

Руководство по эксплуатации
программного обеспечения
ЭСТРА-РОУТЕР

Версия 1.8

Г. Новосибирск, 2022

Содержание

1. Обзор	4
1.1. Назначение	4
1.2. Требования к роутеру.....	4
1.3. Особенности.....	6
1.4. Комплекты.....	6
1.4.1. 3G роутер TELEOFIS RTU968 V1 + ПО ЭСТРА-РОУТЕР.....	6
1.4.2. 3G роутер TELEOFIS RTU968 V2 + ПО ЭСТРА-РОУТЕР.....	7
1.4.3. 3G роутер TELEOFIS RTU968 V4 + ПО ЭСТРА-РОУТЕР.....	7
2. Быстрая настройка	8
3. Описание 3G роутера TELEOFIS RTU968 v2.....	10
3.1. Краткое описание 3G роутера TELEOFIS RTU968 V2.....	10
3.1.1. Внешний вид.....	10
3.1.2. Режимы работы индикаторов.....	11
3.2. Подключение к роутеру TELEOFIS	12
3.2.1. Подключение через Веб-интерфейс	13
3.2.2. Подключение через SSH-соединение.....	13
3.3. Сброс роутера к заводским настройкам.....	15
3.3.1. Аппаратный сброс настроек.....	15
3.3.2. Сброс настроек через Веб-интерфейс	15
3.4. Изменение пароль доступа к роутеру.....	15
3.5. Настройка работы статического IP-адреса мобильного оператора.....	16
3.6. Прием трафика из сети Интернет	17
3.6.1. Полный доступ в сети Интернет к роутеру	18
3.6.2. Доступ к одному порту из сети Интернет (открыть порт).....	18
3.7. Установка ПО ЭСТРА-РОУТЕР на роутер.....	19
3.7.1. Установка ПО ЭСТРА-РОУТЕР через Веб-интерфейс.....	20
3.7.2. Установка ПО ЭСТРА-РОУТЕР через SSH-соединение	20
3.7.3. Работа с файлами роутера	24
3.8. Выключить режим консоли на интерфейсе RS-232.....	26

3.9.	TELEOFIS RTU968: OpenVPN.....	26
3.9.1.	Создание ключей и сертификатов	30
3.9.2.	Создание OpenVPN сервера	38
3.9.3.	Создание OpenVPN клиентов	48
3.10.	Изменение/отключение тестовых серверов для «пинга»	56
3.10.1.	Установка другого адреса тестового сервера для «пинг».....	56
3.10.2.	Отключение Simman	57
4.	Описание ПО ЭСТРА-РОУТЕР.....	58
4.1.	Configurator ESTRA-ROUTER	58
4.2.	Подключение к роутеру.....	58
4.2.1.	Загрузить byteCode.....	60
4.2.2.	Задать новый пароль	60
4.2.3.	Перепрошить.....	61
4.2.4.	Загрузить настройки.....	61
4.2.5.	Скачать настройки.....	62
4.3.	Настройка ПО ЭСТРА-РОУТЕР	63
4.3.1.	Основные настройки	63
4.3.2.	Опрашиваемые устройства.....	66
4.3.3.	МЭК 60870	69
4.3.4.	МЭК 61850	74
4.3.5.	Файлы-примеры настройки устройства.....	77
4.4.	Работа с файлами	79
4.4.1.	Открыть файл настроек роутера	79
4.4.2.	Сохранить настройки роутера в файл	79
4.4.3.	Карта тегов МЭК 60870	79
5.	Техническая поддержка	80

1. Обзор

1.1. Назначение

Программное обеспечение ЭСТРА-РОУТЕР (ПО ЭСТРА-РОУТЕР) – это программное обеспечение, предназначенное для промышленных роутеров TELEOFIS серий RTU968/RTU1068 реализованных на базе процессоров с архитектурой ARM9 (FreeScale i.MX287 454 МГц), с предустановленной операционной системой [OpenWrt](#) Chaos Calmer 15.xx (или выше) и GSM модемом. ПО ЭСТРА-РОУТЕР преобразует ваш роутер в многофункциональный контроллер, предназначенный для реализации систем передачи технологической информации с контролируемых объектов энергетики: РП, ТП, БКТП, реклоузеров и подстанций. ПО ЭСТРА-РОУТЕР осуществляет функцию конвертора (преобразователя) со сбором данных по линиям RS-485/RS-232 (протокол Modbus RTU) и передачу данных по протоколам:

- Modbus RTU Over TCP
- Modbus TCP
- МЭК 60870-5-101 (Slave)
- МЭК 60870-5-104 (Slave)

Назначение ПО ЭСТРА-РОУТЕР – сбор информации с устройств, работающих в линии RS-485/RS-232 по протоколу Modbus RTU и преобразование этих данных в выше представленные протоколы.

1.2. Требования к роутеру

Требования, предъявляемые к роутеру для установки ПО ЭСТРА-РОУТЕР:

- Процессор с архитектурой ARM9
- Установленная операционная система OpenWrt не ниже Chaos Calmer 15.xx
- Наличие двух интерфейсов RS-485/RS-232
- Наличие Ethernet разъемов

- GSM модуль для подключения к сети Интернет через GSM соединение по средствам SIM-карты

В процессе разработки ПО ЭСТРА-РОУТЕР использовался роутер [3G роутера TELEOFIS RTU968 V2](#).

3G роутера TELEOFIS RTU968 V2 имеет следующие возможности:



Рис.1. 3G роутер TELEOFIS RTU968 V2

- Два сетевых разъёма Ethernet 10/100Base-TX (LAN/WAN)
- Сетевые функции: NAT, Firewall, OpenVPN, VLAN, TinyProxy, NAPT и др.
- Поддерживаемые протоколы: SSL/TLS, HTTPS, IPv4/IPv6, PPTP, L2TP, IPSec, PPPoE, DHCP, GRE
- Промышленные интерфейсы RS-232 и RS-485
- Преобразование промышленных протоколов Modbus RTU/ASCII в Modbus TCP
- Два слота для SIM-карт для надёжного беспроводного соединения
- USB Host (тип A) для подключения внешних устройств
- Четыре универсальные линии ввода-вывода I/O
- Слот для карт памяти microSD для хранения большого объёма данных

- Разъём SMA(f) для подключения внешней усиливающей 3G антенны
- Встроенный блок часов реального времени (RTC), позволяющий сохранять ход часов при отключении внешнего питания роутера
- Аппаратный сторожевой таймер WatchDog для перезагрузки роутера в случае системных сбоев
- Монтажное крепление на DIN-рейку и на стену

1.3. Особенности

- ПО ЭСТРА-РОУТЕР можно приобрести отдельно и самостоятельно установить на роутер или сделать заказ на комплект 3G роутера TELEOFIS RTU968 и ПО ЭСТРА-РОУТЕР, в таком случае вы получите роутер с установленным ПО.
- Так как роутеры RTU968/RTU1068 поддерживают технологию виртуальной частной сети (OpenVPN), можно создать полностью закрытую сеть с высокой степенью безопасности и избежать приобретения SIM-карт со статическим IP-адресом для каждого роутера.

1.4. Комплекты

В данном разделе будут предложены несколько комплектов решения вопросов телемеханики и удаленного доступа на базе роутеров TELEOFIS RTU968 и ПО ЭСТРА-РОУТЕР.

1.4.1. 3G роутер TELEOFIS RTU968 V1 + ПО ЭСТРА-РОУТЕР

Компания TELEOFIS прекратила производство 3G роутеров TELEOFIS RTU968 V1. Однако, большое количество этих роутеров используются на существующих работающих объектах. В связи с этим можно усовершенствовать данный роутер установкой ПО ЭСТРА-РОУТЕР.

Данный роутер имеет:

- Ethernet-порт RJ-45 – 2 шт.
- Разъём RS-485 – 1 шт.

- Разъем RS-232 – 1 шт.
- GSM модуль с поддержкой 3G

Если вам необходимо два разъема RS-485 (для опроса устройств и для подключения в сеть МЭК 60870-5-101) необходимо приобрести преобразователь RS-232 в RS-485.

1.4.2. 3G роутер TELEOFIS RTU968 V2 + ПО ЭСТРА-РОУТЕР

Данный роутер пришел на замену выше описанного роутера TELEOFIS RTU968 V1. Он также имеет:

- Ethernet-порт RJ-45 – 2 шт.
- Разъем RS-485 – 1 шт.
- Разъем RS-232 – 1 шт.
- GSM модель с поддержкой 3G

Как и предшественник 3G роутер TELEOFIS RTU968 V2 имеет на борту только один разъем RS-485. При необходимости, нужно подключать преобразователь RS-232 в RS-485.

1.4.3. 3G роутер TELEOFIS RTU968 V4 + ПО ЭСТРА-РОУТЕР

Главными отличиями 3G роутер TELEOFIS V4 от 3G роутера TELEOFIS RTU968 v2 являются:

- Два промышленных интерфейса RS-485
- Разъем RS-232 изменен с DB-9M (COM-порт) на тип "разрывной клеммник"

Данный роутер имеет смысл ставить взамен 3G роутера TELEOFIS RTU968 V2 в случае если вам необходимо 2 разъема RS-485. При выборе этого роутера, вопрос о приобретении и установки преобразователя RS-232 в RS-485 отпадает.

2. Быстрая настройка

Порядок настройки роутера серии TELEOFIS RTU968/TELEOFIS RTU1068.

1. Если вы приобрели только ПО ЭСТРА-РОУТЕР (без роутера в комплекте), рекомендуется [сбросить ваш роутер к заводским настройкам](#) (если вы производите настройку удаленного роутера через Интернет, сброс настроек приведет к потере связи с устройством) и [установить ПО ЭСТРА-РОУТЕР](#). Если вы приобрели ЭСТРА-РОУТЕР (ПО + роутер в комплекте), перейдите к пункту 2.
2. Рекомендуем [изменить пароль доступа к роутеру](#), чтобы повысить уровень безопасности и предотвратить несанкционированный доступ.
3. Если вы собираетесь использовать технологию OpenVPN, [изучите инструкцию и настройте роутер](#). Пропустите пункты 4 и 5.
4. Если вы собираетесь использовать статический IP-адрес предоставляемый мобильный оператором SIM-карты для доступа к роутеру, выполните [настройку статического IP](#).
5. При использовании сети Интернет, необходимо [разрешить входящий трафик из сети](#).
6. Если вы используете закрытую частную сеть в канале связи GSM/GPRS, без доступа в сеть Интернет, необходимо [изменить/отключить «пинг» тестовых серверов](#).
7. Если вы собираетесь использовать интерфейс RS-232, необходимо [отключить его от режима консоли](#).
8. [Подключитесь к роутеру с помощью программы Configurator ESTRA-ROUTER](#).
9. При необходимости [загрузите byteCode](#) (это необходимо сделать, если вы установили ПО ЭСТРА-РОУТЕР на роутер, на котором до этого не было установлено ПО ЭСТРА-РОУТЕР, или роутер был сброшен к заводским настройкам) Рекомендуется [изменить пароль доступа к ПО ЭСТРА-РОУТЕР](#).

10.Рекомендуется перед началом работы с настройками роутера, [считать настройки, установленные в роутере](#), возможно, роутер уже настроен для работы с необходимым (-ыми) устройством (-ам). [Загрузите файл настроек](#) или [создайте настройки роутера](#) и [загрузите их](#).

3. Описание 3G роутера TELEOFIS RTU968 v2

Для получения полного описания 3G роутера TELEOFIS RTU968 V2, необходимо обратиться к [Руководству по эксплуатации](#) предоставляемым производителем роутера [TELEOFIS](#).

В данном разделе будут представлены краткое описание 3G роутера TELEOFIS RTU968 V2 и описание необходимых функций для настройки под ПО ЭСТРА-РОУТЕР.

3.1. Краткое описание 3G роутера TELEOFIS RTU968 V2

3.1.1. Внешний вид

Конструктивно роутер выполнен в металлическом корпусе с классом защиты IP30. Схема и описание кнопок и разъёмов представлены на рисунке 2.

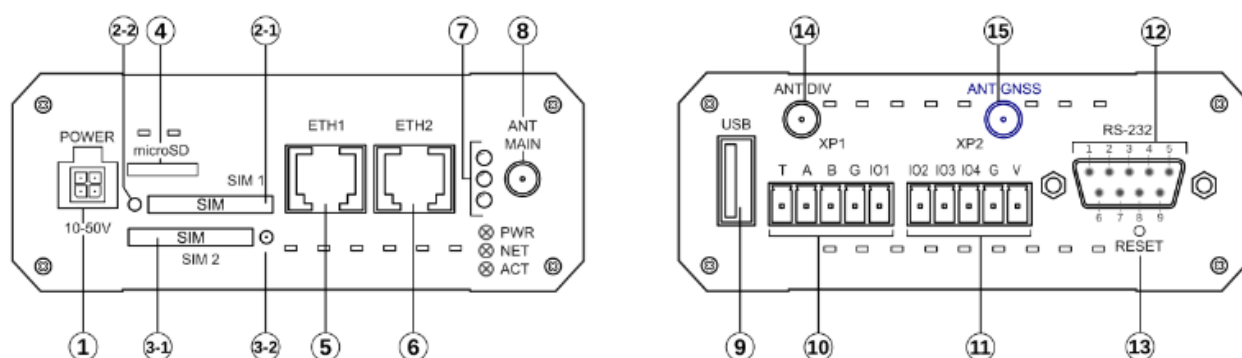


Рис.2. Внешний вид 3G роутера TELEOFIS RTU968 V2

Таблица 1. Разъемы и контакты 3G роутера TELEOFIS RTU968 V2

Обозначение	Описание	
<i>Внешний вид с лицевой стороны</i>		
1	Power	4-контактный разъём MicroFit для подключения питания 10-50В DC
2-1	SIM1	Слот SIM-карты 1
2-2		Кнопка для извлечения SIM-карты 1
3-1	SIM2	Слот SIM-карты 2
3-2		Кнопка для извлечения SIM-карты 2
4	microSD	Слот microSD для карты памяти
5	ETH1	Порт Ethernet1 (LAN/WAN 10/100 Мбит/с), разъём RJ-45
6	ETH2	Порт Ethernet2 (LAN/WAN 10/100 Мбит/с), разъём RJ-45
7		Светодиодные индикаторы (сверху вниз: PWR, NET, ACT)
8	ANT MAIN	Разъём SMA(f) для подключения 3G антенны

<i>Внешний вид с обратной стороны</i>			
9	USB	Разъём USB 2.0, тип A	
10 Клеммный разъём	XP1	T	Вывод встроенного терминального резистора
		A	Сигнал "А+" линии RS-485
		B	Сигнал "В-" линии RS-485
		G	Сигнальная земля (подключается при необходимости)
		IO1	Универсальная линия ввода-вывода 1
11 Клеммный разъём	XP2	IO2	Универсальная линия ввода-вывода 2
		IO3	Универсальная линия ввода-вывода 3
		IO4	Универсальная линия ввода-вывода 4
		G	Земля
		V	Положительный вход внешнего питания 10-50В
12	RS-232	9-контактный разъём DB-9М интерфейса RS-232	
13	RESET	Кнопка для перезагрузки/сброса настроек роутера	
14	ANT DIV	Отсутствует	
15	ANT GNSS	Отсутствует	

3.1.2. Режимы работы индикаторов

На лицевой стороне расположены три светодиодных индикатора: PWR, NET, АСТ. По умолчанию индикаторы настроены на следующие значения:

- PWR – индикатор питания.
- NET – индикатор 3G соединения.
- АСТ – индикатор приема-передачи данных по 3G.

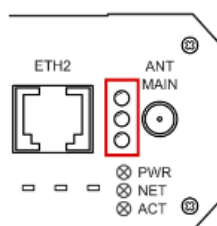


Рис.3. Индикаторы

Таблица 2. Режимы индикации.

Индикатор	Функция	Состояние	Описание
PWR	Питание	Горит непрерывно	Питание подключено
		Не горит	Питание отключено
NET	3G соединение	Горит непрерывно	Установлено 3G соединение
		Не горит	Нет регистрации в 3G сети
АСТ	Прием-передача данных по 3G	Мигает	Идет прием-передача данных о сети 3G

3.2. Подключение к роутеру TELEOFIS

В данном разделе представлены способы подключения через Ethernet сеть.

Параметры по умолчанию:

- IP-адрес: 192.168.88.1
- Логин: root
- Пароль: root

Чтобы произвести подключение к роутеру, необходимо настроить «Сетевое подключение». Ниже описан пример для ОС Windows 10:

- Перейдите в сетевые подключения, например, панель управления (Просмотр: категория) -> Сеть и Интернет -> Центр управления сетями и общим доступом -> Изменение параметров адаптера
- Выберите необходимый интерфейс. Нажмите правой кнопкой мыши на него и выберите «Свойства»
- В списке выберите «IP версии 4 (TCP/IPv4)» и нажмите «Свойства»
- Задайте необходимые параметры для подключения к роутеру (рисунок 4).
- После нажмите «ОК»

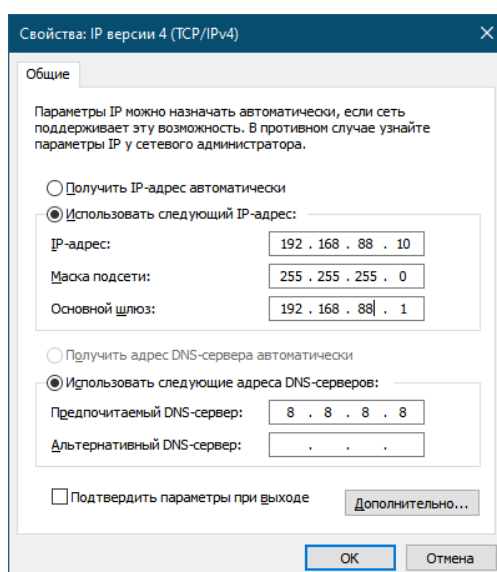


Рис.4. Настройки сетевого подключения (ОС Windows 10)

Соедините ваш компьютер и роутер Ethernet кабелем: разъем RJ-45 на компьютере, и один из разъемов RJ-45 на роутере (ETH1, ETH2).

3.2.1. Подключение через Веб-интерфейс

[Настройте на компьютере интерфейс](#). Откройте любой веб-браузер. В адресной строке введите IP-адрес роутера. Загрузится страница авторизации роутера TELEOFIS. Введите логин и пароль (по умолчанию root/root). После этого вы будете перенаправлены на главную страничку роутера.

3.2.2. Подключение через SSH-соединение

[Настройте на компьютере интерфейс](#). Пример подключения через SSH будет продемонстрирован на ОС Windows 10 с использованием программы PuTTY (свободно распространяемый клиент для различных протоколов удаленного доступа):

- Запустите PuTTY
- В окне программы установите IP-адрес роутера, порт 22 и выберите тип соединения SSH (рисунок 5) и нажмите кнопку «Соединиться»
- Если высветится окно «Предупреждение безопасности PuTTY» нажмите «Да» или «Нет», в зависимости от того, хотите ли вы запомнить ключ сервера.
- Далее будет предложено ввести логин. Введите логин и нажмите «Enter» (по умолчанию root).
- Далее будет предложено ввести пароль. Введите пароль и нажмите «Enter» (по умолчанию root).
- После успешного подключения вы попадете в консоль операционной системы роутера (рисунок 6).

!!!Важно. Подключение через SSH-соединение можно выполнить только при подключении через ETH1/ETH2 если через [OpenVPN](#). Если ваш роутер находится в сети Интернет через 3G соединение и имеет статический IP-

адрес, вам необходимо [открыть порт 22](#) для подключения из сети Интернет по SSH.

