрация по протоколу Modbus включена Активно 1 из 1

Статус Набор правил

- Включен Controllers_02
- Включен Controllers_03

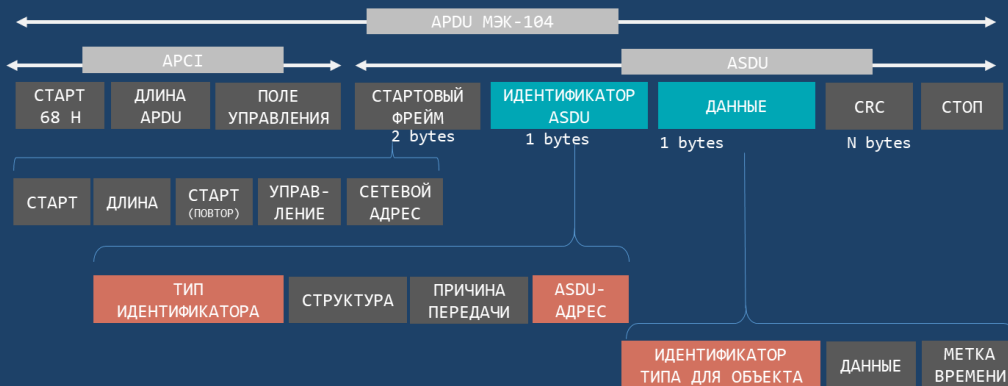
Журнал пакетов АСУ ТП

Modbus МЭК104

Фильтр IP-пакетов - Результат фильтрации за последний час, с 06.12.2021 12:21

✓	Конец интервала	Источник	Назначение	Транспорт..	Порт назн..	Размер	Адрес устр..	Код.Функции	Регистры ч..	Регистры в..	Событие
✓	13:21:16, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	168	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	168	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	912	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:21:16, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	912	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:21:02, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:21:02, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:20:28, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	1121	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:20:28, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	1121	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:20:02, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	728	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:20:02, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	728	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен
✓	13:15:28, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	1140	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:15:28, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	1140	1	03(0x03) - Чтение	Нет данных	Нет данных	66 - Пропущен
✓	13:10:02, 06 Дек 20..	192.168.70.155	192.168.26.212	6-TCP	10002	708	1	03(0x03) - Чтение	0-4	Нет данных	66 - Пропущен

Протокол МЭК 60870-5-104



ГОСТ Р МЭК 60870-5-104-2004

Грунна 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

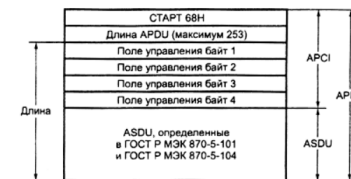


Рисунок 4 - APDU определяемого обобщающего телемеханического стандарта

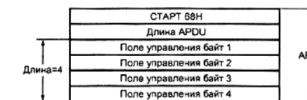


Рисунок 5 - APCI определяемого обобщающего телемеханического стандарта

Фильтрация протокола МЭК 60870-5-104 (4.5.1)

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

Набор правил фильтрации протокола МЭК104 ✕

Набор правил активен

* Название набора правил:

Набор 1

Правила транспортного уровня Правила прикладного уровня Формат протокола

+ Добавить Правил: 57

№	Статус	Имя правила	Общий адрес	Адрес ОИ	Тип	Действие
⋮ 1	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить
⋮ 2	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	⊖ Блокировать
⋮ 3	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить
⋮ 4	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	⊖ Блокировать
⋮ 5	<input checked="" type="checkbox"/>	For_con	1, 10-15	1, 1000-2000	30, 36	✓ Пропустить

Сохранить
Отмена

Протокол Modbus

<https://modbus.org/specs.php>

Advantages of Joining | Join Form | Toolkit | Subscribe to Newsletter

Text Size: S M L

MODBUS PROTOCOL

MODBUS is an application-layer messaging protocol, positioned at level 7 of the OSI model. It provides client/server communication between devices connected on different types of buses or networks.

The de facto industrial serial standard since Формализация протокола MODBUS continues to enable millions of automation devices to communicate. Today, support for the simple and elegant structure of MODBUS continues to grow. The Internet community can access MODBUS at a reserved system port 502 on the TCP/IP stack.

MODBUS is a request/reply protocol and offers services specified by function codes. MODBUS function codes are elements of MODBUS request/reply PDUs. This protocol specification document describes the function codes used within the framework of MODBUS transactions.

