

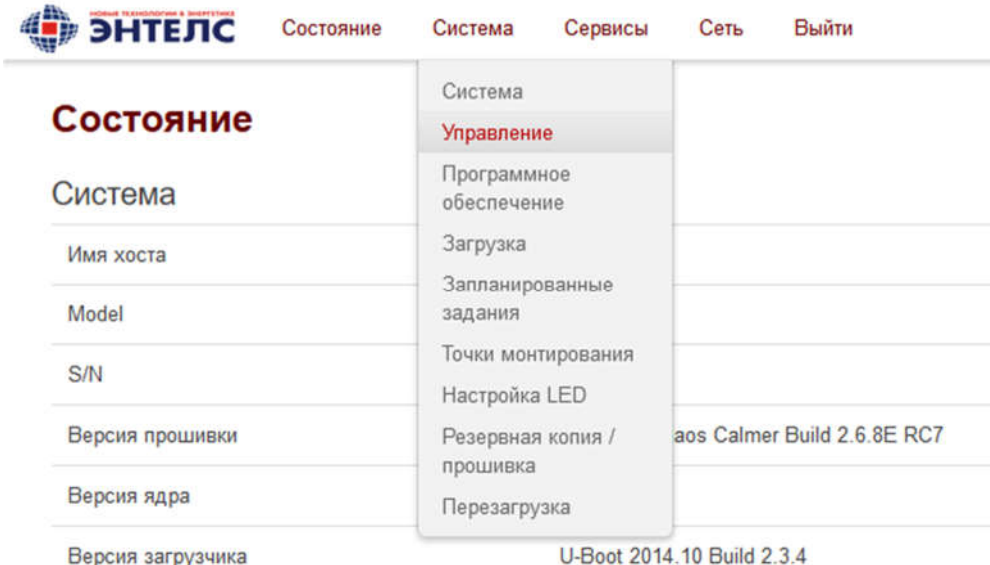
# Рекомендации по обеспечению безопасности контроллера E2R2-G

В данной статье собраны рекомендации по обеспечению максимальной безопасности контроллера E2R2-G.

Логин пользователя root

Необходимо сменить дефолтный пароль для пользователя root, это делается через Веб-интерфейс контроллера.

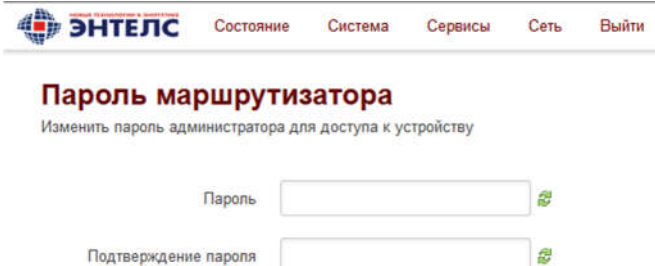
Заходим в Веб-интерфейс, выбираем пункт меню **Система**→**Управление**:



The screenshot shows the ZTELS web interface. At the top, there is a navigation bar with the ZTELS logo and the text 'Новые технологии в энергетике'. The main menu includes 'Состояние', 'Система', 'Сервисы', 'Сеть', and 'Выйти'. The 'Состояние' page is active, displaying system information. A dropdown menu is open under 'Система', with 'Управление' highlighted. The system information table is as follows:

Состояние	
Система	
Имя хоста	
Model	
S/N	
Версия прошивки	aos Calmer Build 2.6.8E RC7
Версия ядра	
Версия загрузчика	U-Boot 2014.10 Build 2.3.4

Меняем пароль



The screenshot shows the 'Пароль маршрутизатора' page in the ZTELS web interface. The page title is 'Пароль маршрутизатора' and the subtitle is 'Изменить пароль администратора для доступа к устройству'. There are two input fields: 'Пароль' (Password) and 'Подтверждение пароля' (Confirm password), each with a green eye icon to toggle visibility. The navigation bar at the top is the same as in the previous screenshot.

Внизу страницы нажимаем **Сохранить и применить**:

Сохранить и применить

Сохранить

Сбросить

## Доступ по SSH



На той же странице есть настройки доступа по SSH:

### Доступ по SSH

Dropbear - это SSH-сервер со встроенным SCP

Dropbear

Удалить

Интерфейс  internet:   
 lan:   
 не определено

Слушать только на данном интерфейсе или, если не определено, на всех



Порт   
 Порт данного процесса Dropbear

Аутентификация с помощью пароля   Разрешить SSH-аутентификацию с помощью пароля

Разрешить пользователю root вход с помощью пароля   Разрешить пользователю root входить в систему с помощью пароля


Порты шлюза   Разрешить удалённым хостам подключаться к локальным перенаправленным портам SSH

Если **интерфейс** стоит в режиме *не определено*, тогда разрешено подключение по SSH к контроллеру по любому интерфейсу, в том числе по GPRS. Не стоит отключать SSH совсем, но лучше перевести подключение в режим **lan**, тогда подключение по SSH будет доступно только при прямом подключении к контроллеру через его порт Eth.