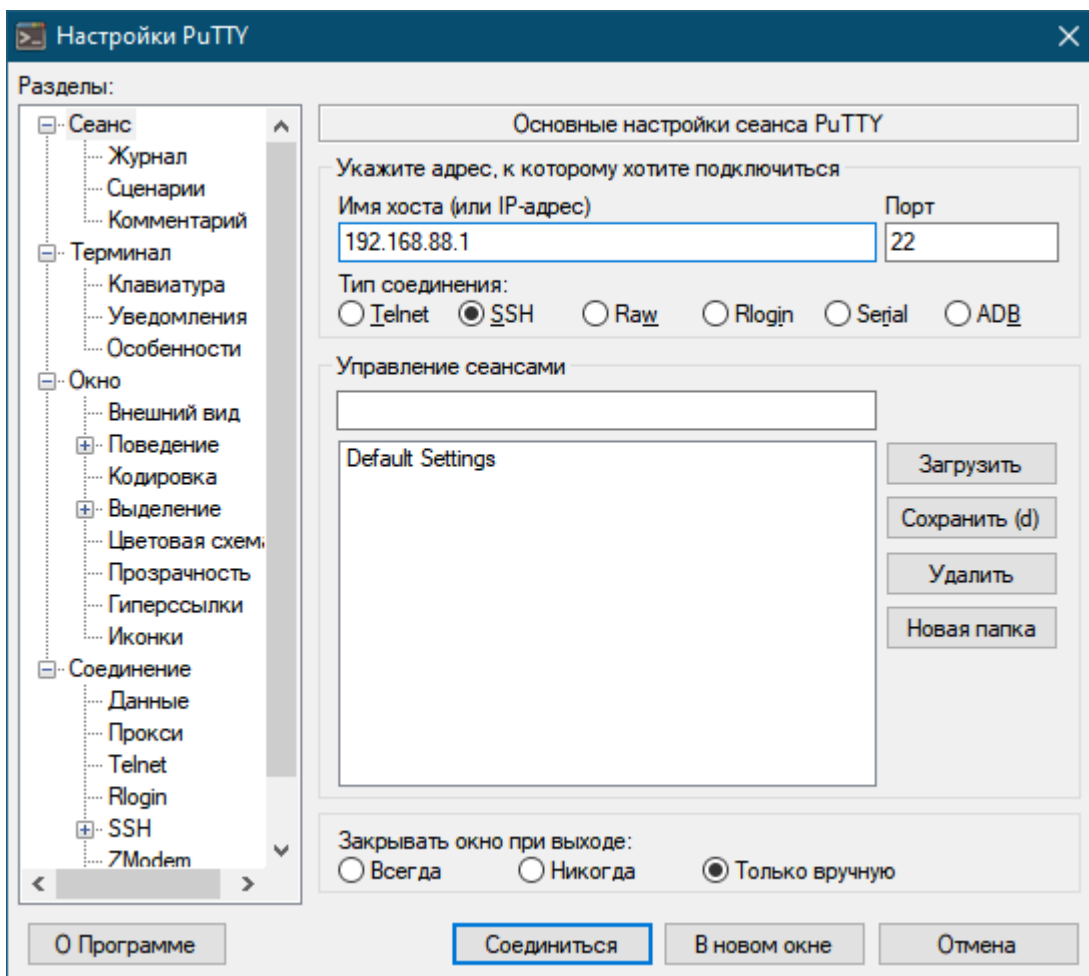


Рис.5. Настройки программы PuTTY

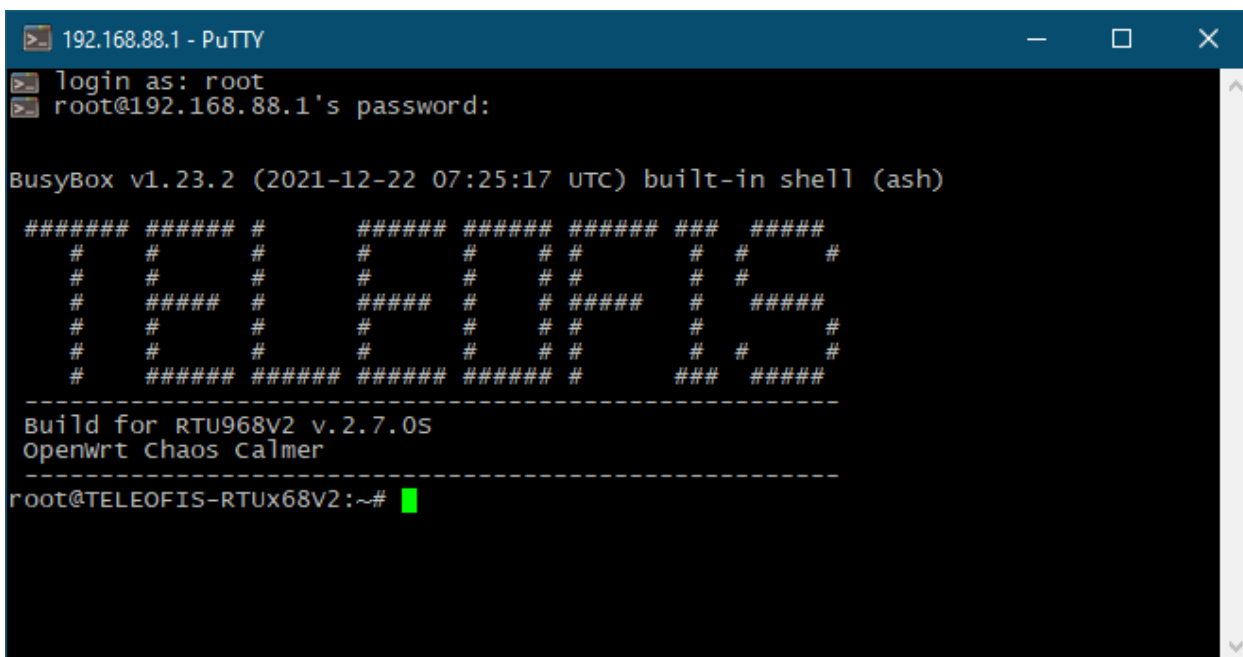


Рис.6. Консоль операционной системы роутера в программе PuTTY

3.3. Сброс роутера к заводским настройкам

3.3.1. Аппаратный сброс настроек

Аппаратный сброс настроек на заводские значения осуществляется с помощью кнопки RESET на задней панели корпуса (рисунок 7).

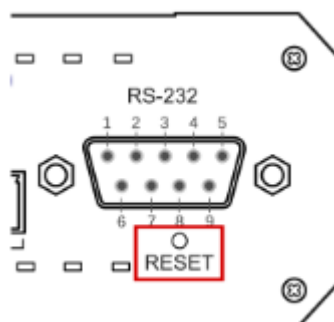


Рис.7. Кнопка сброса настроек

Чтобы сбросить настройки на заводские, удерживайте кнопку RESET от 3 до 8 секунд.

При удержании кнопки до 3 секунд или более 8 секунд – роутер перезагружается.

3.3.2. Сброс настроек через Веб-интерфейс

[Подключитесь к роутеру через Веб-интерфейс](#). Перейдите во вкладку: Система -> Резервная копия/Прошивка. На этой вкладке «Действия» нажмите кнопку «Выполнить сброс».

В открывшемся окне нажмите «ОК» для подтверждения сброса. Сразу после этого начнется удаление раздела конфигурации с последующей перезагрузкой системы.

3.4. Изменение пароль доступа к роутеру

По умолчанию роутер имеет логин root и пароль root. Если вы собираетесь использовать роутер в глобальной сети Интернет **рекомендуется** изменить пароль доступа.

Для этого [подключитесь к роутеру через Веб-интерфейс](#).

Перейдите на страничку: Система -> Управление

На данной странице вы увидите раздел «Пароль маршрутизатора», задайте новый пароль, после чего пролистайте в конец страницы и нажмите кнопку «Сохранить и применить».

Закройте вкладку и подключитесь еще раз к роутеру через Веб-интерфейс. Теперь для подключения необходимо использовать новый пароль.

3.5. Настройка работы статического IP-адреса мобильного оператора

Как правильно при предоставлении оператором связи статического IP-адреса, он передает необходимый набор настроек, например, имя точки доступа (AP), имя пользователя, пароль и т.д.

[Подключитесь к роутеру через Веб-интерфейс](#). Перейдите на страничку: Сервисы -> Менеджер SIM. Прокрутите страничку вниз, до разделов параметры SIM-карты 1, параметры SIM-карты 2. Введите необходимые настройки, например, для статического IP-адреса в Сибирском регионе оператор MTS предоставляет точку доступа: static.sib (рисунок 8). После задания необходимых настроек прокрутите страничку ниже и нажмите кнопку «Сохранить и применить».

Параметры SIM-карты 1

Приоритет	<input type="text" value="high"/>
Имя точки доступа	<input type="text" value="static.sib"/>
Пин код	<input type="text"/>
Имя пользователя	<input type="text"/>
Пароль	<input type="text"/>
Адреса тестовых серверов для пинга	<input type="text"/>

Рис.8. Задания настроек SIM-карты

После этой настройки (при условии, что SIM карта уже установлена) модем регистрируется в сети и с помощью команды «ping» в командной строке можно проверить его наличие в сети Интернет.

Так же можно перейти в раздел: Сеть -> Интерфейсы. В списке интерфейсов должен быть интерфейс INTERNET (3g-internet), в состоянии должен быть указан ваш статической IP-адрес (рисунок 9).

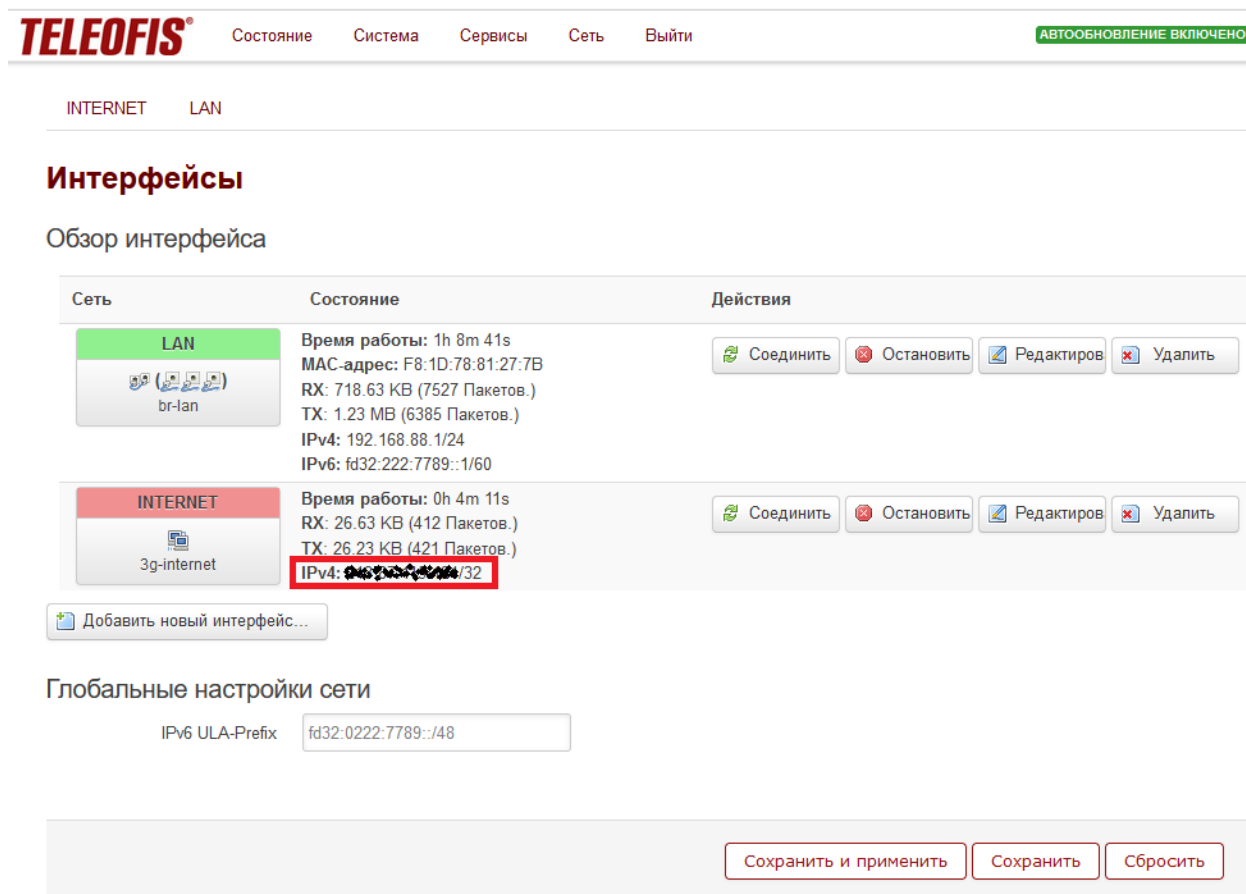


Рис.9. IP-адрес сети Интернет

3.6. Прием трафика из сети Интернет

По умолчанию в роутере включен запрет на прием данных из сети Интернет, это означает, что нельзя подключиться через Веб-интерфейс или к ПО ЭСТРА-РОУТЕР через статический IP-адрес, предоставляемый мобильным оператором.

В этом разделе будет предоставлен алгоритм действий для включения приема данных из сети Интернет. Так как роутер становится доступным из сети Интернет **рекомендуется [изменить пароль доступа к роутеру](#)**.

Есть два варианта предоставления доступа из сети Интернет к роутеру:

1. Полный доступ
2. Открыть один порт

В целях сохранения большей безопасности, **рекомендуется** открывать доступ только отдельным портам, которые будут использоваться

!Важно. При одновременном использовании Интернет-соединения и локального подключения к разъемам ETH1 и/или ETH2 (в режиме DHCP), Интернет соединение SIM-карты нестабильное.

3.6.1. Полный доступ в сети Интернет к роутеру

[Подключитесь к роутеру через Веб-интерфейс](#). Перейдите на страничку: Сеть -> Межсетевой экран. Выберите вкладку «Основные настройки». В разделе «Зоны» установите «Принимать» входящий трафик для «wan» (рисунок 10)

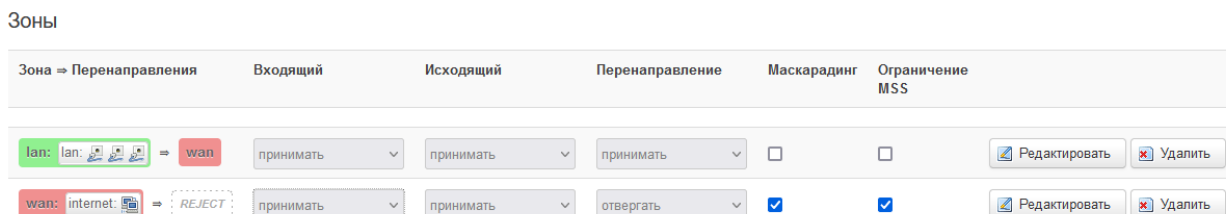


Рис.10. Включить полный доступ в сети Интернет к роутеру

После нажмите кнопку «Сохранить и применить». После этого можно подключаться к роутеру из сети Интернет.

3.6.2. Доступ к одному порту из сети Интернет (открыть порт)

Данный способ предоставления доступа к роутеру разрешает подключаться только по указанному порту. Вы можете создать разрешения для нескольких портов.

[Подключитесь к роутеру через Веб-интерфейс](#). Перейдите на страничку: Сеть -> Межсетевой экран. Выберите вкладку «Основные настройки». Убедитесь, что прием всего входящего трафика из сети Интернет выключен (рисунок 11). У вас включен прием входящего трафика, отключите его (как это показано на рисунке 11) и нажмите кнопку «Сохранить и применить».

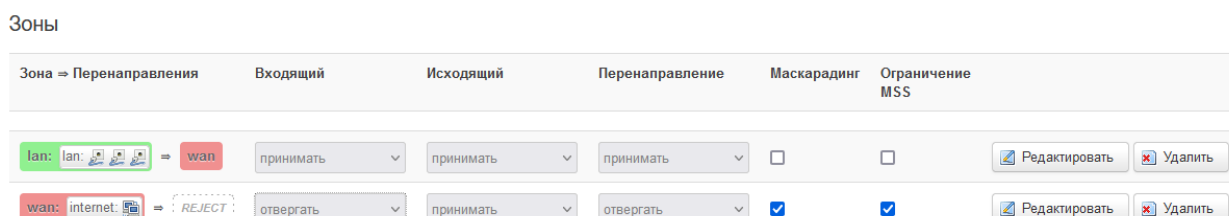


Рис.11. Прием входящего трафика из сети Интернет выключен

Перейдите на вкладку «Правила для трафика». В разделе «Правила для трафика» список портов для которых предоставлен доступ из сети Интернет. Для примера добавим доступ для Веб-интерфейса, это порт 80.

В подразделе «Открыть порты на маршрутизаторе» вводим имя, например, Веб-интерфейс. Выбираем протокол «TCP» и указываем номер порта, который хотим открыть, например, 80 (рисунок 12). После ждем кнопку «Добавить».

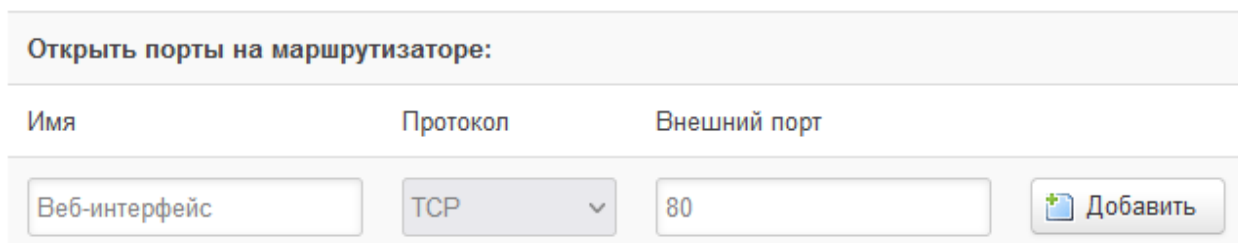


Рисунок 12. Открыть порт

После проделанной процедуры, страница автоматически обновится и в списке «Правила для трафика» появится добавленный вами порт. Далее необходимо пролистать страничку вниз и нажать кнопку «Сохранить и применить».

Доступ к этому порту открыт из сети Интернет.

3.7. Установка ПО ЭСТРА-РОУТЕР на роутер

Установить ПО ЭСТРА-РОУТЕР можно несколькими способами, рассмотрим каждый из них.

3.7.1. Установка ПО ЭСТРА-РОУТЕР через Веб-интерфейс

[Подключитесь к роутеру через Веб-интерфейс](#). Перейдите на страничку: Система -> Программное обеспечение. На вкладке «Действия» в списке «Установленных пакетов» найдите estraApp удалите (если данный пакет установлен).

Перейдите на вкладку «Загрузить». Нажмите кнопку «Обзор» и выберите *.ipk файл ПО ЭСТРА-РОУТЕР. Далее нажмите кнопку «Установить». После этих действия страничка обновится и под кнопкой обзор будет текст: Пакет установлен.

!Важно. Если произошла ошибка установки, необходимо сделать [установку через SSH-соединение](#).

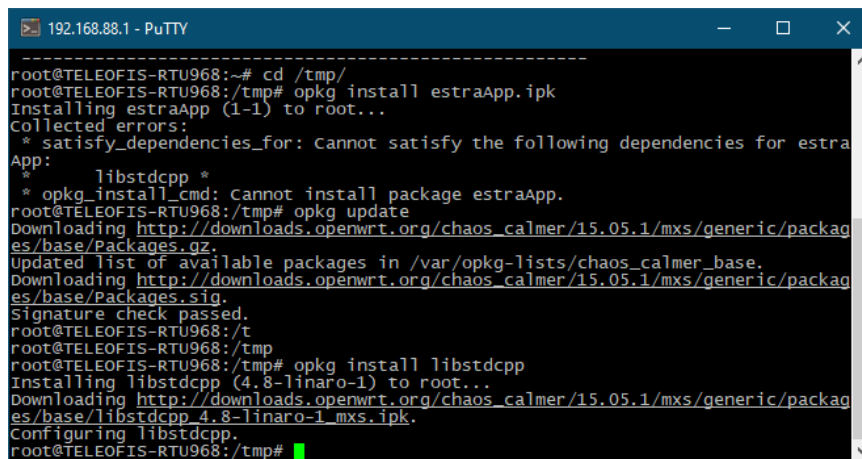
Для того, чтобы убедиться в работоспособности пакета, перейдите на страничку: Состояние -> Процессы. В списке найдите estraApp. Если в списке есть estraApp (например, /sbin/estraApp) значит пакет установлен и запущен. В противном случае повторите установку или обратитесь в [службу технической поддержки](#).

Если вы используете сеть Интернет мобильного оператора, необходимо открыть порт 30000, для [предоставления доступа из сети Интернет](#) к ПО ЭСТРА-РОУТЕР.

3.7.2. Установка ПО ЭСТРА-РОУТЕР через SSH-соединение

[Подключитесь к роутеру через SSH-соединение](#). Установка ПО ЭСТРА-РОУТЕР будет показана на примере программы PuTTY на ОС Windows 10.

Перейдите в каталог tmp с помощью команды `cd /tmp/` (рисунок 13) – необходимо ввести команду и нажать кнопку «Enter».



```
192.168.88.1 - PuTTY
-----
root@TELEOFIS-RTU968:~# cd /tmp/
root@TELEOFIS-RTU968:~/tmp# opkg install estraApp.ipk
Installing estraApp (1-1) to root...
Collected errors:
* satisfy_dependencies_for: Cannot satisfy the following dependencies for estraApp:
* libstdc++ *
* opkg_install_cmd: Cannot install package estraApp.
root@TELEOFIS-RTU968:~/tmp# opkg update
Downloading http://downloads.openwrt.org/chaos_calmer/15.05.1/mxs/generic/packages/base/Packages.gz.
Updated list of available packages in /var/opkg-lists/chaos_calmer_base.
Downloading http://downloads.openwrt.org/chaos_calmer/15.05.1/mxs/generic/packages/base/Packages.sig.
Signature check passed.
root@TELEOFIS-RTU968:~/tmp# opkg install libstdc++
Installing libstdc++ (4.8-linaro-1) to root...
Downloading http://downloads.openwrt.org/chaos_calmer/15.05.1/mxs/generic/packages/base/libstdc++_4.8-linaro-1_mxs.ipk.
Configuring libstdc++
root@TELEOFIS-RTU968:~/tmp#
```

Рис.20. Установка недостающей библиотеки

Теперь снова пробуем установить ПО ЭСТРА-РОУТЕР (opkg install estraApp.ipk). Если ошибка осталась, обратитесь в службу [тех. поддержки](#).

