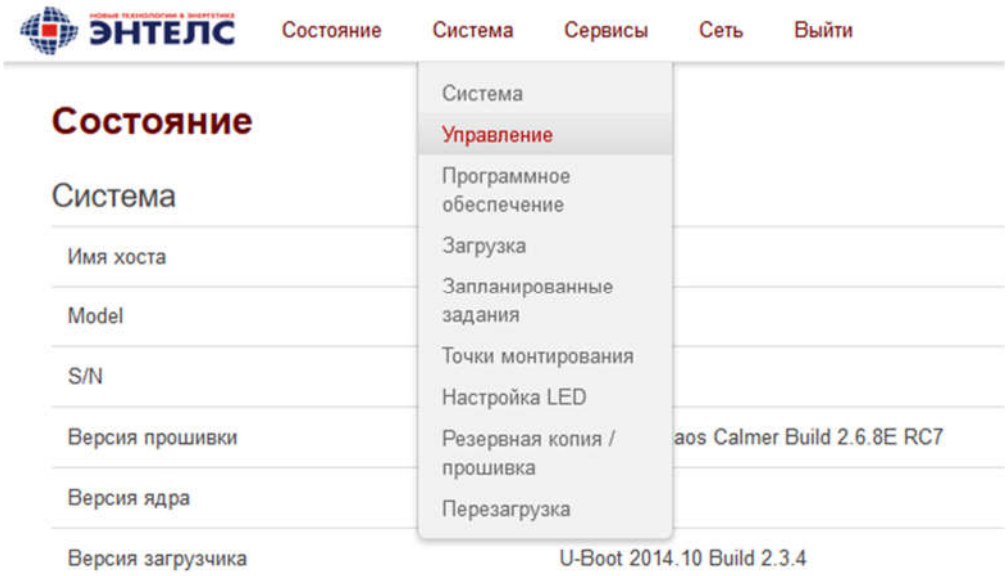
Рекомендации по обеспечению безопасности контроллера E2R2-G

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

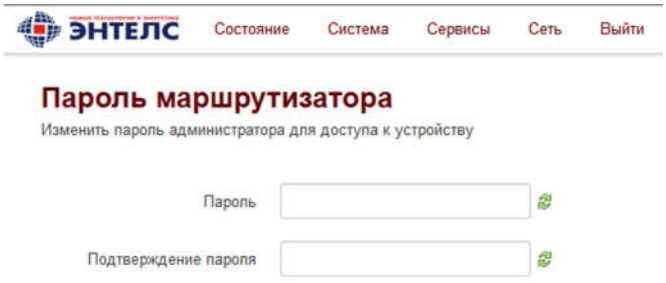
Логин пользователя root

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

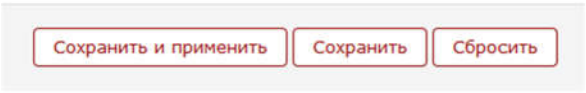
Заходим в Веб-интерфейс, выбираем пункт меню **Система→Управление**:



Меняем пароль

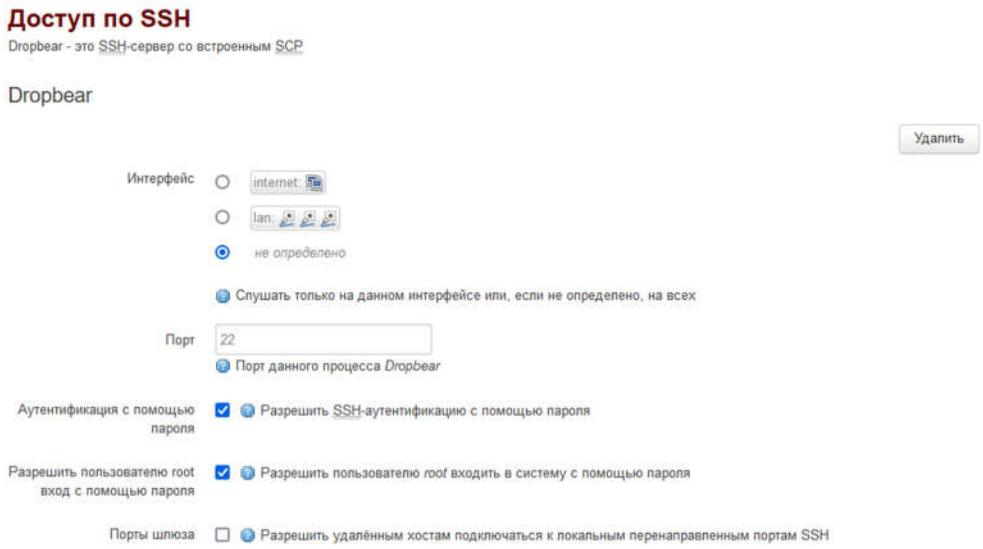


Внизу страницы нажимаем **Сохранить и применить**:

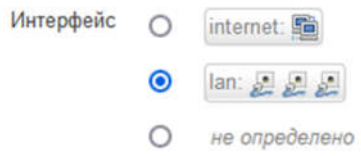


Доступ по SSH

На той же странице есть настройки доступа по SSH:

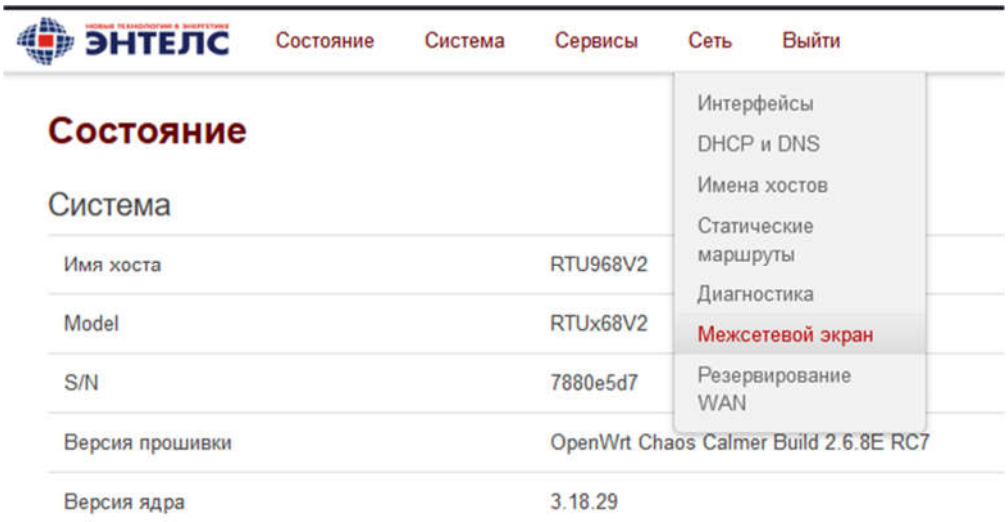


Если **интерфейс** стоит в режиме *не определено*, тогда разрешено подключение по SSH к контроллеру по любому интерфейсу, в том числе по GPRS. Не стоит отключать SSH совсем, но лучше перевести подключение в режим **lan**, тогда подключение по SSH будет доступно только при прямом подключении к контроллеру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