Интерфейс  internet:   
 lan:   
 не определено

## Список открытых портов

Список TCP/UDP портов, доступных для подключения, настраивается на вкладке **Сеть** → **Межсетевой экран**:


Состояние
Система
Сервисы
Сеть
Выйти

---


## Состояние

Система

Имя хоста	RTU968V2
Model	RTUx68V2
S/N	7880e5d7
Версия прошивки	OpenWrt Chaos Calmer Build 2.6.8E RC7
Версия ядра	3.18.29

Интерфейсы  
 DHCP и DNS  
 Имена хостов  
 Статические маршруты  
 Диагностика  
**Межсетевой экран**  
 Резервирование WAN

Далее надо перейти на вкладку **Правила для трафика**:


Состояние
Система
Сервисы
Сеть
Выйти

---

[Основные настройки](#)
[Перенаправления портов](#)
[Правила для трафика](#)
[Пользовательские правила](#)

### Межсетевой экран - Правила для трафика

Правила для трафика определяют политику прохождения пакетов между разными зонами, например, запрет трафика между некоторыми хостами или открытие WAN-портов маршрутизатора.

#### Правила для трафика

Имя	Выбирать	Действие	Включить	Сортировка	
Allow-DHCP-Renew	IPv4-UDP Из любого хоста в wan К любой IP-адрес маршрутизатора, порту port 68 на этом устройстве	Accept input	<input checked="" type="checkbox"/>		<div style="display: flex; align-items: center; gap: 10px;"> <span>+</span> <span>+</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Редактировать</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Удалить</span> </div>

И списка обычно добавленных пользовательских разрешений:

2222	Любой TCP, UDP Из любого хоста в wan К любой IP-адрес маршрутизатора, порту port 2222 на этом устройстве	Accept input	<input checked="" type="checkbox"/>		<div style="display: flex; align-items: center; gap: 10px;"> <span>+</span> <span>+</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Редактировать</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Удалить</span> </div>
2404	Любой TCP, UDP Из любого хоста в wan К любой IP-адрес маршрутизатора, порту port 2404 на этом устройстве	Accept input	<input checked="" type="checkbox"/>		<div style="display: flex; align-items: center; gap: 10px;"> <span>+</span> <span>+</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Редактировать</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Удалить</span> </div>
4001	Любой TCP, UDP Из любого хоста в wan К любой IP-адрес маршрутизатора, порту port 4001 на этом устройстве	Accept input	<input checked="" type="checkbox"/>		<div style="display: flex; align-items: center; gap: 10px;"> <span>+</span> <span>+</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Редактировать</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Удалить</span> </div>
30292	Любой TCP, UDP Из любого хоста в wan К любой IP-адрес маршрутизатора, порту port 30292 на этом устройстве	Accept input	<input checked="" type="checkbox"/>		<div style="display: flex; align-items: center; gap: 10px;"> <span>+</span> <span>+</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Редактировать</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Удалить</span> </div>
80	Любой TCP Из любого хоста в wan К любой IP-адрес маршрутизатора, порту port 80 на этом устройстве	Accept input	<input checked="" type="checkbox"/>		<div style="display: flex; align-items: center; gap: 10px;"> <span>+</span> <span>+</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Редактировать</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Удалить</span> </div>
30294	Любой TCP Из любого хоста в wan К любой IP-адрес маршрутизатора, порту port 30294 на этом устройстве	Accept input	<input checked="" type="checkbox"/>		<div style="display: flex; align-items: center; gap: 10px;"> <span>+</span> <span>+</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Редактировать</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Удалить</span> </div>
102 - MMS	Любой TCP, UDP Из любого хоста в wan К любой IP-адрес маршрутизатора, порту port 102 на этом устройстве	Accept input	<input checked="" type="checkbox"/>		<div style="display: flex; align-items: center; gap: 10px;"> <span>+</span> <span>+</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Редактировать</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">Удалить</span> </div>