Если вы используете сеть Интернет, или ПО ЭСТРА-РОУТЕР должно работать в сети Интернет, необходимо открыть порт 30000, для [предоставления доступа из сети Интернет](#) к ПО ЭСТРА-РОУТЕР.

3.7.3. Работа с файлами роутера

Для работы с файлами (загрузка/выгрузка) воспользуемся программой [WinSCP](#) – свободный графический клиент протоколов SFTP и SCP, предназначенный для Windows. Необходимо скачать и установить данную программу.

После запуска WinSCP отобразится окно для входа, необходимо задать параметры роутера (рисунок 21)

- Протокол – SCP
- Имя хоста – IP-адрес
- Порт – 22
- Имя пользователя – root (по умолчанию)
- Пароль – пароль который установлен роутере (по умолчанию root)

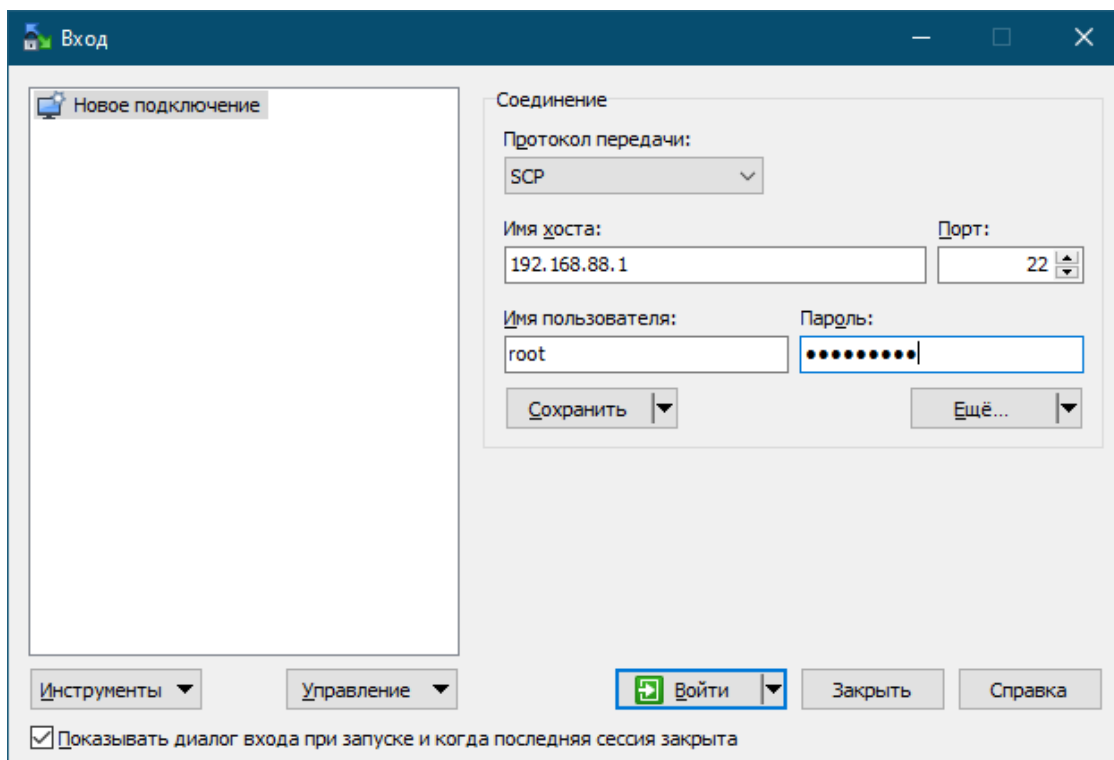


Рис.21. Вход программа WinSCP

Далее нажимаем на кнопку «Войти». При появлении окна о подключении к неизвестному серверу и добавлении его ключа в кэш, нажмите «Да», если хотите запомнить ключ, «Нет» если не запоминать ключ, но продолжить подключение.

В левом окне программы будет представлена файловая система компьютера, а в правом окне файловая система роутера.

Для примера, загрузим файл *.ipk ПО ЭСТРА-РОУТЕР в каталог tmp.

В правом окне вы будете находиться в каталоге пользователя (root), необходимо перейти в корневой каталог, далее в каталог tmp.

В левом окне перейдите в каталог где расположен файл ПО ЭСТРА-РОУТЕР (*.ipk). Нажмите правой кнопкой мыши на файл и в выпадающем меню выберите отправить (рисунок 22). Нажмите «Ок» в появившемся окне. После этого, файл загрузится на роутер и появится в правом окне программы.

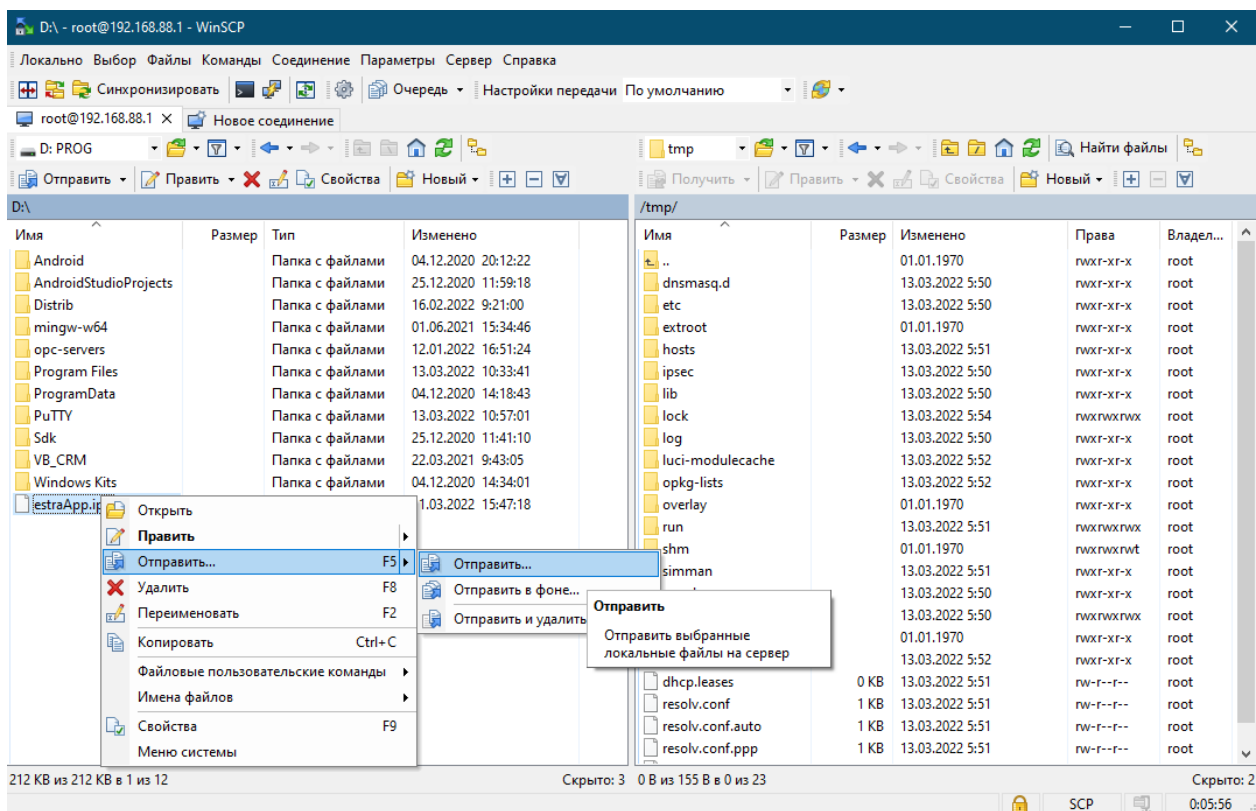


Рис.22. Загрузить файл на роутер с помощью WinSCP

3.8. Выключить режим консоли на интерфейсе RS-232

Если вы собираетесь использовать интерфейс RS-232, необходимо отключить режим консоли, который по умолчанию работает на интерфейсе RS-232. Для этого [подключитесь к роутеру через Веб-интерфейс](#). Перейдите на страничку: Сервисы -> Опрос портов по TCP. Интерфейсу RS-232 соответствует порт с адресом /dev/com0. Найдите его в списке и нажмите кнопку «Редактировать». Страница обновится и отобразятся настройки порта /dev/com0. Нажмите кнопку «Отключить» напротив текста «Отключить консоль». Далее нажмите на кнопку «Сохранить и применить». Роутер автоматически перезагрузиться.

3.9. TELEOFIS RTU968: OpenVPN

OpenVPN — свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами и другими устройствами Ethernet-сети. Она позволяет устанавливать соединения между

компьютерами и другими устройствами сети, находящимися за NAT и сетевым экраном, без необходимости изменения их настроек.

Зачем использовать технологию OpenVPN в сфере энергетики? Если вы собираетесь использовать удаленное подключение к устройствам энергетике в сети Интернет, может возникнуть ряд проблем. Основными из которых являются:

1. Предоставление каждому удаленному объекту статического IP-адреса.
2. Обеспечение необходимой безопасности для минимизации случаев несанкционированного доступа к объектам энергетики.

Первая проблема обусловлена двумя факторами:

- Длина IP-адреса (IPv4) имеет конечный размер, в связи с чем список IP-адресов ограничен. Еще в феврале 2011 года региональным интернет-регистраторам (организации, занимающиеся вопросами адресации и маршрутизации в сети Интернет.) были выделены *последние* пять блоков адресных пространств. Из-за это региональные интернет-регистраторы ограничили выдачу новых адресов. Из этого вытекает второй фактор проблемы предоставление каждому удаленному объекту статический IP-адрес.
- Мобильные операторы предоставляют статический IP-адрес только юридическим лицам и с обязательной ежемесячной абонентской платой.

Вторая проблема заключается в том, что сегодня в сети Интернет расплодилось много злоумышленников, которые с помощью программ-ботов перебирают все существующие IP-адреса. Такие злоумышленники, скорее всего, не получают выгоды для себя в случае несанкционированного доступа к объекту энергетики, но могут предоставить много неприятностей потребителям, обслуживающему персоналу: сброс устройств на заводские настройки, изменение настроек роутера и другие действия, которые могут привести к отключению объекта энергетики или неправильной работе. Так же

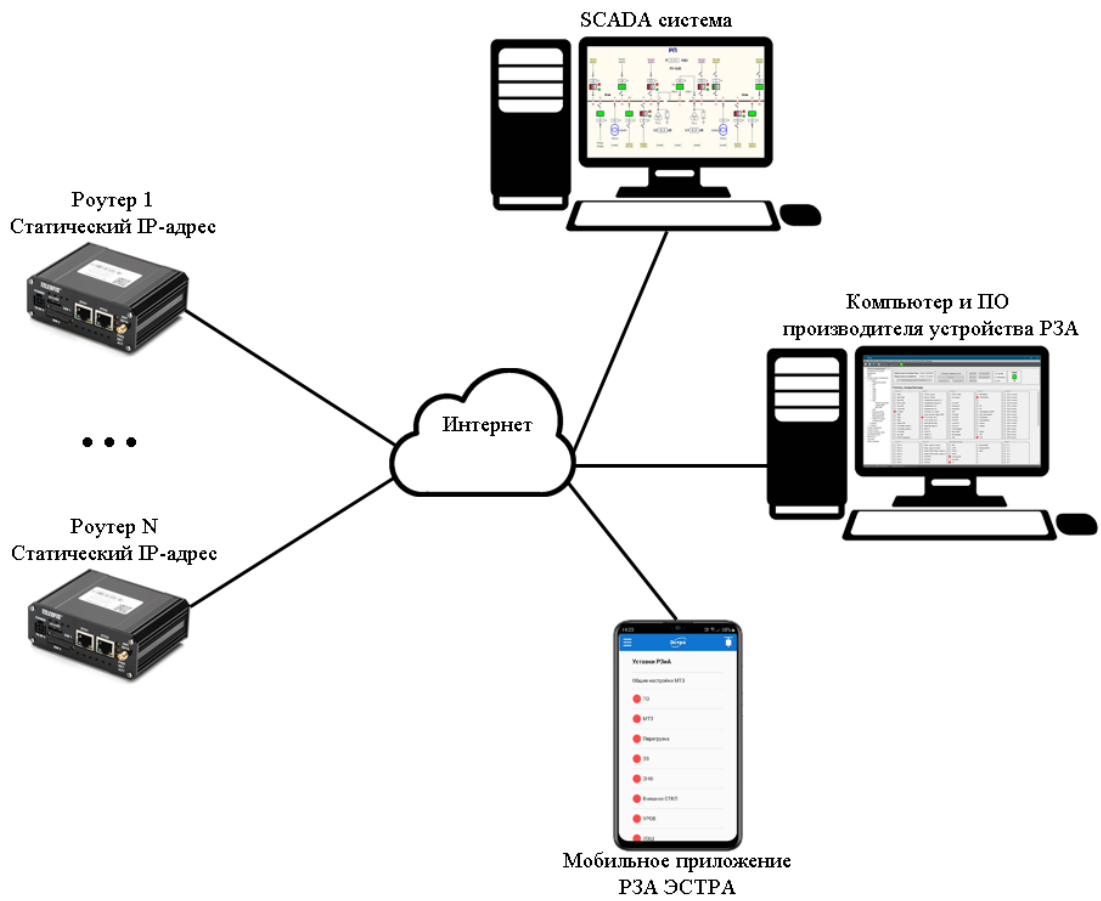
ко второй проблеме можно отнести ситуацию, когда любой человек (конкурент по бизнесу, уволенный сотрудник, обиженный на руководство и т.д.), зная IP-адрес устройства, подключается и приводит объект к отключению или неправильной работе.

На рисунке 23 представлены две структуры организации удаленного доступа:

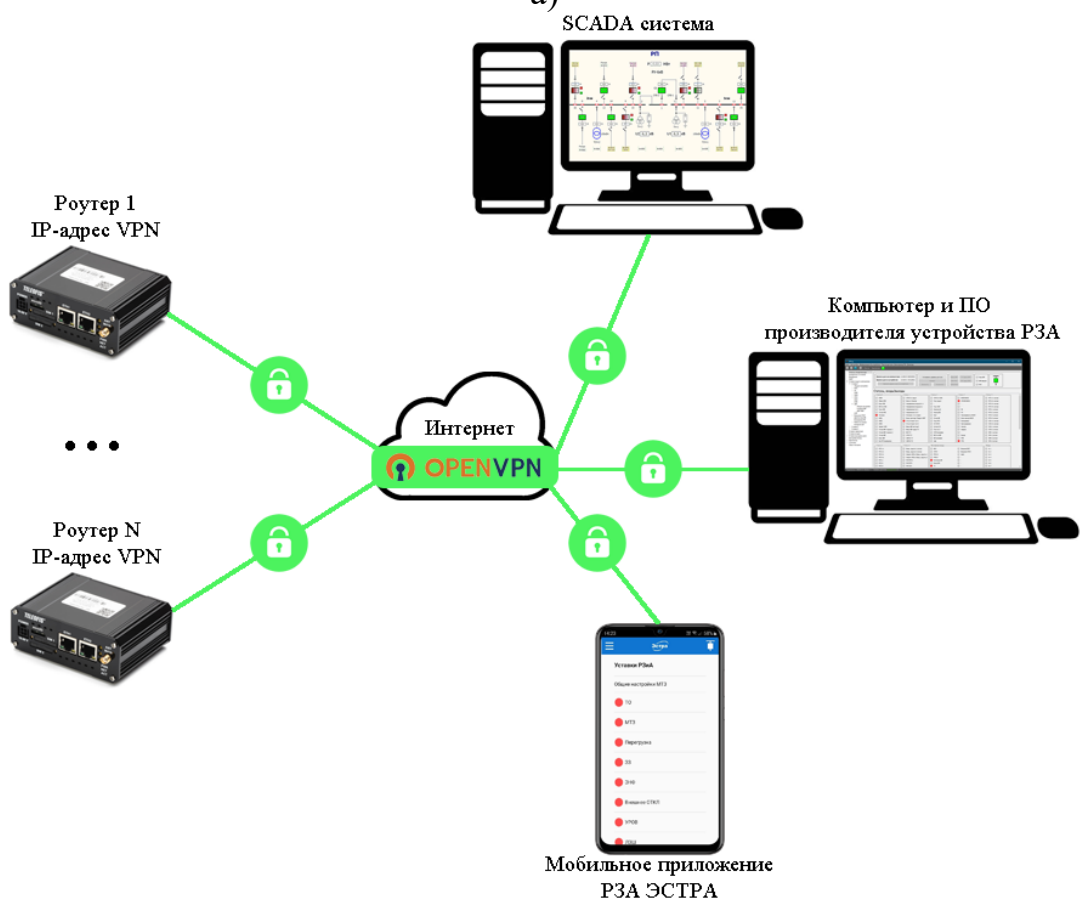
- Открытый канал. Стандартное подключение к удаленным устройствам.
- Защищенный канал с использованием технологии OpenVPN.

Основные плюсы использования технологии OpenVPN:

- Необходимо предоставить статический IP-адрес в сети интернет только одному устройству, которое будет выступать в роли VPN сервера.
- Минимизация рисков несанкционированного доступа к удаленным объектам.
- Зашифрованный канал связи.



а)



б)

Рис.23. а) структура сети без OpenVPN, б) структура сети с OpenVPN

В данном руководстве будет описан принцип настройки OpenVPN для устройств:

- TELEOFIS RTU968 V2 – OpenVPN сервер (статический IP-адрес)
- TELEOFIS RTU968 V1 – OpenVPN клиент
- персональный компьютер (ПК) с операционной системой (ОС) Windows 10 – OpenVPN клиент

В качестве OpenVPN сервера выступает один из роутеров, значит ему необходим статический IP-адрес, предоставляемый сотовым оператором.

3.9.1. Создание ключей и сертификатов

3.9.1.1. ОС Windows 10

OpenVPN можно скачать с [официального сайта](#).

!Важно. В данном руководстве будет представлена инструкция создания ключей и сертификатов с использованием [easyRSA 2](#). Для этого необходимо использовать OpenVPN версии 2.4.*, например [OpenVPN 2.4.12](#).

После скачивания OpenVPN, во время установки необходимо установить галочку «EasyRSA 2 Certificate Management Scripts» (рисунок 24).

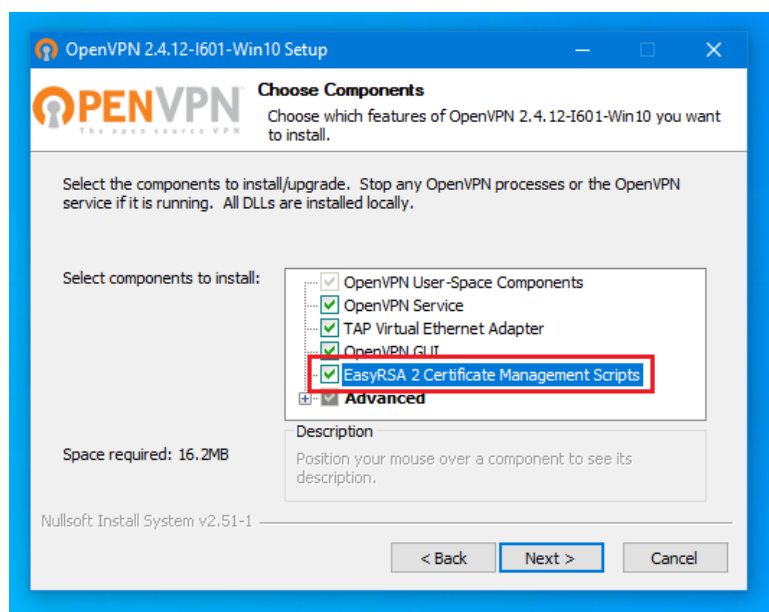


Рис.24. EasyRSA 2 Certificate Management Scripts

Каталог установки по умолчанию: C:\Program Files\OpenVPN. В данном руководстве будет происходить настройка, исходя из того, что путь установки не изменился. Если вы меняете каталог установки, необходимо использовать этот путь в дальнейших операциях описанных в этом руководстве.

Последовательность создания ключей и сертификатов:

Перейдите в каталог easy-rsa в каталоге OpenVPN (рисунок 25).