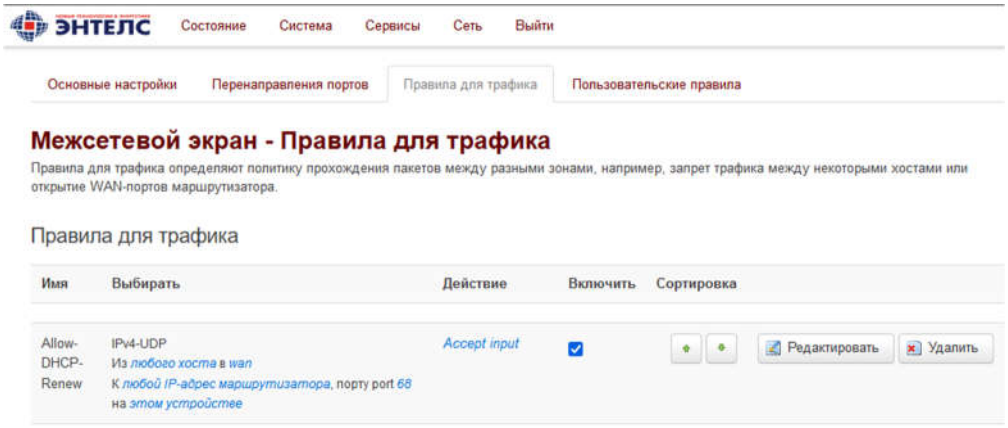


Список открытых портов

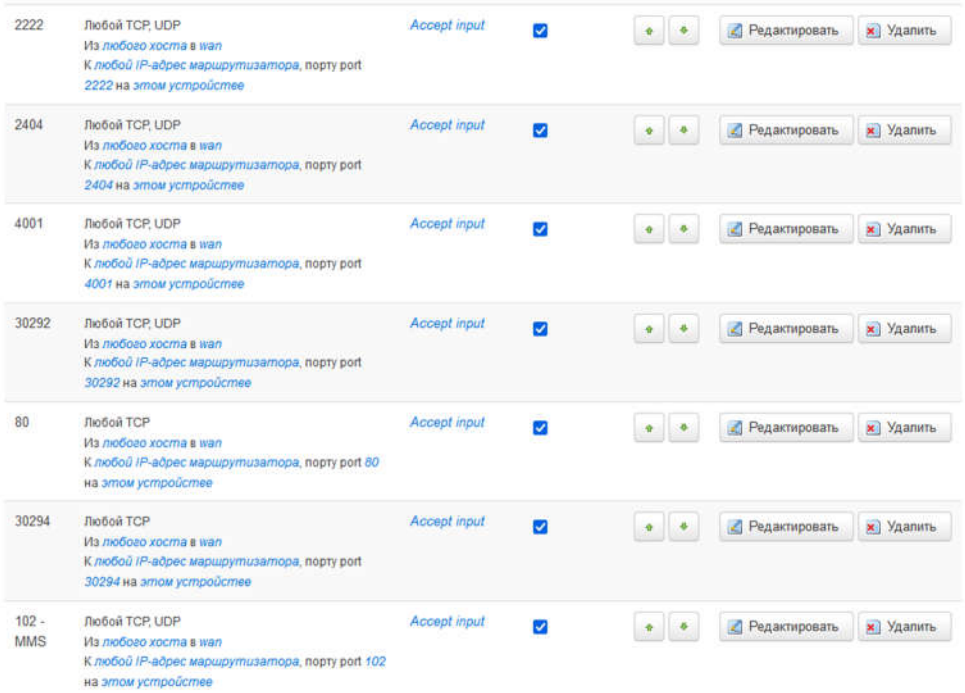
Список TCP/UDP портов, доступных для подключения, настраивается на вкладке **Сеть→Межсетевой экран**:



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



И списка обычно добавленных пользовательских разрешений:



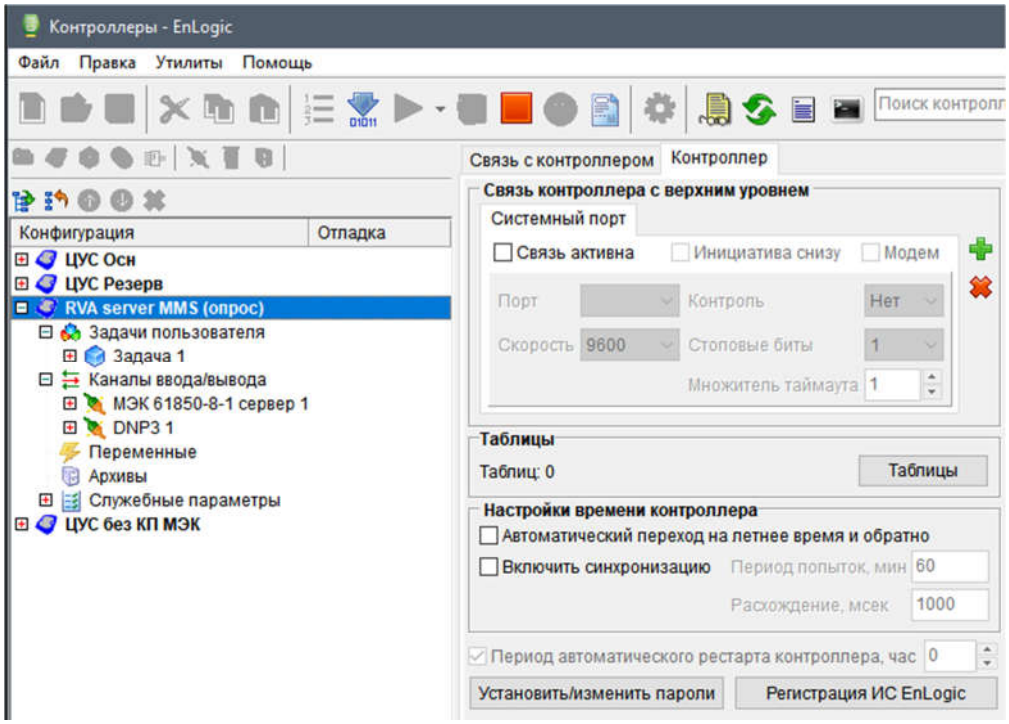
оставить только те порты, которые реально используются.

Порты:

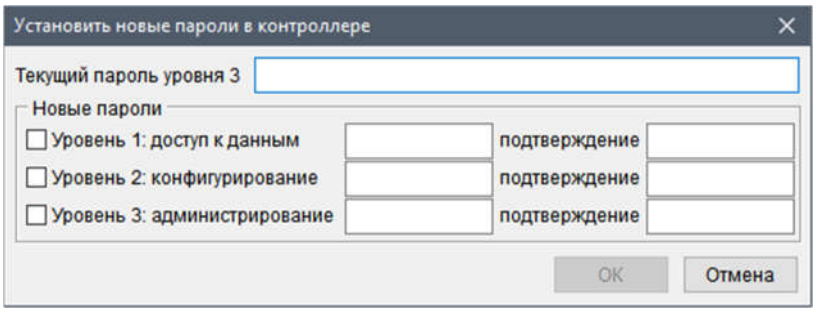
- Порт **2404** - стандартный порт для передачи данных от контроллера по протоколу МЭК 60870-5-104.
- Порт **30292** - порт для связи с контроллером через среду конфигурирования ENLOGIC. Также этот порт используется для передачи данных по протоколу АСКУЭ. Если передача данных АСКУЭ с контроллера не производится (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 подключится к контролеру через среду настройки ENLOGIC, перейти на вкладку Контроллер:



Нажать на кнопку Установить/изменить пароли:

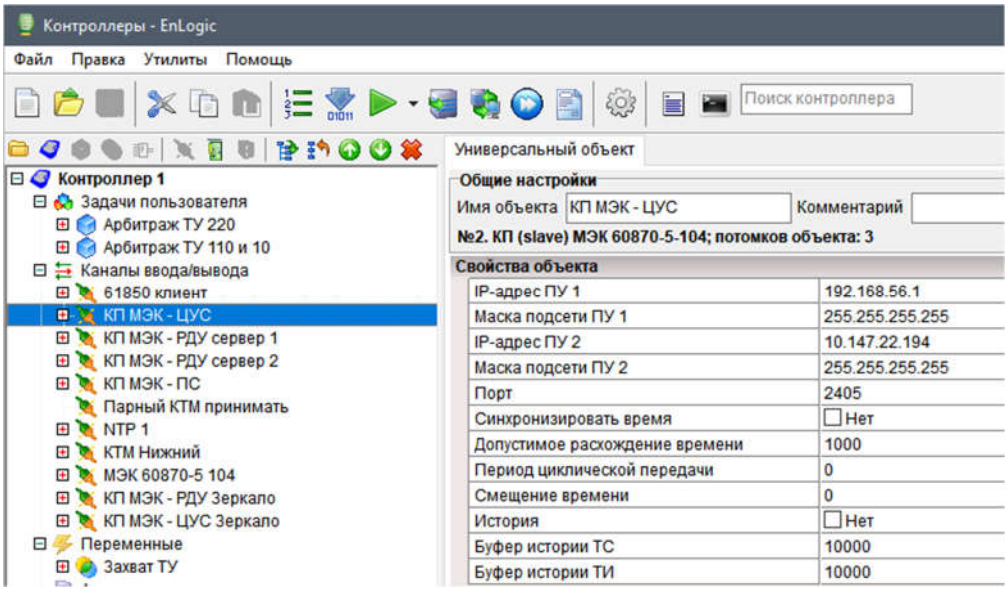


В данном окне надо ввести текущий пароль 3-го уровня, новые пароли, и нажать Ок. Если текущий пароль введен верно, то будет произведена смена паролей всех трех уровней.

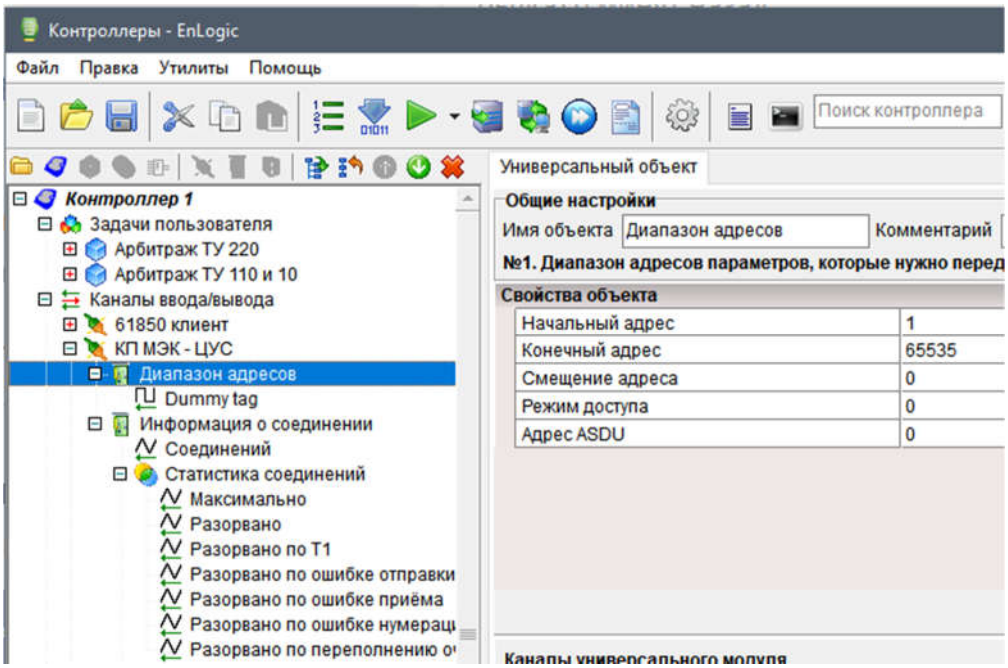
Доступ по протоколу МЭК-104

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.