[MODBUS Protocol Specification](#)

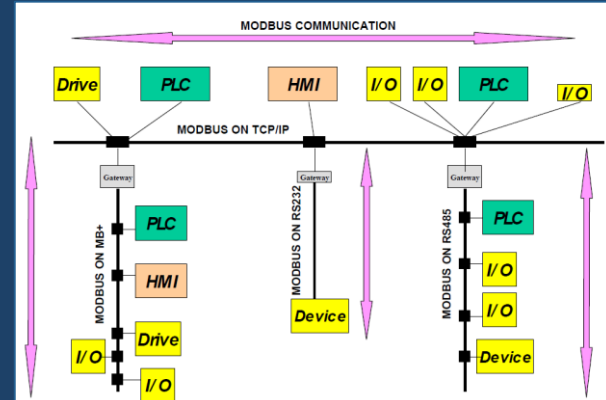
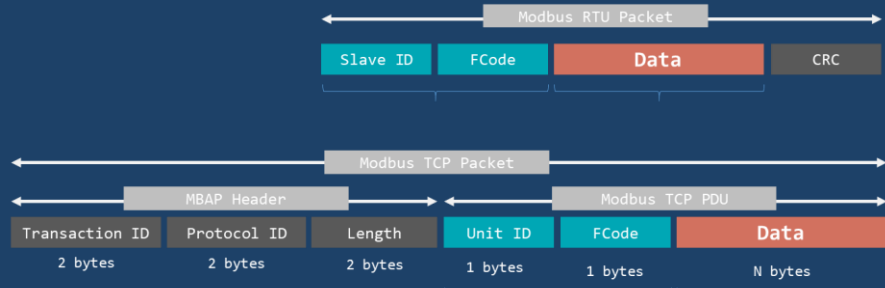


Figure 2: Example of MODBUS Network Architecture

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
	16 bits access	Physical Input Registers	Write Multiple Coils	15	0F	6.11
			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	Diagnostics	Read Exception status	07	07	6.7	
		Diagnostic	08	00-18,20	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	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

Настройка набора правил фильтрации Modbus

Набор правил включен

Название набора:

Правила транспортного уровня Правила прикладного уровня

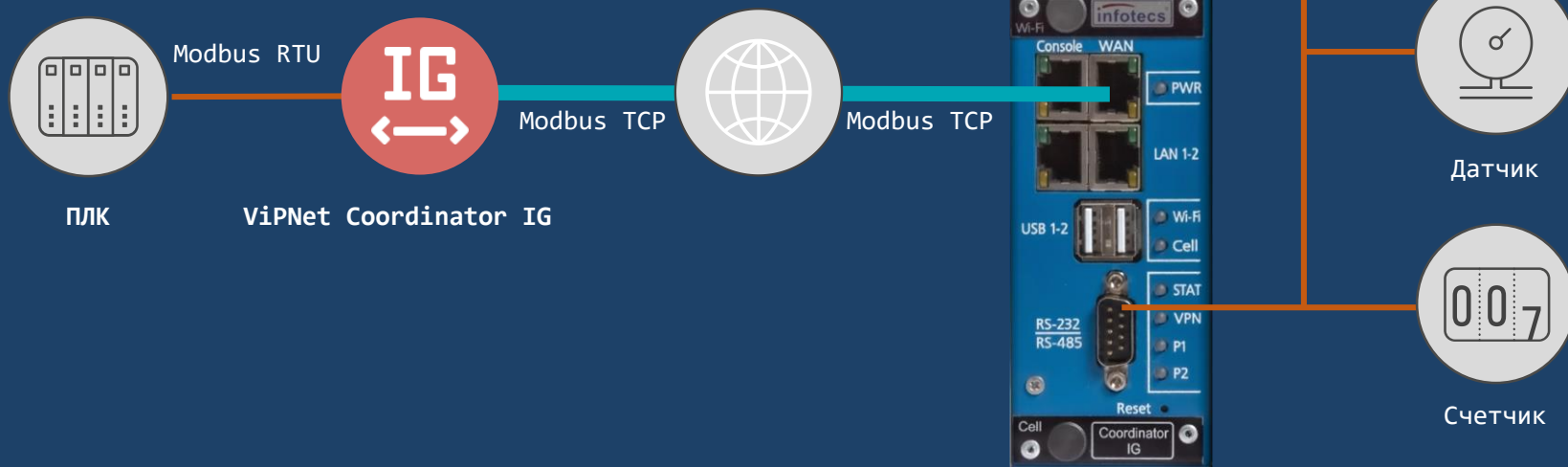
[+](#) Добавить

Таблица	Адрес сервера	Адрес клиента	Протокол	Порт назначения
Local	89.175.26.1	192.168.11.5	tcp	502
VPN	@local	0x00010201	tcp	24358

№	Статус	Имя	Действие	ID	FC	R	W
:: 1	<input checked="" type="checkbox"/>	rule_1	✓ Пропуск...	1, 10-15	2, 3	100-200	Любой
:: 2	<input checked="" type="checkbox"/>	rule_2	✗ Блокиро...	Любой	20	Любой	Любой

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:

Время по умолчанию на
ожидание запроса: мс

Время по умолчанию на
ожидание ответа: мс

Сохранить

Отмена

Настройки интерфейса RS-232

Скорость ТТУ устройства: бод

Контроль бита четности:

Настройки интерфейса RS-485

Скорость ТТУ устройства: бод

Контроль бита четности:

Задержка до отправки: мс

Задержка после отправки: мс

в другой

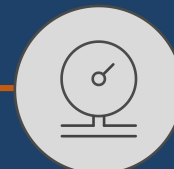
RS-485),

Modbus TCP

Modbus RTU



ПЛК



Датчик



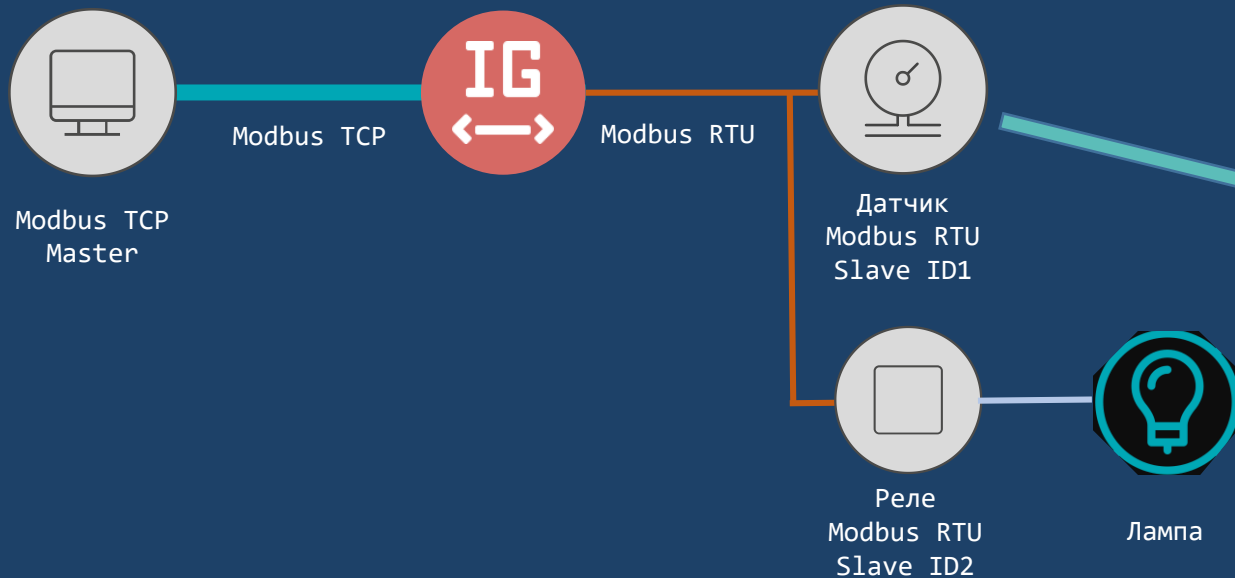
Счетчик

The logo for infotecs, featuring a red curved line above the word "infotecs" in a blue sans-serif font.

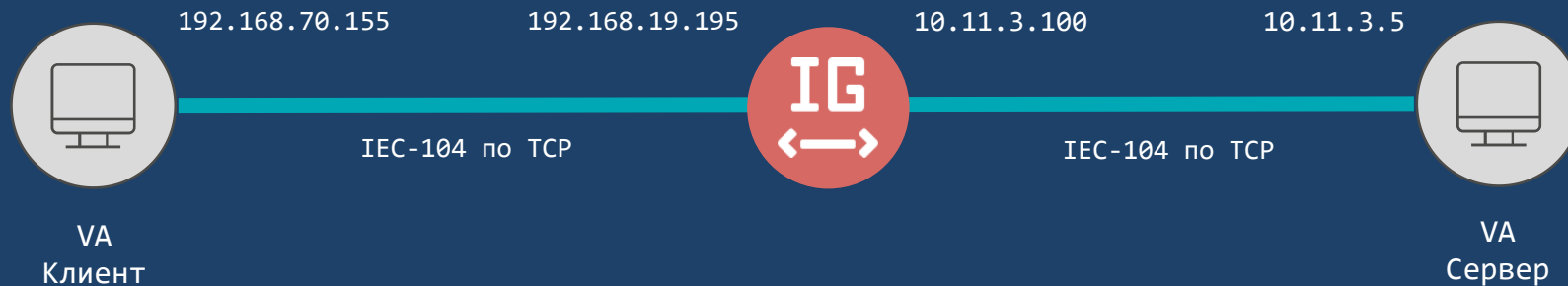
infotecs

Мастер- класс

Modbus – схема стенда



МЭК-104 – схема стенда



Подписывайтесь
на наши соцсети,
там много интересного




infotecs

The logo for infotecs features a red curved line above the word 'infotecs' in a bold, dark blue, sans-serif font.

Андрей Иванов
Andrey.Ivanov2@infotecs.ru

Иван Герасименко
Ivan.Gerasimenko@infotecs.ru