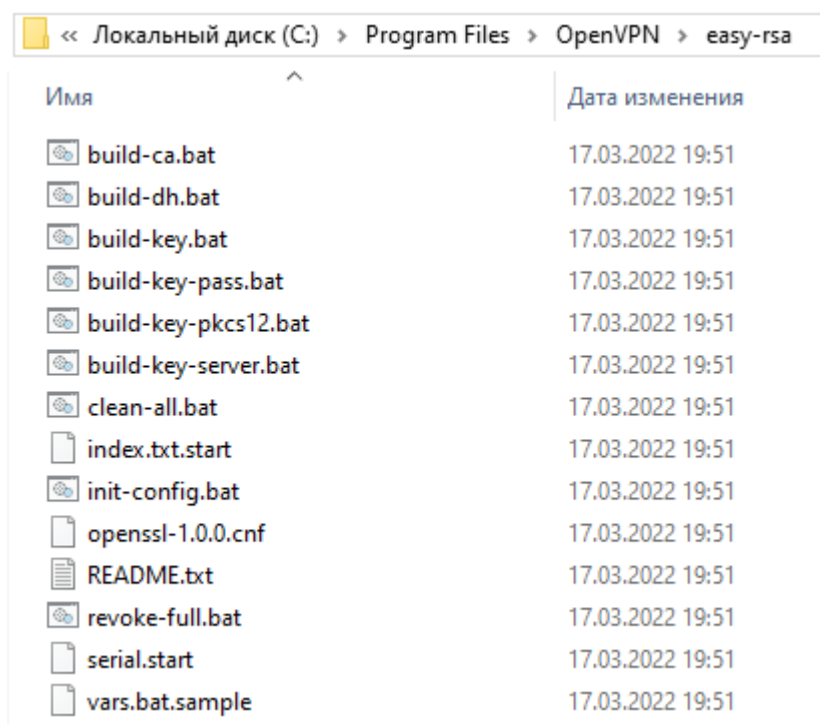


Рис.25. Каталог easy-rsa

Запустите командную строку от имени администратора и перейдите в каталог easy-rsa (рисунок 26).

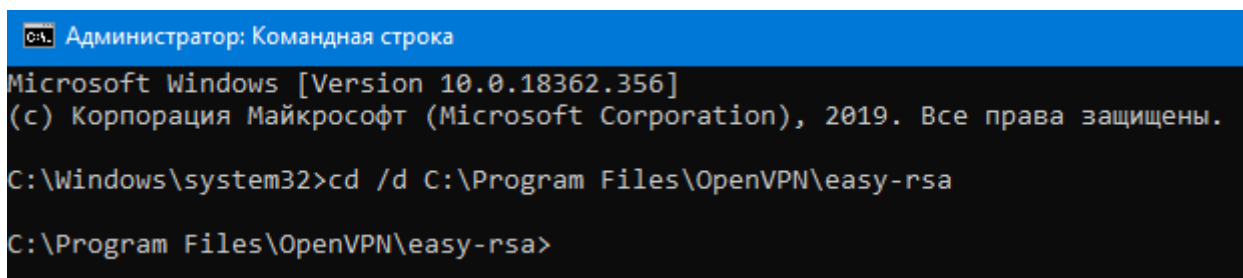


Рис.26. Каталог easy-rsa в командной строке

- Выполните команду init-config.bat в командной строке (рисунок 27).

```

C:\Program Files\OpenVPN\easy-rsa>init-config.bat
C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
Скопировано файлов:          1.
C:\Program Files\OpenVPN\easy-rsa>_

```

Рис.27. Выполнение команды init-config.bat

В результате выполнения команды будет создан файл vars.bat.

Открываем файл vars.bat любым текстовым редактором:

- находим строчку `rem set "PATH=%PATH%;C:\Program Files\OpenVPN\bin"` и удаляем слово `rem` (рисунок 28)
- переходим в конец файла и вносим свои параметры, например, рисунок 29 (там, где «changeme» – оставляем это значение)

```

1  @echo off
2  rem Edit this variable to point to
3  rem the openssl.cnf file included
4  rem with easy-rsa.
5
6  rem Automatically set PATH to openssl.exe
7  FOR /F "tokens=2*" %a IN ('REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN") DO set "PATH=%PATH%;%b\bin"
8
9  rem Alternatively define the PATH to openssl.exe manually
10 set "PATH=%PATH%;C:\Program Files\OpenVPN\bin"

```

Рис.28. Удаление rem

```

40 set KEY_COUNTRY=RU
41 set KEY_PROVINCE=NSK
42 set KEY_CITY=NSK
43 set KEY_ORG=ESTRA
44 set KEY_EMAIL=service@rza-estra.ru
45 set KEY_CN=changeme
46 set KEY_NAME=changeme
47 set KEY_OU=changeme
48 set PKCS11_MODULE_PATH=changeme
49 set PKCS11_PIN=123454321

```

Рис.29. Параметры в конце файла vars.bat

Сохраняем файл vars.bat.

Открываем файл openssl-1.0.0.cnf и ищем строку «default_days». Если данное значение равно 365, то меняем на 3650 и сохраняем файл.

Возвращаемся в командную строку и выполняем последовательно две команды (рисунок 30):

- vars

Создаем сертификат и ключ сервера. Выполнить команду: build-key-server server. На все вопросы ждем Enter, но, в конце будет 2 вопроса: «Sign the certificate?» и «1 out of 1 certificate requests certified, commit?» на них необходимо ответить «Y», рисунок 33.

```
C:\Program Files\OpenVPN\easy-rsa>build-key-server server
Ignoring -days; not generating a certificate
Generating a RSA private key
.....
.....
writing new private key to 'keys\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]:
State or Province Name (full name) [NSK]:
Locality Name (eg, city) [NSK]:
Organization Name (eg, company) [ESTRA]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:
Name [changeme]:
Email Address [service@rza-estra.ru]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'RU'
stateOrProvinceName  :PRINTABLE:'NSK'
localityName         :PRINTABLE:'NSK'
organizationName     :PRINTABLE:'ESTRA'
organizationalUnitName:PRINTABLE:'changeme'
commonName           :PRINTABLE:'changeme'
name                 :PRINTABLE:'changeme'
emailAddress         :IA5STRING:'service@rza-estra.ru'
Certificate is to be certified until Mar 25 05:12:02 2032 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>_
```

Рис.33. Создание сертификата и ключа сервера

Создадим сертификат и ключ для роутера, который выступает клиентом. Подадим команду: build-key router1 (!Важно. router1 – уникальное имя внутри одной OpenVPN сети для каждого клиента. Вы можете задать любое наименование). На все вопросы отвечаем Enter, но не торопимся, на вопрос «Common Name (eg, your name or your server's hostname)» отвечаем router1 (или то наименование, которое вы задали при подаче команды: build-key). А в конце будут два вопроса: «Sign the certificate?» и «1 out of 1 certificate requests certified, commit?» на них необходимо ответить «Y», рисунок 34.

```
C:\Program Files\OpenVPN\easy-rsa>build-key router1
Ignoring -days; not generating a certificate
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'keys\router1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]:
State or Province Name (full name) [NSK]:
Locality Name (eg, city) [NSK]:
Organization Name (eg, company) [ESTRA]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:router1
Name [changeme]:
Email Address [service@rza-estra.ru]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'RU'
stateOrProvinceName :PRINTABLE:'NSK'
localityName      :PRINTABLE:'NSK'
organizationName  :PRINTABLE:'ESTRA'
organizationalUnitName:PRINTABLE:'changeme'
commonName        :PRINTABLE:'router1'
name              :PRINTABLE:'changeme'
emailAddress       :IA5STRING:'service@rza-estra.ru'
Certificate is to be certified until Mar 25 05:21:18 2032 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

Рис.34. Создание сертификата и ключа для роутера

По алгоритму, описанному выше, создадим сертификат и ключ для компьютера: build-key computer1 (рисунок 35).

```
C:\Program Files\OpenVPN\easy-rsa>build-key computer1
Ignoring -days; not generating a certificate
Generating a RSA private key
.....++++
writing new private key to 'keys\computer1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [RU]:
State or Province Name (full name) [NSK]:
Locality Name (eg, city) [NSK]:
Organization Name (eg, company) [ESTRA]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:computer1
Name [changeme]:
Email Address [service@rza-estra.ru]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'RU'
stateOrProvinceName  :PRINTABLE:'NSK'
localityName         :PRINTABLE:'NSK'
organizationName     :PRINTABLE:'ESTRA'
organizationalUnitName:PRINTABLE:'changeme'
commonName           :PRINTABLE:'computer1'
name                 :PRINTABLE:'changeme'
emailAddress         :IASSTRING:'service@rza-estra.ru'
Certificate is to be certified until Mar 25 05:26:28 2032 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

Рис.35. Создание сертификата и ключа для компьютера

Теперь перейдем с помощью проводника в каталог easy-rsa, рисунок 36.

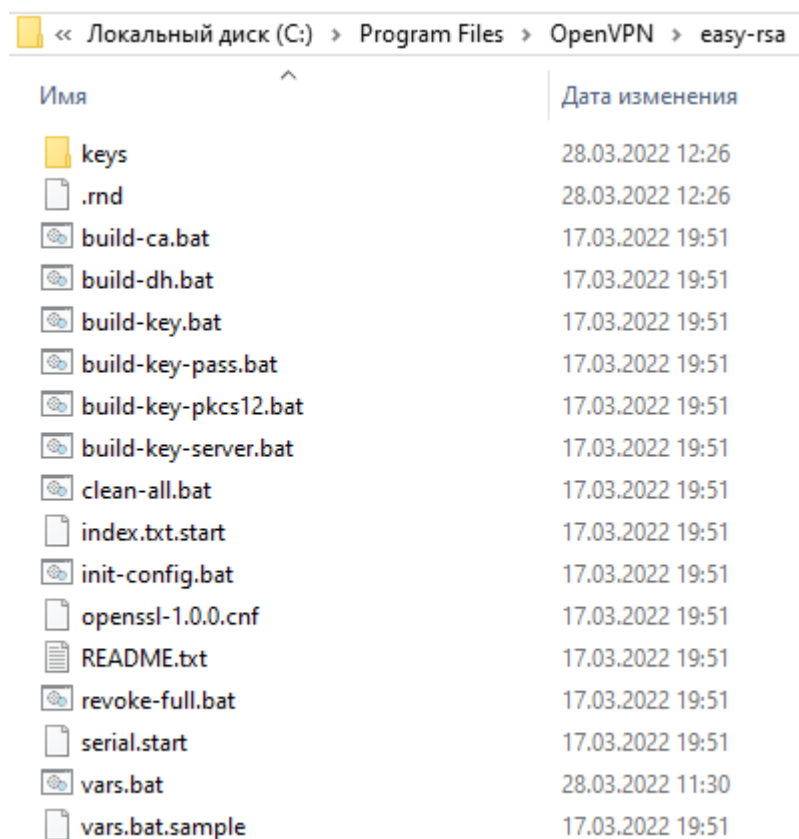


Рис.36. Каталог easy-rsa после создания ключей и сертификатов

В каталоге keys расположены все сертификаты и ключи, созданные нами. Создадим 3 каталога (для роутера-сервера, роутера-клиента и компьютера-клиента) и поместим туда необходимые файлы, рисунок 37.

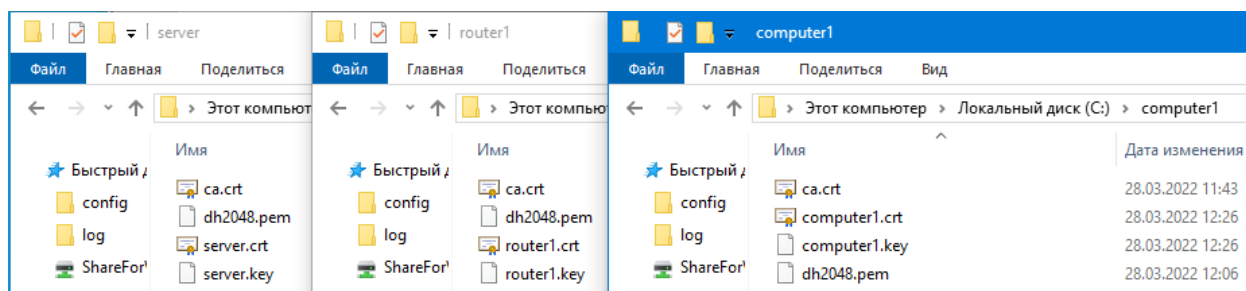


Рис.37. Каталоги для каждого хоста OpenVPN сети.

!Важно. Для таких клиентов как компьютер или смартфон необходимо создать еще один файл *.ovpn, чтобы программа OpenVPN могла правильно считать и использовать созданные нами сертификаты и ключи. Создадим такой файл для computer1. Назовем файл config.ovpn и поместим в каталог с сертификатом и ключом для computer1, рисунок 38.

Имя	Дата изменения
ca.crt	28.03.2022 11:43
computer1.crt	28.03.2022 12:26
computer1.key	28.03.2022 12:26
config.ovpn	28.03.2022 12:42
dh2048.pem	28.03.2022 12:06

Рис.38. Каталог для клиента computer1

Теперь откроем файл config.ovpn с помощью любого текстового редактора и внесем данные, рисунок 39.

```

client
dev tun
proto udp
remote 213.87.115.134 Статический IP-адрес OpenVPN сервера
resolv-retry infinity
nobind
persist-key
persist-tun
ca ca.crt
cert computer1.crt Наименование файла сертификата
key computer1.key Наименование файла ключа
dh dh2048.pem Наименование файла ключа Деффи-Хелмана
tls-client
float
keepalive 10 120
comp-lzo
verb 0

```

Рис.39. Содержание файла config.ovpn

3.9.2. Создание OpenVPN сервера

В данном руководстве будет описано создание OpenVPN сервера на базе 3G роутера TELEOFIS RTU968 V2. Вы можете сделать сервер как на другом роутере с поддержкой OpenVPN и наличием статического IP-адреса, так и на компьютере со статическим IP-адресом.

Подключаемся к роутеру через [Веб-интерфейс](#). Переходим на страничку Сервисы -> OpenVPN. Создадим новый процесс OpenVPN:

- наименование: ESTRAvpnServer
- тип: Server configuration for a routed multi-client VPN

И нажимаем кнопку «Добавить» (рисунок 40).

Процессы OpenVPN

Список настроенных процессов OpenVPN и их текущее состояние



Включить	Запущено	Старт/Стоп	Порт	Протокол
Эта секция пока не содержит значений				
ESTRAvpnServer	Server configuration for a routed	 Добавить		
			Сохранить и применить	Сохранить Сбросить

Рис.40. Добавить процесс OpenVPN (Сервер)

После этого загрузится страничка основных настроек. Нажмите на расширенные настройки «Switch to advanced configuration» (рисунок 41).

Обзор » Процесс "ESTRAvpnServer"

Switch to advanced configuration

verb 

Установить уровень вывода

tun_ipv6 Включить поддержку IPv6 для устройства tun

Рис.41. Расширенные настройки

Выбираем категорию конфигурации: Service (рисунок 42).

Обзор » Процесс "ESTRAvpnServer"

Switch to basic configuration

Категория конфигурации: Service | Networking | VPN | Cryptography

Рис.42. Категория конфигурации: Service

Добавляем параметр log. Для этого нажимаем на «-- Дополнительное поле --», выбираем в списке «log» и нажимаем кнопку «Добавить» (рисунок 43). После этого данный параметр появится в списке, нажимаем кнопку «Сохранить» (рисунок 44).

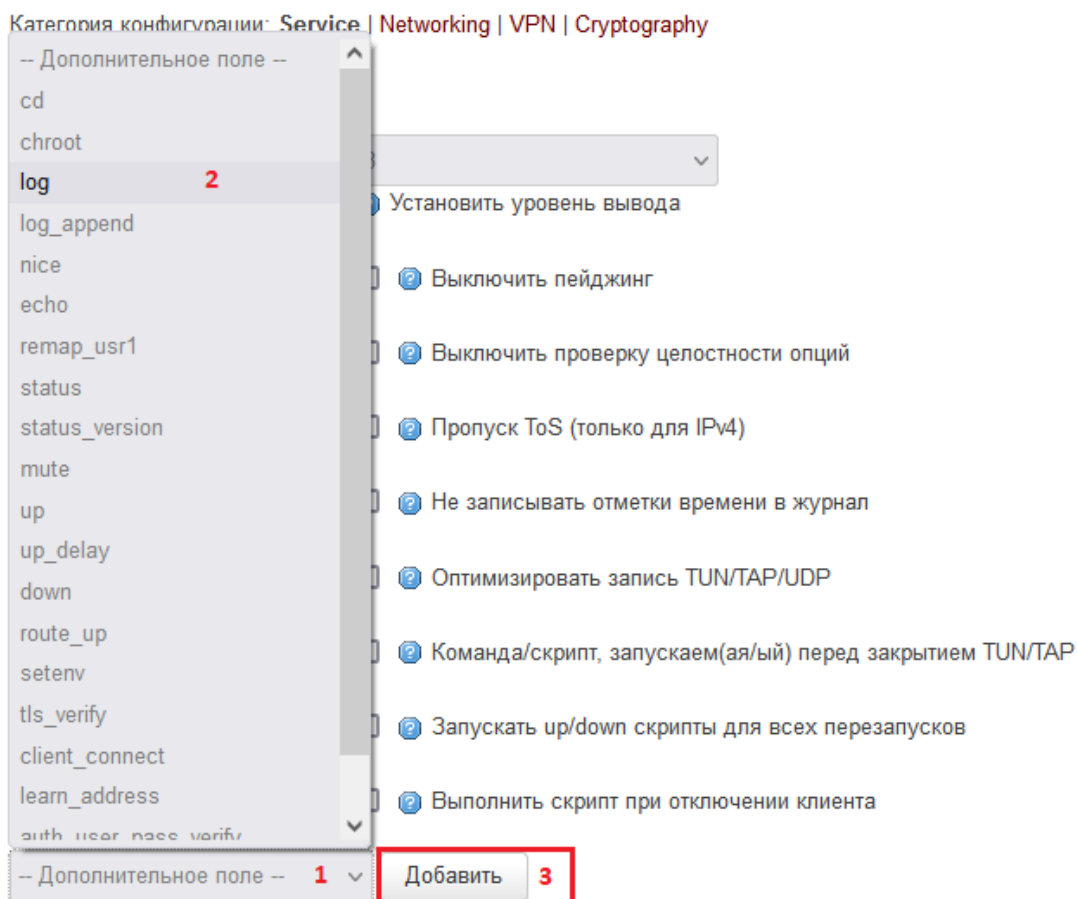


Рис.43. Добавить параметр «log»

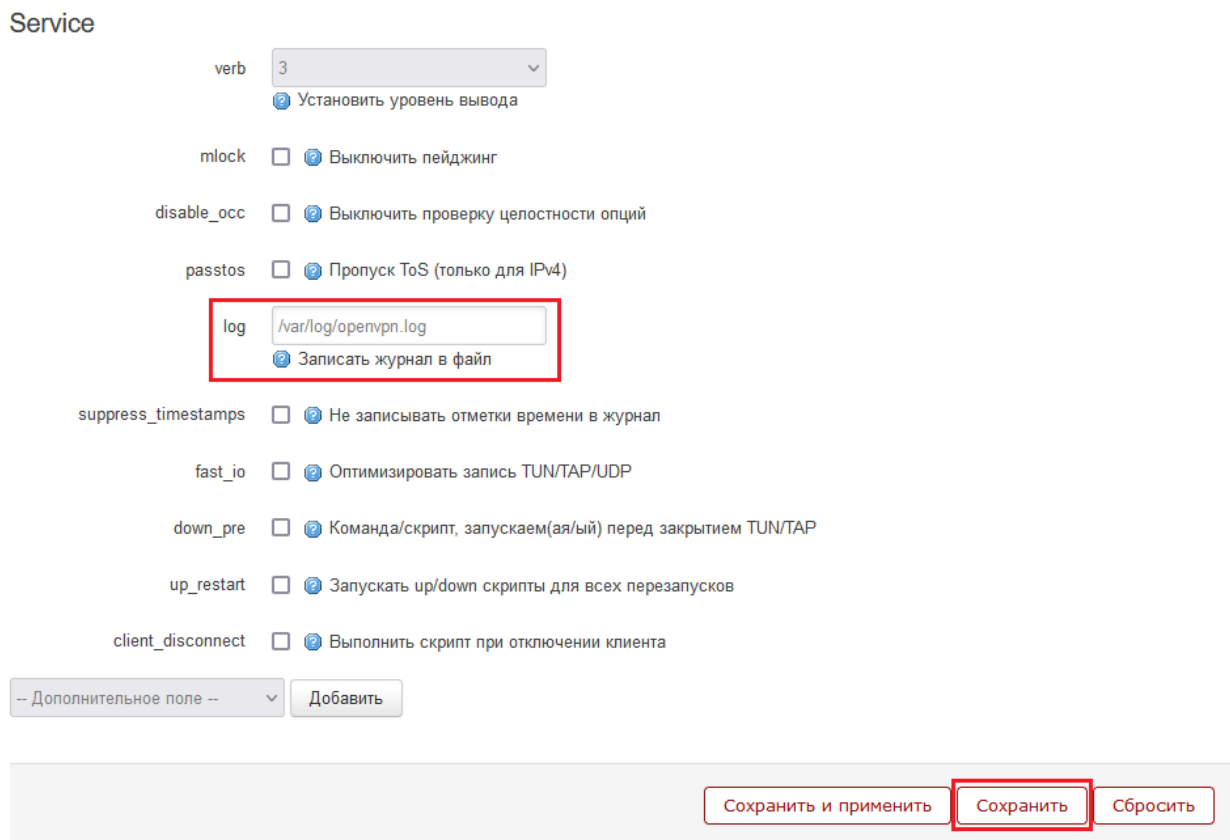


Рис.44. Сохранения параметров конфигурации Service

Переходим в категорию конфигурации Networking.