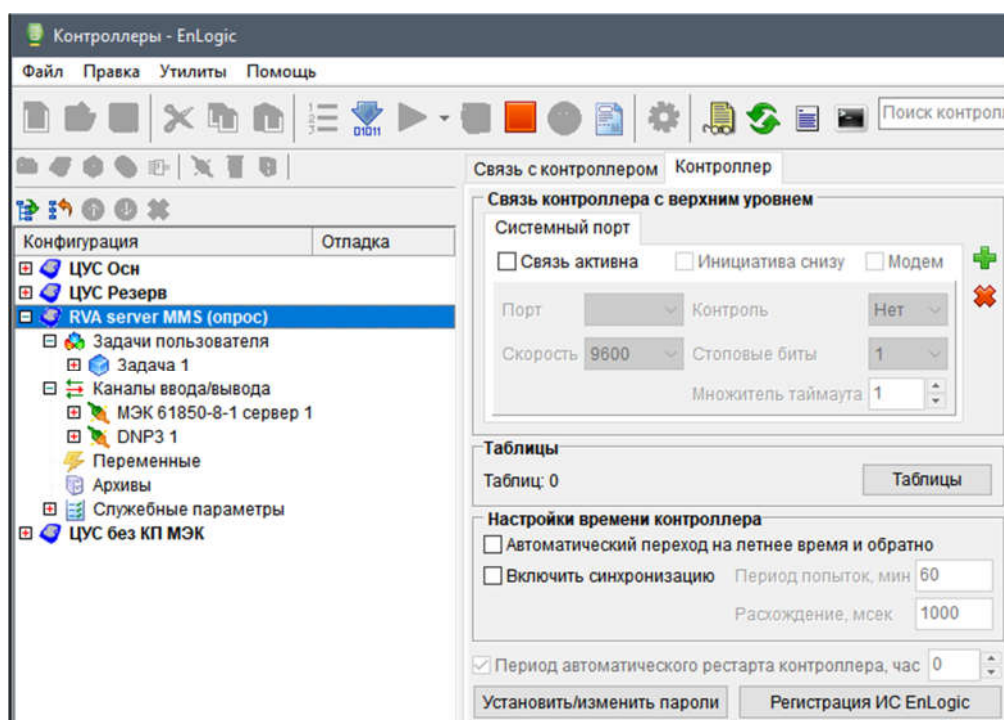
оставить только те порты, которые реально используются.

Порты:

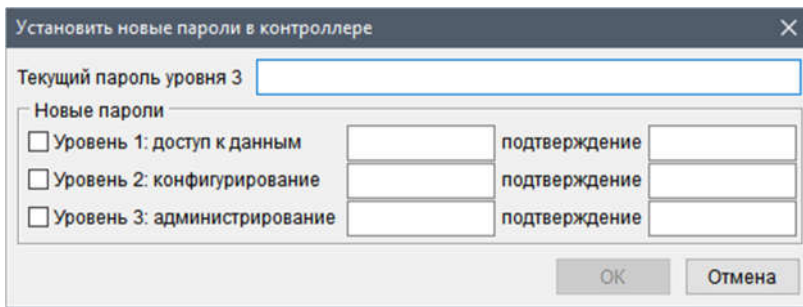
- Порт **2404** - стандартный порт для передачи данных от контроллера по протоколу МЭК 60870-5-104.
- Порт **30292** - порт для связи с контроллером через среду конфигурирования ENLOGIC. Также этот порт используется для передачи данных по протоколу АСКУЭ. Если передача данных АСКУЭ с контроллера не производится (только задачи телемеханики), тогда данный порт можно закрыть, а при необходимости настройки контроллера открыть его снова.
- Порт **80** - доступ по HTTP на данный Веб-интерфейс. Если закрыть этот порт, то связь с контроллером через Веб будет потеряна (лучше оставить открытым).
- Порт **30294** - порт для доступа на технологический HTTP/REST сервер контроллера. Данный функционал доступен только в версиях программного обеспечения начиная с 2022 года. Функций телеуправления по данному порту нет. Если нет необходимости явного использования данной функции, то лучше порт закрыть.
- Порт **102** - используется для подключения к контроллеру по протоколу МЭК 61850-8-1 MMS. Если функция не используется, то лучше порт закрыть.
- Порты вида **4001, 4002, 2222** - обычно используются для транзитного режима для доступа к конечным устройствам - счетчикам и пр. Не используемые порты можно закрыть.

## Права доступа через среду настройки ENLOGIC

Необходимо подключиться к контроллеру через среду настройки ENLOGIC, перейти на вкладку Контроллер:



Нажать на кнопку Установить/изменить пароли:

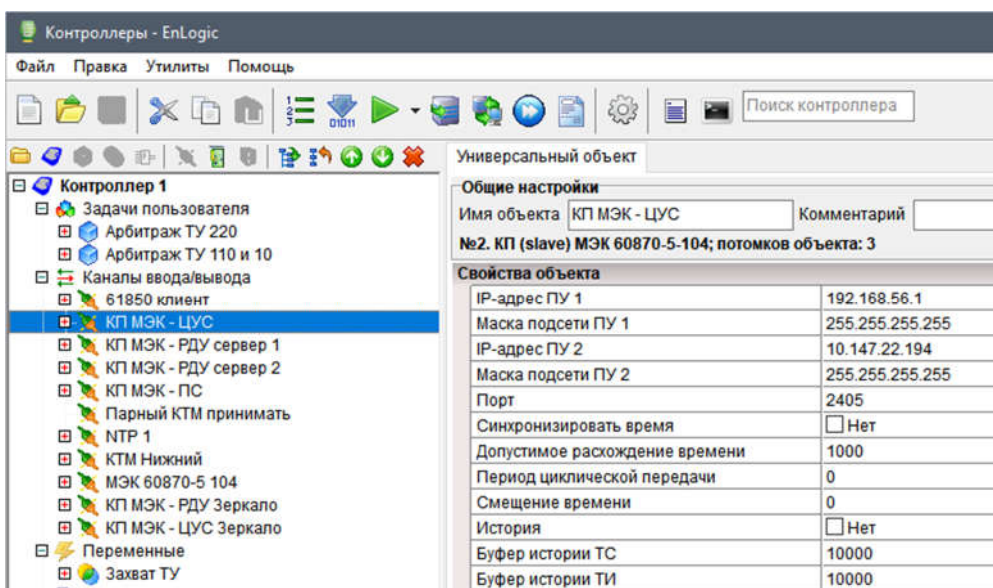


В данном окне надо ввести текущий пароль 3-го уровня, новые пароли, и нажать Ок. Если текущий пароль введен верно, то будет произведена смена паролей всех трех уровней.

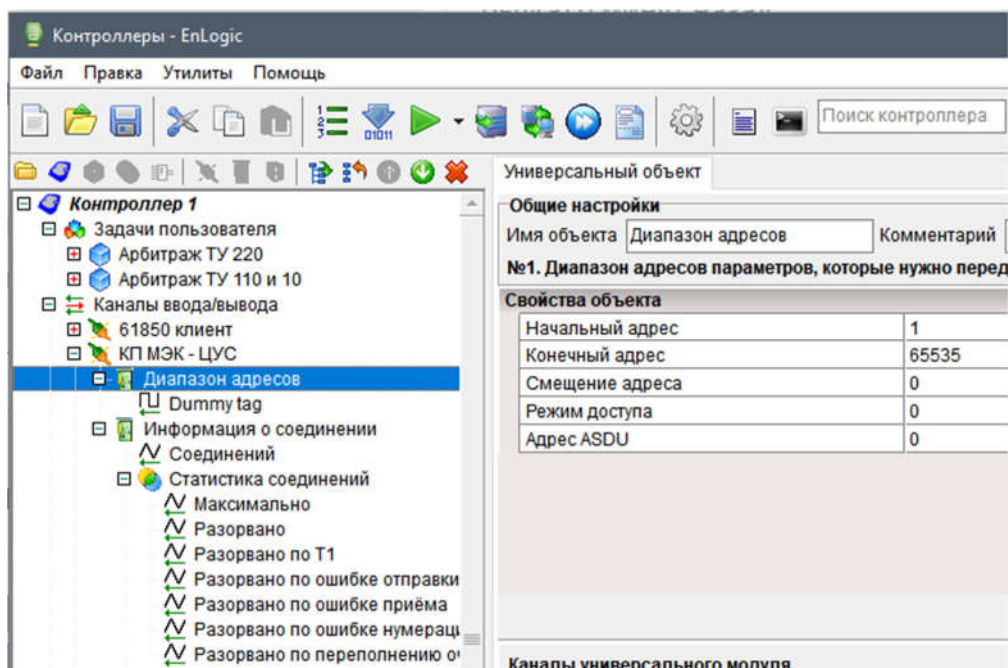
## Доступ по протоколу МЭК-104

Средствами настройки ENLOGIC рекомендуется разрешить подключение по протоколу МЭК-104 только с определенных IP-адресов. В идеале - с IP-адресов только основного и резервного сервера ЦППС/SCADA. Подробные детали настройки можно найти в справочной системе, здесь приведем конкретный пример.

Добавить в контроллер в Каналы ввода/вывода протокол **КП МЭК-104** (группа Телемеханика), и задать у него настройки IP-адресов ПУ (пункт управления, клиент МЭК-104):



В протокол необходимо добавить модуль **Диапазон адресов** с тегом, настройки можно оставить по умолчанию. Также для диагностики рекомендуется добавить модуль **Информация о соединении**:



Далее необходимо загрузить конфигурацию в контроллер.

При такой настройке контроллер будет разрешать подключение по протоколу МЭК-104 только с двух заданных IP-адресов ПУ 1 и ПУ 2.

При задании адреса 192.168.0.X и маски 255.255.255.0 (значение X неважно) - будет разрешено соединение от ПУ в диапазоне адресов от 192.168.0.1 до 192.168.0.254.