- Добавляем параметр «topology» и устанавливаем значение «subnet»
- Добавляем параметр «port» и устанавливаем порт (по умолчанию 1194)
- Остальные параметры настраиваются по необходимости

После этого нажимаем кнопку сохранить (рисунок 45).

Обзор » Процесс "ESTRAvpnServer"

Switch to basic configuration

Категория конфигурации: Service | Networking | VPN | Cryptography

Networking

port 1194
Номер локального и удалённого TCP/UDP порта

...

persist_remote_ip Не изменять удалённый IP-адрес при перезапуске

management_query_passwords Запросить канал управления для закрытого ключа

management_hold Запустить OpenVPN в спящем режиме

topology subnet
'net30', 'p2p' или 'subnet'

-- Дополнительное поле -- Добавить

Сохранить и применить Сохранить Сбросить

Рис.45. Настройки конфигурации Networking

Переходим в категорию конфигурации: VPN

Устанавливаем параметры нашей VPN сети (параметры сервера), например, 10.0.100.0 255.255.255.0 (рисунок 46). В таком случае имеем пул IP-адресов 10.0.100.1-10.0.100.255, где 10.0.100.1 – OpenVPN сервер.

server 10.0.100.0 255.255.255.0
Настроить режим сервера

Рис.46. Параметры VPN сети

Разрешаем клиентам обмен сообщениями между собой (рисунок 47)

client_to_client Разрешить общение клиентов друг с другом

Рис.47. Разрешение общения клиентов друг с другом

Добавляем параметр «ifconfig_pool_persist», оставляем в нем параметр по умолчанию: /etc/openvpn/ipp.txt 600.

Остальные параметры задаются опционально.

Нажимаем кнопку «Сохранить».

/etc/openvpn/ipp.txt – это путь к файлу, где будут указаны IP-адреса каждому клиенту. Необходимо создать этот файл, для этого с помощью программы WinSCP [подключимся к файловой системе роутера](#). Перейдем в каталог /etc/openvpn/ и создадим файл ipp.txt (рисунок 48, 49).

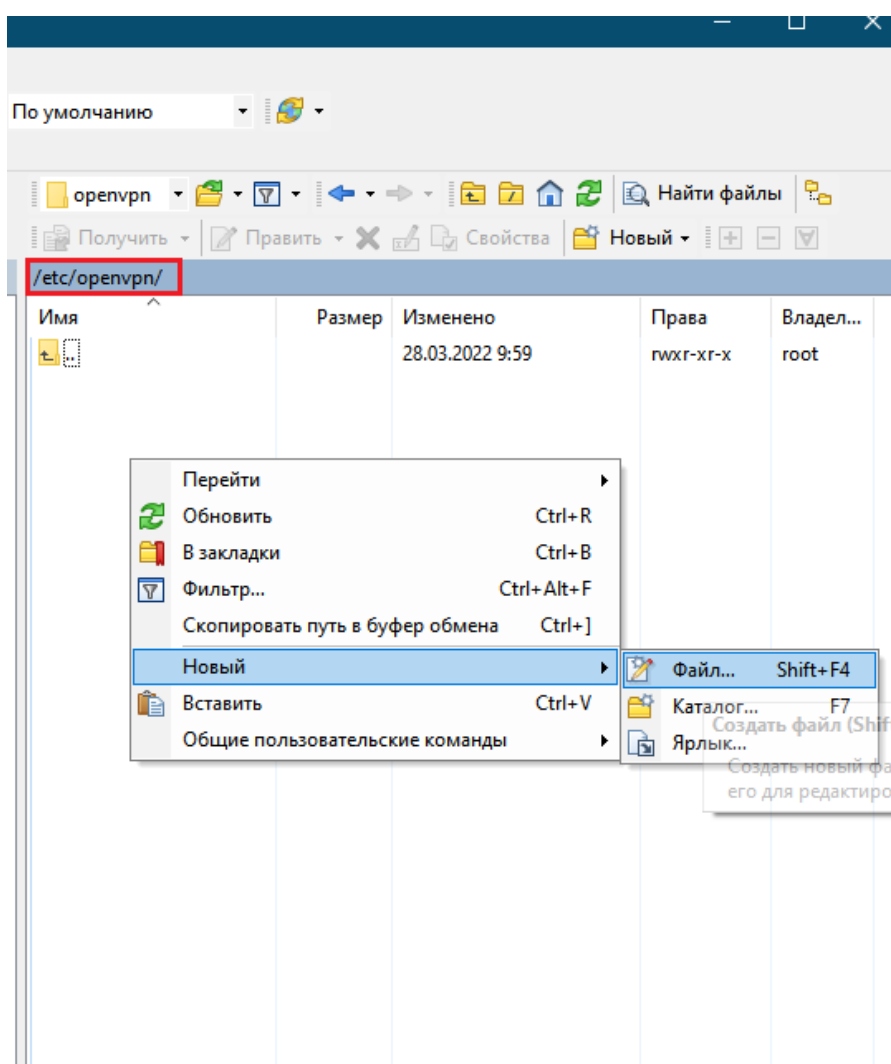


Рис.48. Создать файл ipp.txt на роутере

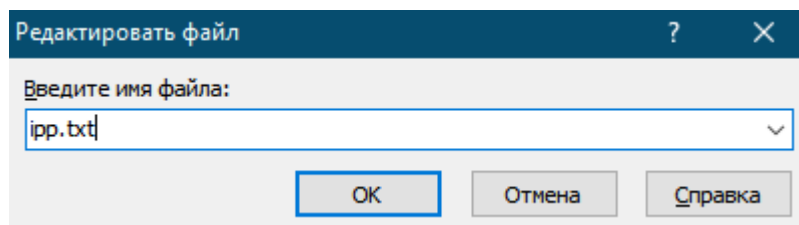


Рис.49. Имя файла ipp.txt

В файл записываем IP адреса для каждого клиента (имя клиента,IP-адрес), нажимаем кнопку «Сохранить» и закрываем окно редактирования, рисунок 50.

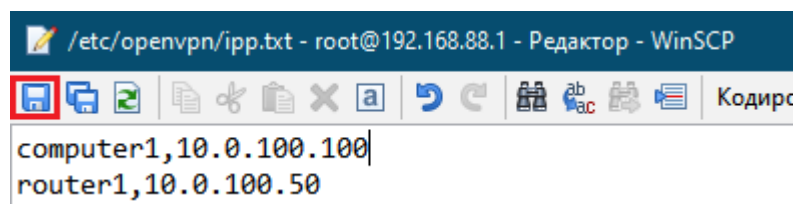


Рис.50. IP-адреса для каждого клиента

После этого программу WinSCP можно закрыть. Возвращаемся к Веб-интерфейсу роутера, для дальнейшей настройки.

Переходим в категорию конфигурации: Cryptography

Используем созданные файлы в пункте 3.9.1 для сервера:

- Добавляем и устанавливаем центр сертификации CA
- Добавляем и устанавливаем ключ Деффи-Хелмана
- Добавляем и устанавливаем сервисный сертификат server.crt
- Добавляем и устанавливаем сервисный ключ server.key
- Устанавливаем галочку `ssl_server`
- Остальные параметры задаются опционально

Нажимаем кнопку «Сохранить и применить» (рисунок 51).

Cryptography

[?](#) Отключить проверку повторов

[?](#) Заглушить вывод предупреждений повторов

[?](#) Выключить вектор инициализации шифра

[?](#) Включить TLS в режиме сервера

ca
[?](#) Центр сертификации

dh
[?](#) Параметры алгоритма DH

cert
[?](#) Локальный сертификат

key
[?](#) Локальный секретный ключ

[?](#) Разрешить только одну сессию

[?](#) Выйти при ошибке согласования TLS

[?](#) Не кешировать пароли --askpass или --auth-user-pass

Рис.51. Параметры категории конфигурации Cryptography

Переходим в основное окно OpenVPN. Ставим галочку «Включить», нажимаем кнопку «Сохранить и применить» и запускаем сервер (рисунок 52).

OpenVPN

Процессы OpenVPN

Список настроенных процессов OpenVPN и их текущее состояние

	Включить	Запущено	Старт/Стоп	Порт	Протокол	
ESTRAvpnServer	<input checked="" type="checkbox"/> 1	нет	3 <input type="button" value="start"/>	1194	udp	<input type="button" value="Редактировать"/> <input type="button" value="Удалить"/>
	<input type="text"/>	Empty client configuration	<input type="button" value="Добавить"/>			

Рис.52. Запускаем OpenVPN сервер

Переходим на страничку Сеть -> Интерфейсы и создаем новый интерфейс, рисунок 53.

Интерфейсы

Обзор интерфейса

Сеть	Состояние	Действия
LAN br-lan	Время работы: 2h 15m 18s MAC-адрес: F8:1D:78:81:27:7B RX: 833.59 КВ (7379 Пакетов.) TX: 2.40 МВ (7855 Пакетов.) IPv4: 192.168.88.1/24 IPv6: fd32:222:7789::1/60	<input type="button" value="Соединить"/> <input type="button" value="Остановить"/> <input type="button" value="Редактиров"/> <input type="button" value="Удалить"/>
INTERNET 3g-internet	Время работы: 2h 14m 29s RX: 26.05 МВ (48329 Пакетов.) TX: 25.70 МВ (46163 Пакетов.) IPv4: 213.87.115.134/32	<input type="button" value="Соединить"/> <input type="button" value="Остановить"/> <input type="button" value="Редактиров"/> <input type="button" value="Удалить"/>

Рис.53. Добавить новый интерфейс

Задаем наименование, тип протокола «неуправляемый» и включаем интерфейс tun0 (если tun0 нет в списке, то выбираем пользовательский интерфейс и пишем tun0) рисунок 54.

Создать интерфейс

Имя нового интерфейса:
 Допустимые символы: A-Z, a-z, 0-9 и _

Note: interface name length
 Maximum length of the name is 15 characters including the automatic protocol/bridge prefix (br-, 6in4-, pppoe- etc.)

Протокол нового интерфейса:

Создать мост над несколькими интерфейсами:

Включить следующий интерфейс

- Ethernet-адаптер: "eth0" (lan)
- Ethernet-адаптер: "eth1" (lan)
- Ethernet-адаптер: "gretap0"
- Ethernet-адаптер: "ip6gre0"
- Ethernet-адаптер: "ip6tnl0"
- Ethernet-адаптер: "teql0"
- Ethernet-адаптер: "tun0"
- Ethernet-адаптер: "tunl0"
- Ethernet-адаптер: "usb0" (lan)
- Пользовательский интерфейс:

Рис.54. Создание нового интерфейса

Нажимаем кнопку «Применить». После этого загрузится страничка «Основные настройки». Переходим на страничку

«дополнительные/расширенные настройки» и устанавливаем галочку «Запустить при загрузке», рисунок 55. Нажимаем кнопку «Сохранить».

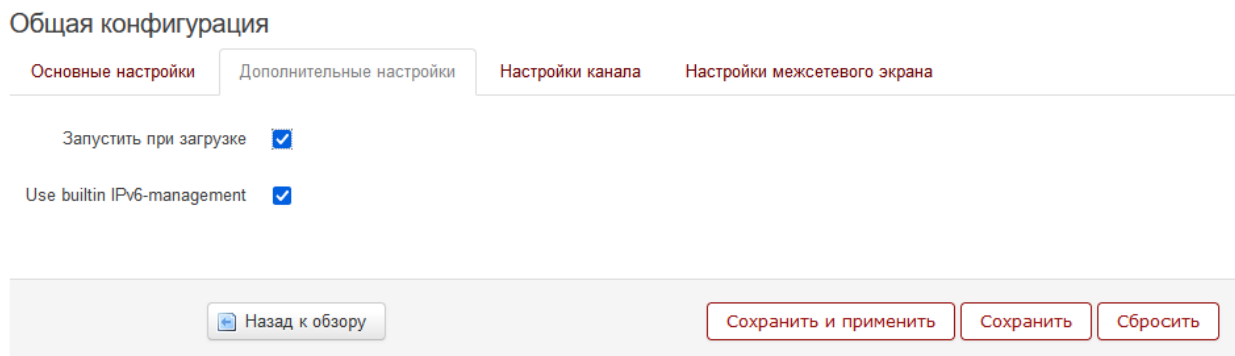


Рис.55. Дополнительные настройки

Переходим на вкладку «Настройки межсетевого экрана». Создаем зону сетевого экрана, рисунок 56. Нажимаем кнопку «Сохранить и применить»

Интерфейсы - VPN

На этой странице вы можете настроить сетевые интерфейсы. Вы можете объединить несколько интерфейсов в мост, выбрав опцию "Объединить в мост" и введя список интерфейсов, разделенных пробелами. Вы также можете использовать VLAN-обозначения вида ИНТЕРФЕЙС.НОМЕРVLAN (напр.: eth0.1).

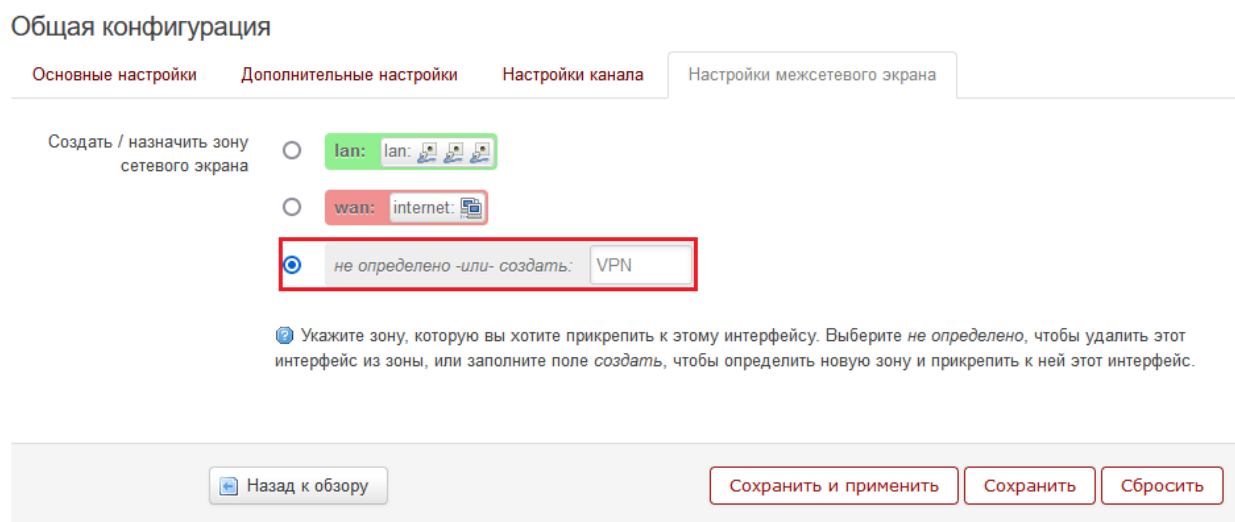


Рис.56. Настройка межсетевого экрана

Переходим в раздел Сеть -> Межсетевой экран. Переходим в Редактирование VPN, рисунок 57.

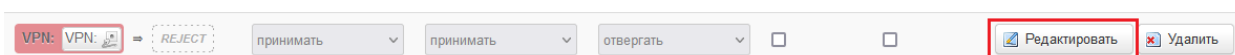


Рис.57. Редактировать VPN

Устанавливаем параметры в соответствии с рисунком 58 и нажимаем кнопку «Сохранить и применить».

Основные настройки | **Дополнительные настройки**

Имя:

Входящий:

Исходящий:

Перенаправление:

Маскарадинг

Ограничение MSS:

Использовать сети: VPN:

internet:

lan:

создать:

Перенаправление между зонами

Данные настройки управляют перенаправлением между этой (VPN) и другими зонами. Трафиком *зон-получателей* является трафик **исходящий** из "VPN". Трафиком *зон-источников* является трафик **направленный в "VPN"**. Перенаправление является *однонаправленным*, то есть перенаправление из lan в wan *не* допускает перенаправление трафика из wan в lan.

Разрешить перенаправление в зоны назначения:

lan: lan:

wan: internet:

Разрешить перенаправление из зон-источников:

lan: lan:

wan: internet:

Рис.58. Параметры межсетевого экрана зоны VPN

Переходим на вкладку «Правила для трафика» и открываем порт для VPN соединения. Вносим параметры и нажимаем «Добавить», рисунок 59

Открыть порты на маршрутизаторе:

Имя	Протокол	Внешний порт	
<input type="text" value="VPN"/>	TCP+UDP <input type="text" value="v"/>	<input type="text" value="1194"/>	<input type="button" value="Добавить"/>

Рис.59. Открыть порт для VPN

После этого порт появится в списке. С помощью стрелочки «вверх» необходимо переместить этот порт наверх, рисунок 60 и нажать кнопку «Сохранить и применить».

Правила для трафика

















Имя	Выбирать	Действие	Включить	Сортировка	
VPN	Любой TCP, UDP Из <i>любого хоста</i> в wan К <i>любой IP-адрес маршрутизатора</i> , порту port 1194 на этом устройстве	Accept input	<input checked="" type="checkbox"/>	 	 Редактировать  Удалить
Allow-DHCP-Renew	IPv4-UDP Из <i>любого хоста</i> в wan К <i>любой IP-адрес маршрутизатора</i> , порту port 68 на этом устройстве	Accept input	<input checked="" type="checkbox"/>	 	 Редактировать  Удалить
Allow-Ping	IPv4-ICMP с типе echo-request Из <i>любого хоста</i> в wan К <i>любой IP-адрес маршрутизатора</i> на этом устройстве	Accept input	<input checked="" type="checkbox"/>	 	 Редактировать  Удалить
Allow-IGMP	IPv4-IGMP Из <i>любого хоста</i> в wan К <i>любой IP-адрес маршрутизатора</i> на этом устройстве	Accept input	<input checked="" type="checkbox"/>	 	 Редактировать  Удалить

Рис.60. Порт VPN

Переходим на страничку Сеть -> Интерфейсы и проверяем, что интерфейсу VPN выдан IP-адрес, рисунок 61.






Сеть	Состояние	Действия
VPN  tun0	Время работы: 0h 4m 37s MAC-адрес: 00:00:00:00:00:00 RX: 0.00 B (0 Пакетов.) TX: 0.00 B (0 Пакетов.) IPv4: 10.0.100.1/24	 Соединить  Остановить  Редактиров  Удалить

Рис.61. Проверка IP-адреса интерфейса VPN

Если IP-адрес не выдан, необходимо перейти на страничку Сервисы -> OpenVPN и перезапустить OpenVPN: stop/start. После этого перейти на страничку Сеть -> Интерфейсы и при необходимости перезапустить интерфейс.

3.9.3. Создание OpenVPN клиентов

В данном разделе будут описаны процедуры создания OpenVPN клиентом на базе 3G роутера TELEOFIS RTU968 v1 и персонального компьютера с операционной системой Windows 10.

3.9.3.1. OpenVPN клиент TELEOFIS RTU968

Подключаемся к роутеру через [Веб-интерфейс](#). Переходим на страничку Сервисы -> OpenVPN. Создадим новый процесс OpenVPN:

- наименование: ESTRAvpnClient
- тип: Client configuration for a routed multi-client VPN

И нажимаем кнопку «Добавить» (рисунок 62).

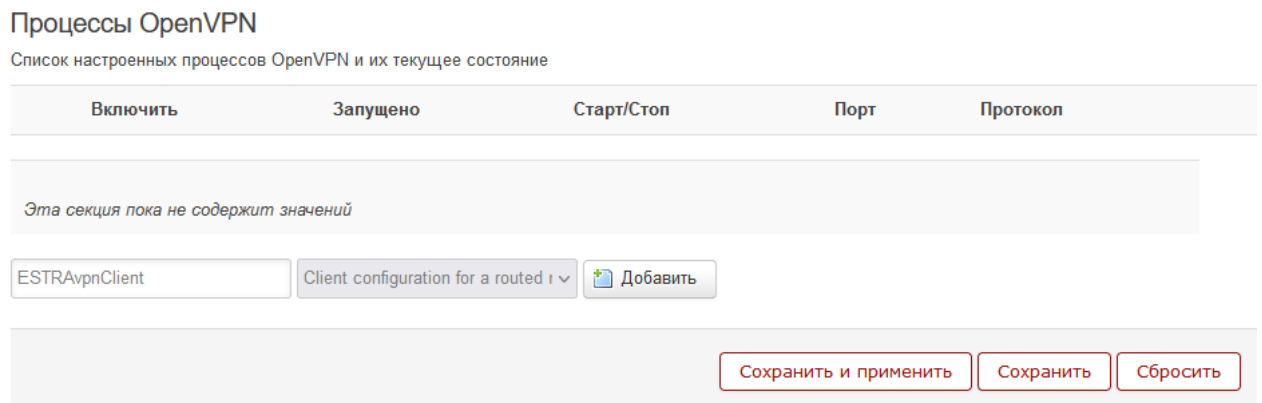


Рис.62. Создание OpenVPN клиента

После это загрузится страничка настроек нового процесса OpenVPN. Необходимо перейти к расширенным настройкам (Switch to advanced configuration), рисунок 63.

Обзор » Процесс "ESTRAvpnClient"

[Перейти к расширенным настройкам](#)

verb

3

[Установить уровень вывода](#)

Рис.63. Переход к расширенным настройкам

Переходим к категории конфигурации Service, рисунок 64.

Обзор » Процесс "ESTRAvpnClient"

[Перейти к основным настройкам](#)

Категория конфигурации: **Service** | Networking | VPN | Cryptography

Рис.64. Категория конфигураций Service

Добавляем и устанавливаем параметр «log», рисунок 65.

log
[?](#) Записать журнал в файл

Рис.65. Параметр «log»

Нажимаем кнопку «Сохранить» и переходим к категории конфигурации Networking. Задаем основные параметры, в соответствии с рисунком 66.

port
[?](#) Номер локального и удалённого TCP/UDP порта

float [?](#) Позволить удалённому хосту изменять IP-адрес или порт

nobind [?](#) Не выполнять привязку к локальному адресу и порту

dev
[?](#) устройство tun/tap

persist_tun [?](#) Не закрывать устройство tun/tap при перезапуске

persist_key [?](#) Не считывать заново ключ при перезапуске

Рис.66. Основные параметры категории конфигурации Networking

Нажимаем кнопку «Сохранить» и переходим к категории конфигурации VPN.

Устанавливаем основные параметры, в соответствии с рисунком 67.

Остальные параметры опциональные и зависят от настроек сервера.

client [?](#) Настроить режим клиента

pull [?](#) Принимать опции, отправленные с сервера


remote  **IP-адрес OpenVPN сервера**
[?](#) Имя удалённого хоста или IP-адрес

Рис.67. Основные параметры категории конфигурации VPN

Нажимаем кнопку «Сохранить» и переходим к категории конфигурации Cryptography. Используем файлы, которые были созданы для роутера в пункте [3.9.1](#) и устанавливаем параметры (рисунок 68):

- Добавляем центр сертификации CA
- Добавляем ключ Диффи-Хелмана
- Добавляем сертификат роутера router1.crt
- Добавляем ключ роутера router1.key
- В параметре remote_cert_tls выбираем server
- Активируем параметр tls_client

The image shows a configuration interface for the Cryptography category. At the top, the 'tls_client' parameter is checked with a blue checkmark and a help icon, with the text 'Включить TLS в режиме клиента'. Below this are four file upload sections, each with a label, a file size, and a help icon:

- ca**: Загруженный файл (2.40 KB), help icon, and 'Центр сертификации'.
- dh**: Загруженный файл (432.00 B), help icon, and 'Параметры алгоритма DH'.
- cert**: Загруженный файл (8.04 KB), help icon, and 'Локальный сертификат'.
- key**: Загруженный файл (3.25 KB), help icon, and 'Локальный секретный ключ'.

At the bottom, the 'remote_cert_tls' parameter is a dropdown menu currently showing 'server' with a downward arrow, and a help icon with the text 'Требовать явного использования ключа в сертификате'.

Рис.68. Основные настройки категории конфигурации Cryptography


Остальные параметры опциональные и настраиваются в зависимости от конфигурации сервера.

Нажимаем кнопку «Сохранить и применить».

Переходим к списку процессов OpenVPN. Устанавливаем галочку «Включить», нажимаем кнопку «Сохранить и применить» и запускаем процесс, рисунок 69.

Процессы OpenVPN

Список настроенных процессов OpenVPN и их текущее состояние

Включить	Запущено	Старт/Стоп	Порт	Протокол	
<input checked="" type="checkbox"/>	нет	 start	1194	udp	<input type="button" value="Редактировать"/> <input type="button" value="Удалить"/>

Empty client configuration

Рис.69. Запуск процесса OpenVPN клиент

Переходим на страничку Сеть -> Интерфейсы и создаем новый интерфейс, рисунок 70.

Обзор интерфейса

Сеть	Состояние	Действия
LAN br-lan	Время работы: 12h 7m 13s MAC-адрес: F8:1D:78:80:0D:67 RX: 1.29 MB (15328 Пакетов.) TX: 2.71 MB (10583 Пакетов.) IPv4: 192.168.88.1/24 IPv6: fd32:222:7789::1/60	<input type="button" value="Соединить"/> <input type="button" value="Остановить"/> <input type="button" value="Редактиров"/> <input type="button" value="Удалить"/>
INTERNET 3g-internet	Время работы: 12h 6m 44s RX: 2.06 MB (19646 Пакетов.) TX: 2.40 MB (21284 Пакетов.) IPv4: 100.70.176.11/32	<input type="button" value="Соединить"/> <input type="button" value="Остановить"/> <input type="button" value="Редактиров"/> <input type="button" value="Удалить"/>

Рис.70. Добавить новый интерфейс

Задаем наименование, тип протокола «неуправляемый» и включаем интерфейс tun0 (если tun0 нет в списке, то выбираем пользовательский интерфейс и пишем tun0) рисунок 71.

Создать интерфейс

Имя нового интерфейса
? Допустимые символы: A-Z, a-z, 0-9 и _

Note: interface name length ? Maximum length of the name is 15 characters including

Протокол нового интерфейса

Создать мост над несколькими интерфейсами

Включить следующий интерфейс

- Ethernet-адаптер: "eth0" (lan)
- Ethernet-адаптер: "eth1" (lan)
- Ethernet-адаптер: "gretap0"
- Ethernet-адаптер: "ip6gre0"
- Ethernet-адаптер: "ip6tnl0"
- Ethernet-адаптер: "teql0"
- Ethernet-адаптер: "tun0"
- Ethernet-адаптер: "tunl0"
- Пользовательский интерфейс:

Рис.71. Параметры добавляемого интерфейса

Нажимаем кнопку «Применить». После этого попадаем на страничку «Общая конфигурация». Переходим во вкладку «Расширенные настройки» и устанавливаем «Запустить при загрузке» и нажимаем кнопку «Сохранить», рисунок 72.

Запустить при загрузке

Use builtin IPv6-management

Рис.72. Расширенные настройки интерфейса

Переходим во вкладку «Настройки межсетевого экрана», создаем зону сетевого экрана (рисунок 73) и нажимаем кнопку «Сохранить и применить».

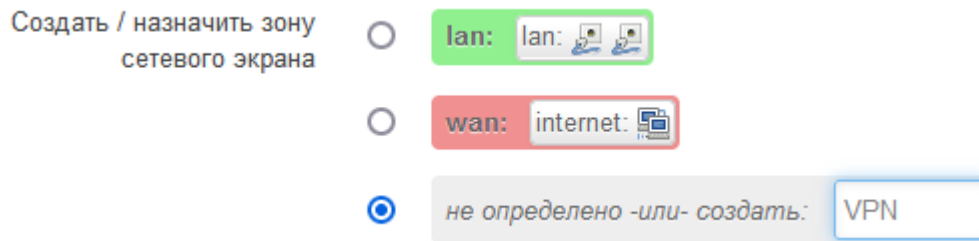


Рис.73. Создать зону сетевого экрана

Переходим на страничку Сеть -> Межсетевой экран. Переходим к редактированию созданного интерфейса, рисунок 74.

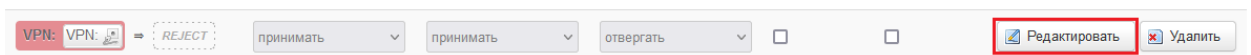
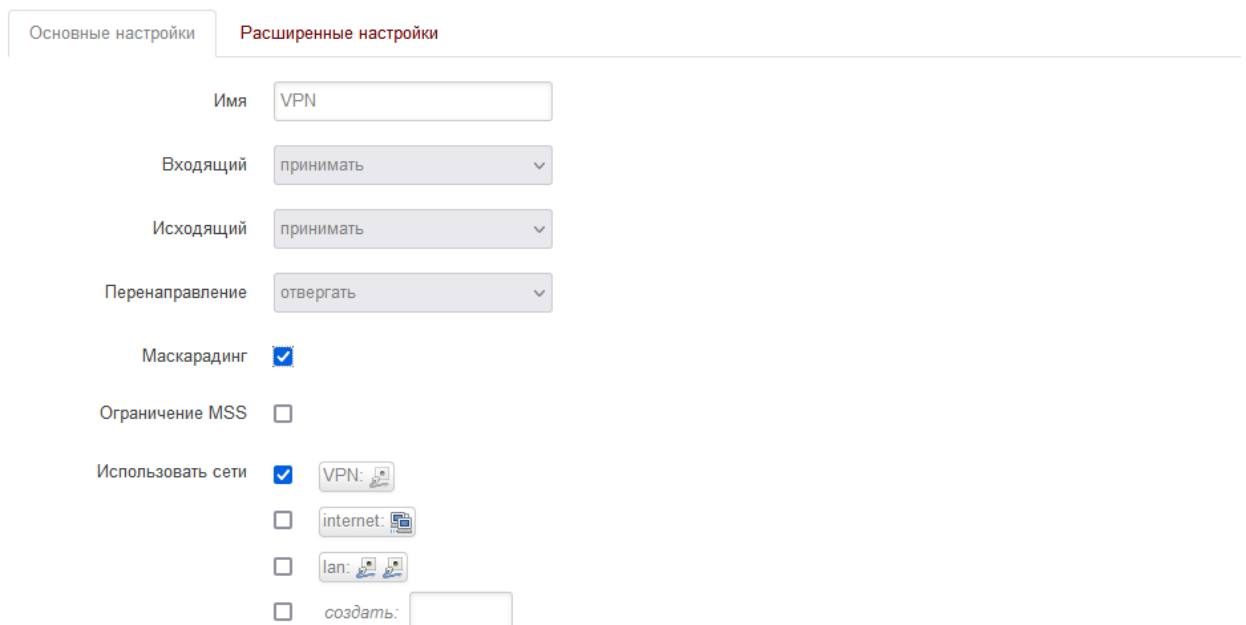


Рис.74. Редактировать интерфейс VPN

Устанавливаем настройки в соответствии с рисунком 75 и нажимаем кнопку «Сохранить и применить».



Перенаправление между зонами

Данные настройки управляют перенаправлением между этой (VPN) и другими зонами. Трафиком зон-получателей является трафик **исходящий** из "VPN". Трафиком зон-источников является трафик **направленный в "VPN"**. Перенаправление является **однаправленным**, то есть перенаправление из lan в wan не допускает перенаправление трафика из wan в lan.

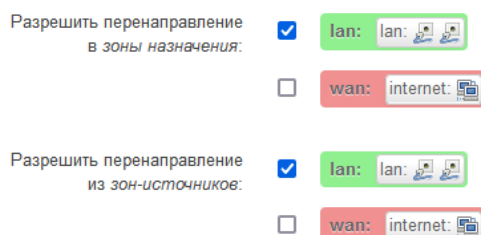


Рис.75. Параметры Зоны VPN

Переходим на страничку Сеть -> Интерфейсы и проверяем, что интерфейсу VPN выдан IP-адрес, рисунок 76.

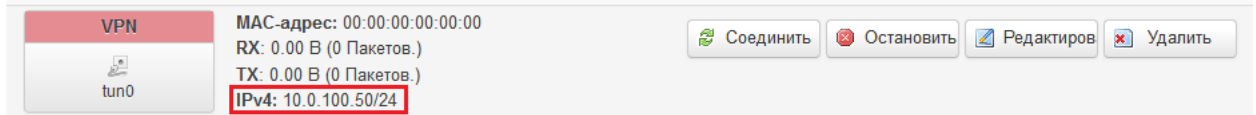


Рис.76. Проверка IP-адреса интерфейса VPN

Если IP-адрес не выдан, необходимо перейти на страничку Сервисы -> OpenVPN и перезапустить OpenVPN: stop/start. После этого перейти на страничку Сеть -> Интерфейсы и при необходимости перезапустить интерфейс.

3.9.3.2. OpenVPN клиент ПК ОС Windows 10

Копируем файлы, созданные в пункте 3.9.1 для компьютера, в каталог C:\Users\host\OpenVPN\config (по умолчанию), рисунок 77.

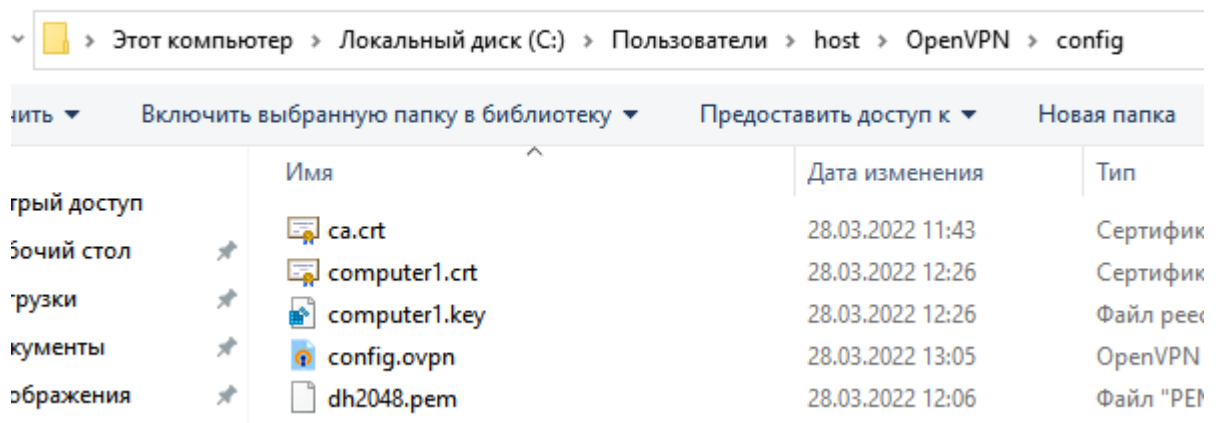


Рис.77. Фалы OpenVPN для персонального компьютера.

После этого подключаемся к OpenVPN сервер:

Запускаем программу OpenVPN GUI

В «трее» находим OpenVPN, нажимаем правой кнопкой мыши и выбираем «Подключиться» (рисунок 78).

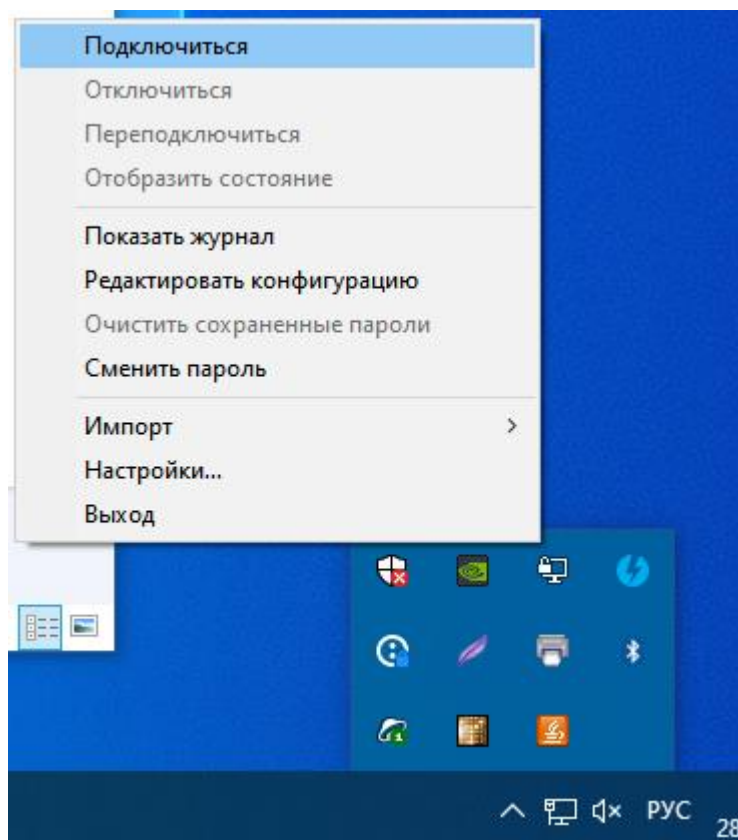


Рис.78. Запуск OpenVPN на Windows 10

После это на экране появится окно подключения, а после успешного подключения, в правом нижнем углу появится сообщение об успешном подключении к OpenVPN серверу.

3.10. Изменение/отключение тестовых серверов для «пинга»

Роутеры TELEOFIS по умолчанию настроены на периодическую проверку связи с помощью «пинга» тестовый сервером (8.8.8.8/8.8.4.4). Если ваша SIM-карта находится в закрытой частной сети, от куда нет доступа в сеть интернет, то роутер с определенной периодичностью будет перезагружать интерфейсы связи. Таким образом, будет теряться связь с устройством. Чтобы это не происходило, необходимо установить другой IP-адрес тестового сервера (который всегда будет доступен в вашей сети) или отключить Simman сосем.

3.10.1. Установка другого адреса тестового сервера для «пинг»

Перейдите во вкладку «Сервисы -> Менеджер SIM». В разделе «Настройки» в поле «Адреса тестовых серверов для пинга» задайте необходимый IP-адрес.

После этого прокрутите страницу вниз и нажмите кнопку «Сохранить и применить».

3.10.2. Отключение Simman

Рекомендуется использовать данный способ, только в том случае, если нет тестовых серверов для «пинга». Перейдите во вкладку «Сервисы -> Менеджер SIM».

В разделе «Настройки» уберите галочку «Включить» для описания: «Для переключения необходима перезагрузка». После этого прокрутите страницу вниз и нажмите кнопку «Сохранить и применить». После этих действий, роутер не будет проверять связь путем выполнения команды «пинг» с тестовым сервером.

Так же необходимо проверить и, при необходимости, удалить конфигурации «PingControl». Перейдите во вкладку «Сервисы -> PinControl». На загруженной странице удалите все конфигурации и нажмите кнопку «Сохранить и применить».

4. Описание ПО ЭСТРА-РОУТЕР

В данном разделе представлены описание программного обеспечения Configurator ESTRA-ROUTER (ПО Configurator ESTRA-ROUTER) и описание настройки роутера с ПО ЭСТРА-РОУТЕР с помощью ПО Configurator ESTRA-ROUTER.

4.1. Configurator ESTRA-ROUTER

ПО Configurator ESTRA-ROUTER предназначено для подключения к роутеру с установленным ПО ЭСТРА-РОУТЕР. После запуска программы откроется главное окно программы рисунок 79.

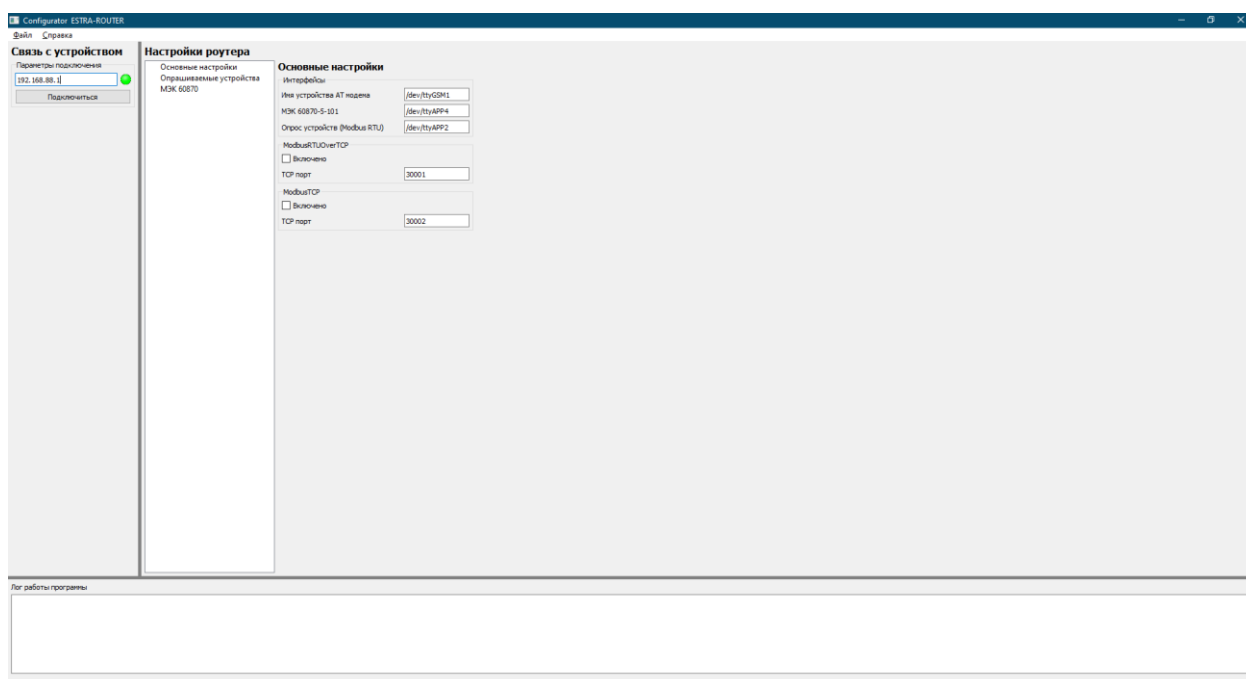


Рис.79. Главное окно программы Configurator ESTRA-ROUTER

В верхней части программы расположена полоса элементов меню, в середине размещена главная рабочая область, в нижней части программы расположено окно с логом работы программы.

4.2. Подключение к роутеру

После запуска Configurator ESTRA-ROUTER происходит постоянный ping IP-адреса введенного в поле «Параметры подключения»: если горит зеленый индикатор, значит устройство находится в сети, если горит красный

индикатор, значит устройство с введенным IP-адресом не в сети или на нем заблокирована функция ответа на ping сообщение.

Если ваша сеть использует Proxu-сервер, при подключении к ЭСТРА-РОУТЕР могут понадобиться настройки Proxu (при условии, что компьютер, на котором вы работает не настроен на работу через Proxu-сервер). Для этого, в параметрах подключения выберите Proxu, задайте адрес Proxu-сервера и порт подключения. При необходимости укажите «Логин/Пароль» (информация о Proxu предоставляет лицами, которые организовали и поддерживают вашу сеть).

Чтобы подключиться к роутеру, введите его IP-адрес ([1-255].[0-255].[0-255].[0-255]) и нажмите кнопку подключиться. Откроется окно для ввода пароля. Данный пароль никак не связан с паролем пользователя в операционной системе OpenWrt. Данный пароль относится к ПО ЭСТРА-РОУТЕР, по умолчанию estraRoot. После успешного подключения к роутеру в окне «Лог работы программы» появится соответствующее сообщение, например, 15.03.2022 10:47:51.959: Подключились к устройству. ip = 192.168.88.1, а в разделе «Связь с устройством» появятся разделы (рисунок 80):

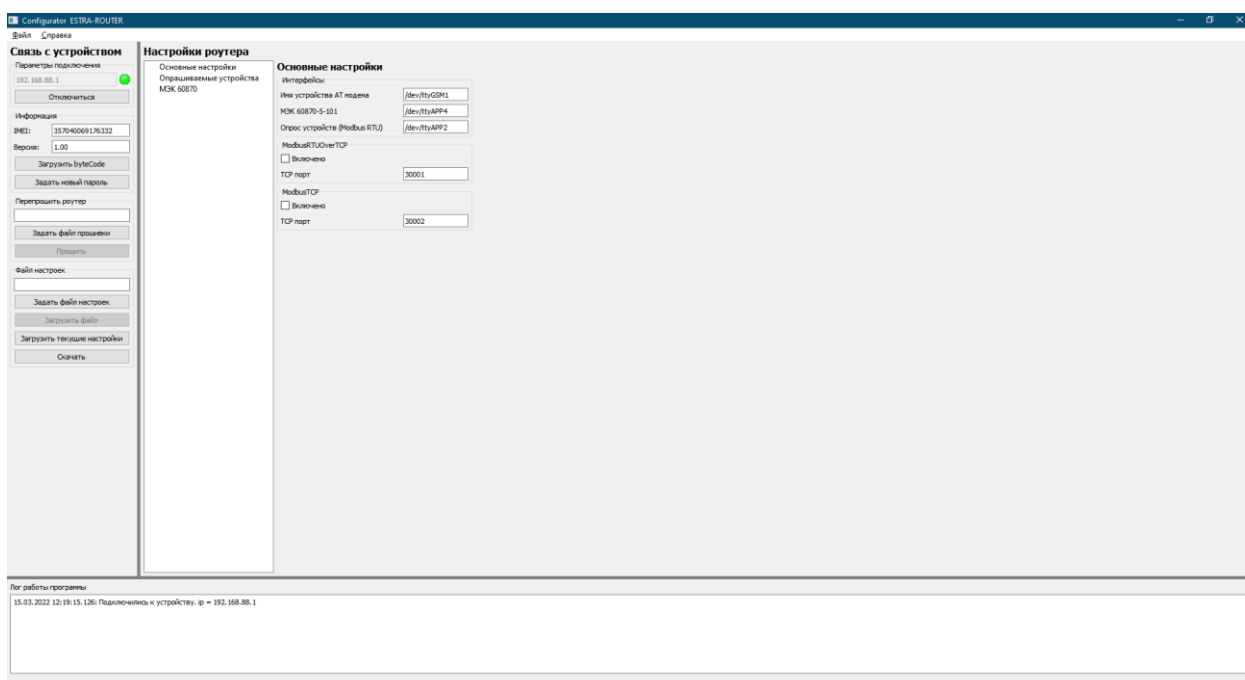


Рис.80. Главное окно после подключения к роутеру

Информация – в данном разделе отображается IMEI роутера, версия ПО ЭСТРА-РОУТЕР, установленного в роутере, кнопка «Загрузить byteCode» и кнопка «Задать новый пароль».

Перепрошить роутер – в данном окне находятся поле, где отображается имя файла прошивки (при наведении мыши высвечивается полный путь к файлу), кнопка «Задать файл прошивки» и кнопка «Прошить», которая активна, когда задан файл прошивки.

Файл настроек – в этом окне находятся поле, где отображается имя файла настроек (при наведении мыши высвечивается полный путь к файлу), кнопка «Задать файл настроек», кнопка «Загрузить файл», которая активна, когда задан файл настроек, кнопка «Загрузить текущие настройки», загружает те настройки, которые выставлены в данный момент в разделе «Настройки роутера» и кнопка «Скачать» – скачивает настройки из роутера и отображает в разделе «Настройки роутера».

4.2.1. Загрузить byteCode

byteCode – файл, необходимый для корректной работы ПО ЭСТРА-РОУТЕР. Данный файл индивидуальный для каждого устройства. Имеет имя соответствующее IMEI конкретного роутера. Для его получения необходимо обратиться в компанию ООО НПП ЭСТРА.

Нажмите кнопку «Загрузить byteCode», в появившемся окне выберите файл. В разделе «Лог работы программы» вы увидите ряд сообщений:

```
15.03.2022 11:11:19.847: ByteCode отправлен роутеру  
15.03.2022 11:11:20.013: ByteCode загружен. Роутер будет перезагружен  
15.03.2022 11:11:20.247: Отключились от устройства. ip = 192.168.88.1  
15.03.2022 11:11:20.263: Ошибка соединения с устройством(1). ip = 192.168.88.1
```

Это означает, что файл загружен и происходит перезагрузка роутера.

4.2.2. Задать новый пароль

Для подключения к ПО ЭСТРА-РОУТЕР необходимо ввести пароль. Пароль по умолчанию: estraRoot. **Рекомендуется** изменить пароль.

Чтобы изменить пароль нажмите кнопку «Задать новый пароль». В появившемся окне введите новый пароль и нажмите «Ок», после этого высветится еще одно окно, для повторного ввода пароля, введите его и нажмите «Ок». Если введенные вами пароли одинаковы, в разделе «Лог работы программы» появится соответствующее сообщение, например, 15.03.2022 11:18:09.669: Новый пароль установлен.

Если вы забыли пароль обратитесь в [службу технической поддержки](#).

4.2.3. Перепрошить

Нажмите кнопку «Задать файл прошивки». Выберите *.ipk файл и нажмите кнопку «Прошить». После этого начнется процесс перепрошивки. По его окончании в разделе «Лог работы программы» вы увидите:

15.03.2022 11:37:01.794: Файл прошивки загружен. Роутер будет перезагружен
15.03.2022 11:37:07.946: Отключились от устройства. ip = 192.168.88.1
15.03.2022 11:37:07.946: Ошибка соединения с устройством(1). ip = 192.168.88.1

Вовремя перепрошивки может происходить потеря пакетов, программа автоматически будет перепосылать данные. В разделе «Лог работы программы» пользователь будет проинформирован.

!Важно. Перепрошивка не удаляет byteCode и не сбрасывает пароль, установленный на роутере.

4.2.4. Загрузить настройки

Загрузить настройки можно двумя способами:

- Задать файл с настройками и загрузить его
- Внести настройки в окне программы и, без сохранения их в файл, загрузить в роутер.

4.2.4.1. Загрузить файл настроек

Нажмите кнопку «Задать файл настроек», выберите файл *.conf. Нажмите кнопку «Загрузить файл». После этого начнется процесс загрузки файла

настроек. По окончании в разделе «Лог работы программы» появятся сообщения:

15.03.2022 11:54:37.757: Загрузка файла настроек начата
15.03.2022 11:54:50.783: Настройки загружены. Роутер будет перезагружен
15.03.2022 11:54:52.138: Отключились от устройства. ip = 192.168.88.1
15.03.2022 11:54:52.138: Ошибка соединения с устройством(1). ip = 192.168.88.1

Во время загрузки файла настроек может происходить потеря пакетов, программа автоматически будет переправлять данные. В разделе «Лог работы программы» пользователь будет проинформирован.

4.2.4.2. Загрузить текущие настройки

Чтобы загрузить текущие настройки необходимо нажать кнопку «Загрузить текущие настройки». После этого начнется процесс загрузки текущих настроек. По окончании в разделе «Лог работы программы» появятся сообщения:

15.03.2022 11:57:19.759: Загрузка текущих настроек начата
15.03.2022 11:57:32.640: Настройки загружены. Роутер будет перезагружен
15.03.2022 11:57:33.930: Отключились от устройства. ip = 192.168.88.1
15.03.2022 11:57:33.930: Ошибка соединения с устройством(1). ip = 192.168.88.1

Вовремя загрузки текущих настроек может происходить потеря пакетов, программа автоматически будет переправлять данные. В разделе «Лог работы программы» пользователь будет проинформирован.

4.2.5. Скачать настройки

Чтобы скачать настройки, которые сейчас используются в роутере нажмите кнопку «Скачать» в разделе «Файл настроек». После этого начнется скачивание настроек. По окончании считанные настройки отобразятся в разделе «Настройки роутера», а в разделе «Лог работы программы» появятся сообщения:

15.03.2022 12:00:15.216: Скачивание файла настроек начато
15.03.2022 12:00:28.322: Файл настроек считан
15.03.2022 12:00:29.319: Файл, считанный из роутера открыт

Если скачать настройки не удалось, и в разделе «Лог работы программы» появилось сообщение:

27.05.2022 06:56:31.817: Скачивание файла настроек начато
27.05.2022 06:56:31.943: Ошибка скачивания файла настроек

Значит в роутере не установлены никакие настройки. Необходимо создать их и загрузить в роутер.

4.3. Настройка ПО ЭСТРА-РОУТЕР

Настройка роутера с установленным ПО ЭСТРА-РОУТЕР производится в разделе «Настройки роутера». Данный раздел имеет дерево элементов, где каждый элемент – это отдельный раздел настроек, и окно ввода параметров выбранного элемента.

4.3.1. Основные настройки

Раздел основные настройки имеет несколько подразделов. Рассмотрим каждый из них отдельно.

4.3.1.1. Интерфейсы

В данном разделе необходимо указать пути к интерфейсам. Эту информацию необходимо получить из руководства по эксплуатации на роутер, который вы используете. В программе Configurator ESTRA-ROUTER по умолчанию установлены значения для 3G роутера TELEOFIS RTU968 V2:

Таблица 3. Интерфейсы по умолчанию (3G роутера TELEOFIS RTU968 V2)

Название	Значение	Описание
Имя устройства АТ модема	/dev/ttyGSM1	Интерфейс, через который идет связь с модулем GSM. Если данный интерфейс будет задан неправильно, ПО ЭСТРА-РОУТЕР не сможет работать корректно, так как не будет возможности считать IMEI.
МЭК 60870-5-101	/dev/ttyAPP4	Интерфейс для подключения роутера в сеть МЭК 60870-5-101. По умолчанию RS-232
Опрос устройств (Modbus RTU)	/dev/ttyAPP2	Интерфейс для опроса устройств по протоколу Modbus RTU, данные которых необходимо преобразовать в другие протоколы. По умолчанию RS-485

У роутеров разных производителей или даже разной версии одной серии роутеров могут быть другие параметры интерфейсов:

Таблица 4. Интерфейсы по умолчанию (3G роутера TELEOFIS RTU968 V1)

Название	Значение	Описание
Имя устройства АТ модема	/dev/ttyACM3	GSM модуль
МЭК60870-5- 101	/dev/ttyAPP4	RS-232
Опрос устройств (Modbus RTU)	/dev/ttyAPP1	RS-485

Таблица 5. Интерфейсы по умолчанию (3G роутера TELEOFIS RTU968 V4)

Название	Значение	Описание
Имя устройства АТ модема		GSM модуль
МЭК60870-5- 101		RS-485 (1)
Опрос устройств (Modbus RTU)		RS-485 (2)

4.3.1.2. Modbus RTU Over TCP

Modbus RTU Over TCP – это протокол Modbus RTU упакованный в TCP. Принцип работы следующий:

Пользователь посылает Modbus RTU пакет, ПО ЭСТРА-РОУТЕР перенаправляет его в сеть опроса устройств (Modbus RTU), полученный ответ отправляет пользователю. Таким образом, создается прямой канал связи с необходимым устройством по протоколу Modbus RTU.

Чтобы включить данный модуль установите галочку «Включить». Необходимо задать TCP порт через, который пользователь будет подключаться. Необходимо [открыть этот порт](#), если вы собираетесь пользоваться этим протоколом в сети Интернет, без OpenVPN.

4.3.1.3. Modbus TCP

Modbus TCP – это протокол для передачи данных через TCP/IP-соединение. Принцип работы следующий:

Пользователь посылает Modbus TCP пакет, ПО ЭСТРА-РОУТЕР преобразует его в пакет Modbus RTU и отправляет в сеть Опроса устройств (Modbus RTU), полученный ответ преобразуется в пакет Modbus TCP и отправляется пользователю. Таким образом, создается прямой канал связи с необходимым устройством (которое работает по протоколу Modbus RTU) по протоколу Modbus TCP.

Чтобы включить данный модуль установите галочку «Включить». Необходимо задать TCP-порт через, который пользователь будет подключаться. Необходимо [открыть этот порт](#), если вы собираетесь пользоваться этим протоколом в сети Интернет, без OpenVPN.

4.3.1.4. Аутентификация пользователей

Данный режим предназначен для подключения к устройствам РЗА производства ООО НПП «ЭСТРА» с помощью программы UProg или мобильного приложения РЗА ЭСТРА по протоколам «Modbus RTU Over TCP» и «Modbus TCP» с использованием средств аутентификации (логин/пароль). Для активации данного режима необходимо установить галочку «Включено».

!!!Важно. Когда активирован данный режим подключиться по протоколам «Modbus RTU Over TCP» и «Modbus TCP» без аутентификации не получится, соединение будет рваться. Поэтому, если к роутеру помимо устройства РЗА производства ООО НПП «ЭСТРА» подключены другие устройства, и связь с ними осуществляется по протоколам «Modbus RTU Over TCP» и «Modbus TCP», не рекомендуется использовать данный режим.

Режим аутентификации пользователей может быть реализован в двух видах:

- Сервер. В этом случае необходимо задать TCP порт, по которому смогут подключаться клиенты (другие роутеры) для обновления базы данных пользователь. Так же необходимо создать пользователей (связки логин/пароль), по которым можно произвести подключение, для этого нажмите кнопку «Настройка пользователей». Пароли пользователей

хранятся в виде хеш-суммы. Если вы забыли пароль, поменять его нельзя, в таком случае, необходимо удалить пользователя и создать нового с новым паролем.

- Клиент. Для работы в этом режиме в сети должен находиться роутер, настроенный в режиме сервера и иметь IP-адрес, по которому можно к нему подключиться. В настройках клиента задается IP-адрес роутера-сервера аутентификации пользователя и TCP порт. Клиент считывает базу данных пользователей с сервера и предоставляет доступ по полученным данным. Считывание базы данных пользователей происходит с интервал 1 час, а также при каждом подключении пользователя к роутеру по логину и паролю.

4.3.2. Опрашиваемые устройства

В данном разделе необходимо задать настройки интерфейса для проса устройств (это может быть, как RS-485, так и RS-232, в зависимости от того какую настройку вы зададите в [разделе интерфейсы](#)) и добавить опрашиваемые устройства.

Чтобы добавить устройство нажмите правой кнопкой мыши на элемент «Опрашиваемые устройства» в дереве элементов и выберите нужный пункт, рисунок 81.

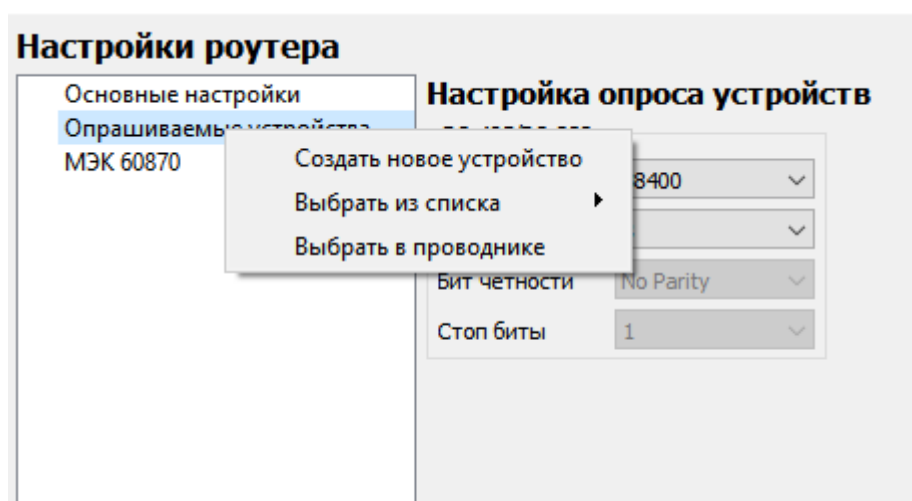


Рис.81. Добавление опрашиваемого устройства

После того как устройство добавлено, необходимо установить ему Modbus адрес.

4.3.2.1. Создать новое устройство

При создании нового устройства высветится окно с вводом наименования. Наименование должно быть уникальным.

После того как устройство создано, оно появится в дереве элементов. Нажатием правой кнопки мыши по элементу можно переименовать и удалить его.

Далее необходимо [редактировать настройки устройства](#).

4.3.2.1.1. Редактировать настройки устройства

Редактирование настроек устройства позволяет добавить/переименовать/удалить разделы/элементы устройства. Вы так же может настроить устройства и сохранить настройку в файл и в дальнейшем использовать этот файл для создания настроек роутера и не создавать это устройство заново. Для сохранения настроек устройства нажмите кнопку «Сохранить устройство в файл» рисунок 82.

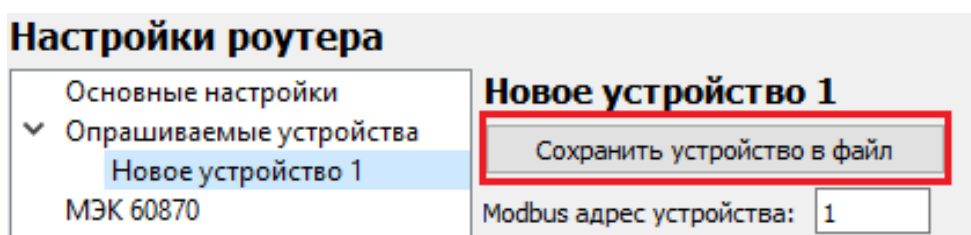


Рис.82. Сохранить настройки устройства

Для создания нового раздела нажмите правой кнопкой мыши на любой из созданных разделом или в любую часть в таблицы элементов устройства, если ни один из разделов не создан, то выберите пункт «Добавить раздел», рисунок 83.

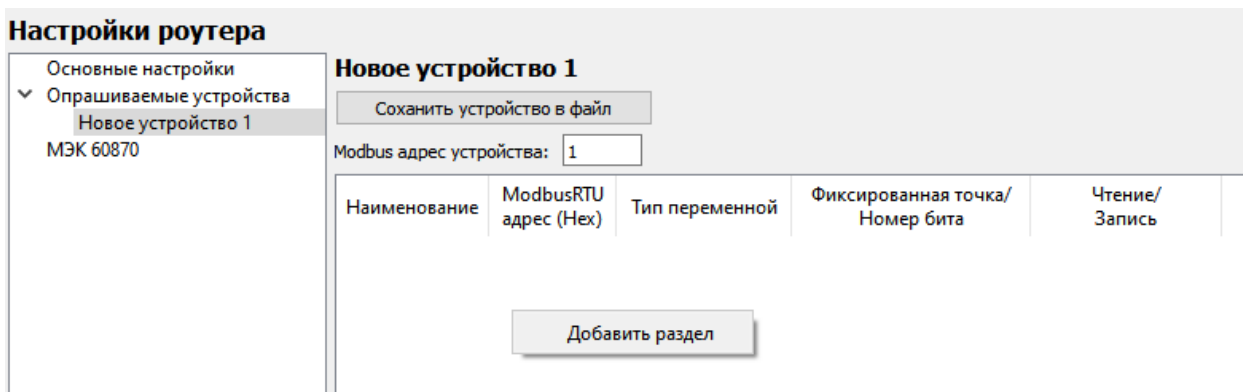


Рис.83. Добавить новый раздел

Нажав правой кнопкой мыши на раздел можно: добавить новый раздел, переименовать раздел, удалить раздел и добавить в него элемент (рисунок 28).

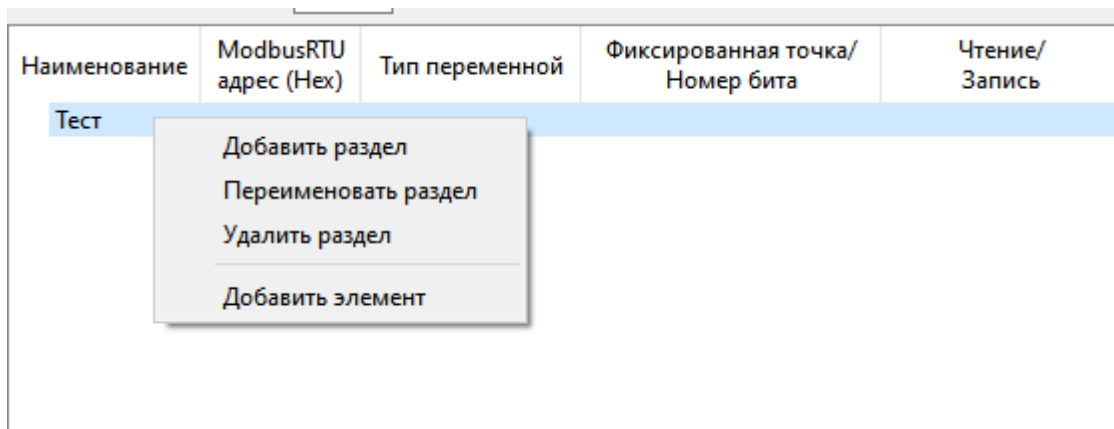


Рис.83. Контекстное меню раздела

Добавлять разделы и элементы необходимо в соответствии с картой памяти устройства, для которого вы создаете файл.

Для примера, добавим несколько элементов в соответствии с картой памяти устройства защиты для реклоузера и пункта секционирования [МКЗП-ПС с комбинированным датчиком КДТН-01](#) (рисунок 84):

1. «Статус 0. Питание» - адрес 0x0110, битовое значение (тип переменной bool), номер бита 6, только чтение.
2. «Текущее значение тока фазы А» - адрес 0x0120, беззнаковое число (uint16), один разряд после запятой, только чтение.
3. «Текущее значение активной мощности» - адрес 0x01CC, знаковое число (int16), целое число, только чтение

4. «Пароль доступа» - адрес 0x02F8, знаковое число (int16), целое число, чтение и запись.
5. Команда «ВКЛЮЧИТЬ» - адрес 0x0001, беззнаковое число (uint16), целое число, только запись.

Наименование	ModbusRTU адрес (Hex)	Тип переменной	Фиксированная точка/ Номер бита	Чтение/ Запись
Тест				
Статус 0. Питание	110	bool	6	Только чтение
Текущее значение тока фазы А	120	uint16	1	Только чтение
Текущее значение активной мощности	1CC	int16	0	Только чтение
Пароль доступа	2F8	int16	0	Чтение и запись
ВКЛЮЧИТЬ	1	uint16	0	Только запись

Рис.84. Элементы устройства в соответствии с картой памяти МКЗП-ПС

4.3.2.2. Выбрать устройство из списка

При выборе устройства из списка, оно автоматически добавится и ему присвоится имя (то которое прописано в его конфигурационном файле). При необходимости вы можете [редактировать устройство](#). Задайте Modbus адрес устройству.

4.3.2.3. Выбрать устройство в проводнике

Вы можете указать файл на конфигурацию устройства с помощью проводника. После того как вы выберете файл, устройство автоматически присвоится имя (то которое прописано в конфигурационном файле). При необходимости вы можете [редактировать устройство](#). Задайте Modbus адрес устройству.

4.3.3. МЭК 60870

При переходе в настройку раздела МЭК 60870 отображается окно настроек, которое имеет три вкладки «Настройки», «Теги» и «Виртуальные теги».

4.3.3.1. Настройки. МЭК 60870-5-101 Slave

ПО ЭСТРА-РОУТЕР позволяет модему выступать в сети МЭК 60870-5-101 в качестве устройства Slave. Чтобы включить данный модуль, установите галочку «Включено».

Интерфейс МЭК 60870-5-101 задается в разделе [«Интерфейсы»](#) основных настроек.

Таблица 6. Настройки МЭК 60870-5-101

Название	Описание
Скорость	Скорость передачи данных (RS-485/RS-232), бод/с
Биты данных	Количество битов данных (RS-485/RS-232)
Бит четности	Не используется – всегда No parity
Стоп биты	Не используется – всегда 1
Link size in bytes	Размер адреса в байтах: не используется – всегда 1
COT size in bytes	Размер причины передачи в байтах
CA size in bytes (ASDU)	Размер ASDU адреса в байтах
IOA size in bytes	Размер адреса объекта информации в байтах
Mode	Режим работы: несбалансированный/сбалансированный
Address Link	Адрес роутера в сети МЭК 60870-5-101
Address Link Other Station	Адрес удаленного устройства (устройство, которое собирает информации) – актуально для сбалансированного режима
IDLE Timeout	Время проверки связи, мс
Timeout for ask	Время для запроса – актуально для сбалансированного режима

4.3.3.2. Настройка. МЭК 60870-5-104 Server

ПО ЭСТРА-РОУТЕК позволяет модему выступать в качестве сервера МЭК 60870-5-104, т.е. Slave устройства в сети МЭК 60870-5-104. Чтобы включить данный модуль, установите галочку «Включено».

Таблица 7. Настройки МЭК 60870-5-104

Название	Описание
COT size in bytes	Размер причины передачи в байтах
CA size in bytes (ASDU)	Размер ASDU адреса в байтах
IOA size in bytes	Размер адреса объекта информации в байтах
TCP порт	TCP порт для подключения к модулю МЭК 60870-5-104

4.3.3.3. Теги

При переходе на вкладку «Теги» отображается таблица с тегами МЭК 60870. Для всех модулей МЭК 60870 теги одни. Теги автоматически формируются исходя из [настроек «Опрашиваемых устройств»](#): задаются имена, адреса, типы. Пользователь может изменить:

- Использование тега – галочка слева от наименования тега.
- Спорадическая передача данных и Минимальное/Максимальное значение спорадической передачи данных (для некоторых типов тегов)

Таблица 8. Поддерживаемые типы тегов в ПО ЭСТРА-РОУТЕР

Номер	Мнемоника ASDU	Описание
<1>	M_SP_NA_1	Однобитовая информация
<11>	M_ME_NB_1	Значение измеряемой величины, масштабированное значение
<13>	M_ME_NC_1	Значение измеряемой величины, короткий формат с плавающей запятой
<45>	C_SC_NA_1	Однопозиционная команда
<49>	C_SE_NB_1	Команда уставки, масштабированное значение

Спорадическую передачу можно задать только для тегов чтения <1>, <11> и <13>. Параметры спорадической передачи (Минимум/Максимум) можно задать только для <11> и <13>.

Принцип работы спорадической передачи:

1. Для тега типа <1> всегда, когда изменилось значение.
2. Для тегов типа <11> и <13> задаются значения минимум и максимум:
 - 2.1. если минимум и максимум заданы нулем – то значение этого тега передается каждый раз, когда изменилось его значение;
 - 2.2. если текущее значение тега не попадает в диапазон от минимума до максимума и его предыдущее значение не соответствует текущему, то происходит отправка нового значения;
 - 2.3. если текущее значение тега попадает в диапазон от минимума до максимума, но при этом предыдущее значение не попадало в диапазон, то происходит отправка;
 - 2.4. в других случаях спорадическая передача не выполняется.

4.3.3.4. Виртуальные теги

Виртуальными тегами называются теги, созданные пользователем, которые не имеют прямой связи с устройством. Т.е. этот тег не является однозначным.

Реализовано создание виртуальных тегов только типа C_SC_NA_1 <45> - однопозиционная команда.

Виртуальные теги следуют за основными тегами, следовательно, их адреса продолжают после адресов основных тегов.

Чтобы создать виртуальный тег, нажмите ПКМ в поле настройки и выберите пункт меню «Добавить». После этого необходимо заполнить информацию о теге.

Чтобы удалить виртуальный тег, нажмите ПКМ на линию тега, который необходимо удалить (нажимать нужно в районе полей «Адрес», «Тип»), в выпадающем меню выбрать пункт «Удалить».

Параметры виртуального тега:

- Наименование – информация для пользователя.
- Адрес – задается программой. Изменить нельзя.
- Тип – задается программой. Изменить нельзя.
- Modbus адрес устройства – адрес устройства, которое подключено к ЭСТРА-РОУТЕР.
- Команда 0 (Hex) адрес Modbus RTU – адрес, по которому необходимо записать значение, когда в тег передали значение 0. Если никаких действий выполнять не нужно, когда в тег записали 0, то адрес устанавливаем 0.
- Команда 0 (значение) – значение, которое необходимо записать по указанному выше адресу, когда в тег записали 0.
- Команда 1 (Hex) адрес Modbus RTU – адрес, по которому необходимо записать значение, когда в тег передали значение 1. Если никаких действий выполнять не нужно, когда в тег записали 1, то адрес устанавливаем 0.
- Команда 1 (значение) – значение, которое необходимо записать по указанному выше адресу, когда в тег записали 1.

- pre Команда (Hex) адрес Modbus RTU – адрес, по которому необходимо записать значение, перед выполнением основного действия. Если никаких действий выполнять не нужно, то адрес устанавливаем 0.
- pre Команда (значение) – значение, которое необходимо записать по указанному выше адресу.
- post Команда (Hex) адрес Modbus RTU – адрес, по которому необходимо записать значение, после выполнением основного действия. Если никаких действий выполнять не нужно, то адрес устанавливаем 0.
- post Команда (значение) – значение, которое необходимо записать по указанному выше адресу.

Рассмотрим на примере команд «Включить/Отключить» выключатель в устройствах серии МКЗП. Необходимо сделать, чтобы при записи в тег значения 0 – выполнялась команда «Отключить», а при записи значения 1 – выполнялась команда «Включить». В устройствах МКЗП данные команды выполняются только если есть соответствующие права доступа. Итак, создадим виртуальный тег и заполним параметры:

- Наименование: Включить/Отключить.
- Адрес/Тип: заданы программой.
- Modbus адрес устройства: предположим, что у устройства адрес 1.
- Команда 0 (Hex) адрес Modbus RTU: необходимо послать команду «Отключить». В МКЗП для этого используется регистр с адресом 1 (0x0001).
- Команда 0 (значение): в устройствах МКЗП необходимо записать число 0xA00C. Переведем это число в 10-ную систему счисления – 40972. **Внимание!** В программе используется тип значений int16 (диапазон – 32768... 32767), это означает, что введенное значение, будет преобразовано к этому типу, в итоге в ячейке будет записано значение - 24564. Это значение соответствует 16-ому значению 0xA00C.

- Команда 1 (Hex) адрес Modbus RTU: необходимо послать команду «Включить». В МКЗП для этого используется регистр с адресом 1 (0x0001).
- Команда 1 (значение): в устройствах МКЗП необходимо записать число 0xA003. Переведем это число в 10-ную систему счисления – 40963. После преобразования в ячейке будет записано -24573.
- pre Команда (Hex) адрес Modbus RTU: так как для выполнения команд телеуправления необходим соответствующий уровень доступа, записываем уровень доступа по адресу 2F8 (0x02F8).
- pre Команда (значение): установим «Сервисный» уровень доступа. По умолчанию «1234».
- post Команда (Hex) адрес Modbus RTU: после выполнения команды сбросим уровень доступа, адрес 2F8 (0x02F8).
- post Команда (значение): для сброса уровня доступа необходимо записать значение -1.

Таким образом получаем следующую настройку виртуального тега для «Включения/Отключения», рисунок 85.

Настройки МЭК 60870											
Настройки Теги Виртуальные теги											
Наименование	Адрес	Тип	Modbus адрес устройства	Команда 0 (Hex) адрес Modbus RTU	Команда 0 (значение)	Команда 1 (Hex) адрес Modbus RTU	Команда 1 (значение)	pre Команда (Hex) адрес Modbus RTU	pre Команды (значение)	post Команда (Hex) адрес Modbus RTU	post Команда (значение)
1 Включить/Отключить	177	M_SC_NA_1 <45>	1	1	-24564	1	-24573	2F8	1234	2F8	-1

Рис.85. Настройка виртуального тега

4.3.4. МЭК 61850

В ПО ЭСТРА-РОУТЕР МЭК 61850 реализован в виде Сервера MMS.

Важно!!! МЭК 61850 имеет ограниченный функционал. Для ознакомления с возможностями, обязательно прочтите данный раздел до конца. При необходимости, скачайте ПО Configurator ESTRA-ROUTER и в офлайн режиме ознакомьтесь с реализованными функциями МЭК 61850. Так же рекомендуем обратиться в [отдел тех. поддержки](#) для уточнения интересующих вас вопросов.

Предоставление возможности работы на подобных преобразователях по протоколам GOOSE и Sampled Values не имеет смысла, так как невозможно обеспечить необходимые показатели по скорости работы – ограничение вносит обмен информацией с устройством РЗА по интерфейсу «RS-485», который физически не поддерживает скорости необходимые для работы по протоколам GOOSE и Sampled Values.

При переходе в настройку раздела МЭК 61850 отображается окно настроек, которое имеет две вкладки «Основные настройки» и «Логические устройства».

4.3.4.1. Основные настройки

Данная вкладка имеет основные настройки для МЭК 61850:

Галочка «Включено» – используется или нет МЭК 61850.

TCP порт – порт, необходимый для подключения по протоколу MMS, по умолчанию 102.

Наименование IED – наименование Интеллектуального Электронного Устройства, в соответствии со стандартом МЭК 61850.

4.3.4.2. Логические устройства

ПО ЭСТРА-РОУТЕР поддерживает создание нескольких логических устройств (LD). Для каждого LD создаются свои логические узлы (LN). Список поддерживаемых логических узлов и их содержание (объекты данных (DO) или атрибуты данных (DA)) представлен в таблице 9.

Таблица 9. Логические узлы, поддерживаемые ПО ЭСТРА-РОУТЕР

Наим. LN	Описание LN	Наим. DO/DA	Описание DO/DA
LLN0	Системные функции	LockKey	Положение ключа режима управления (ИСТИНА – местное, ЛОЖЬ – дистанционное)
LPHD	Информация о физическом устройстве	PhyHealth	Контроль исправности устройства
		PwrUp	Индикатор наличия оперативного питания
		PwrDn	Индикатор потери оперативного питания
		ROMHealth	Исправность ПЗУ
		AdcFail	Отказ АЦП
		MemRs	Сброс часов или памяти вследствие перезагрузки
		CRFail	Ошибка конфигурации
CSWI	Оперативное управление коммутационным	Pos	Положение

	аппаратом		
GGIO	Дискретные входы/выходы	IO1-IO16	Вход/выход
MMTR	Трехфазный учет электроэнергии	TotVAh	Суммарная полная энергия
		TotWh	Суммарная активная энергия
		TotVARh	Суммарная реактивная энергия
		SupWh	Активная энергия (направление – к шинам)
		SupVARh	Реактивная энергия (направление – к шинам)
		DmdWh	Активная энергия (направление – от шин)
		DmdVARh	Реактивная энергия (направление – от шин)
MMXU	Трехфазные измерения	TotW	Суммарная активная мощность
		TotVar	Суммарная реактивная мощность
		TotPF	Суммарный коэффициент мощности
		Hz	Частота
		PPV	Напряжение фаза-фаза: pHsAB – фаза AB pHsBC – фаза BC pHsCA – фаза CA
		PhV	Напряжение фаза-фаза: pHsA – фаза A pHsB – фаза B pHsC – фаза C
		A	Напряжение фаза-фаза: pHsA – фаза A pHsB – фаза B pHsC – фаза C
MSQI	Последовательность и небаланс	SeqA	ПП, ОП, НП тока: PP – прямая последовательность OP – обратная последовательность NP – нулевая последовательность
		SeqV	ПП, ОП, НП напряжения: PP – прямая последовательность OP – обратная последовательность NP – нулевая последовательность
XCBR	Силовой выключатель	OpCtn	Счетчик операций
		EmgTr	Аварийное отключение выключателя
		Pos	Положение выключателя (2 варианта): 1. Включено, Отключено, НЦУ 2. Состояние

Все используемые логические узлы работают только в режиме чтения, т.е. вы можете считать измерения, положения выключателя и другие параметры, но нельзя управлять выключателем или изменять какие-нибудь другие параметры.

4.3.4.3. Связь со SCADA, АСУ ТП и т.д.

Для интеллектуальных электронных устройств в МЭК 61850 предусмотрены файлы описания возможностей и описания конфигурации устройства:

- ICD (IED Capabilities Description) – файл описания возможностей устройства

- CID (Configured IED Description) – файл описания конфигурации устройства

При создании полноценной цифровой подстанции из устройства считывается файл ICD, после чего в специальной программе производится настройка цифровой подстанции. В итоге создаются CID файлы для каждого интеллектуального электронного устройства. После чего CID файлы загружаются в устройства.

На данный момент ПО ЭСТРА-РОУТЕР не работает с файлами ICD/CID. Однако это не мешает производить опрос устройства по стандарту МЭК 61850 по протоколу MMS. В стандарте описано много сервисов передачи данных, таких как:

- процедуры установления связи между клиентом и сервером (Associate, Abort, Release)
- считывание информационной модели (GetServerDirectory, GetLogicalDeviceDirectory, GetLogicalNodeDirectory)
- считывание значений переменных (GetAllDataValues, GetDataValues и т.д.)
- передача значений переменных в виде отчётов (Report)
- и другие

4.3.5. Файлы-примеры настройки устройства

В корне программа Configurator ESTRA-ROUTER находится каталог example. В этом каталоге находятся файлы-примеры настройки ЭСТРА-РОУТЕР для некоторых типов защит, например, exp_MKZP_PS_RTUv2.conf – файл настройки роутера для работы с устройств РЗА МКЗП-ПС.

Все файла настройки имеют одинаковую настройку за исключением карты адрес, она настроена в соответствии с картой памяти каждого устройства.

Ниже написаны настройки, заданные в этих файлах:

Основные настройки:

- Интерфейсы – для работы с 3G роутером TELEOFIS RTU968 V2.
- Modbus RTU Over TCP – включено, порт 30001.
- Modbus TCP – включено, порт 30002.
- Аутентификация пользователь – выключено.

Опрашиваемые устройства:

- RS-485/RS-232: скорость – 38400; биты данных – 8; бит четности – No parity; стоп биты – 1.
- Устройство – в соответствии с тем, какое устройство выбрано.
- Modbus адрес устройства – 1.

МЭК 60870:

- МЭК 60870-5-101 Client – выключено.
- МЭК 60870-5-104 Server – включено.
- МЭК 60870-5-104 Server – TCP порт – 2404.
- МЭК 60870-5-104 Server – COT size in bytes – 2
- МЭК 60870-5-104 Server – CA size in bytes (ASDU) – 2
- МЭК 60870-5-104 Server – IOA size in bytes – 3
- МЭК 60870-5-104 Server – Max count tags in packet – 32
- Все теги используются. Спорадическая передача отключена.

МЭК 61850:

- Используется.
- TCP порт – 102
- Наименование IED – ESTRA
- Создано одно логическое устройство, которое содержит следующие логические узлы: LLN0, LPHD1, MMXU1(MMXU2), MMTR1, MSQI1(MSQI2), GGIO1, GGIO2, XCBR.

4.4. Работа с файлами

Для работы с файлами необходимо использовать пункт меню «Файл» в левом верхнем углу программы.

4.4.1. Открыть файл настроек роутера

Чтобы открыть файл настроек роутера нажмите пункт меню «Файл» и выберите «Открыть файл настроек роутера». После это необходимо выбрать файл (*.confr). После этого считанные настройки отобразятся в разделе «Настройки роутера».

4.4.2. Сохранить настройки роутера в файл

После настройки параметров роутера в разделе «Настройки роутера» их можно сохранить в файл. Для этого необходимо нажать пункт меню «Файл» и выбрать «Сохранить настройки роутера в файл». После этого выбрать задать имя файла и сохранить.

4.4.3. Карта тегов МЭК 60870

Для предоставления карты тегов МЭК 60870 пользователям SCADA систем (или других программ, работающих по протоколам МЭК 60870) предусмотрена функция сохранения карты тегов в файл формата PDF.

Рекомендуется считать актуальные настройки из устройства в ПО Configurator ESTRA-ROUTER, после это создавать файл тегов.

Нажмите на пункт меню «Файл» и выберете «Сохранить теги МЭК 60870 в файл PDF». После это необходимо задать имя файл и сохранить.

5. Техническая поддержка

По вопросам технической поддержки обращайтесь в ООО НПП ЭСТРА:

ООО НПП ЭСТРА

630108, Новосибирск, ул. Станционная, д. 30а, корп. 3

тел: +7 (800) 333-20-83 (звонок бесплатный)

<https://rza-estra.ru/>, e-mail: service@rza-estra.ru