ИСО 9001

КОНТРОЛЛЕР ПРОГРАММИРУЕМЫЙ ЛОГИЧЕСКИЙ

"М3000-Т ИНСАТ"

Руководство по эксплуатации

АЦДР.421455.003 РЭп

2025

СОДЕРЖАНИЕ

Настоящее руководство по эксплуатации предназначено для ознакомления обслуживающего персонала с устройством, конструкцией, работой и техническим обслуживанием Контроллера программируемого логического «М3000-Т Инсат» версии 3.00 (далее по тексту контроллер или ПЛК). Контроллер выпускается согласно ТУ АЦДР.421455.003 и имеет декларацию соответствия ТР ТС.

В специальных версиях ПО контроллера X.X5 (последняя цифра «5») по сравнению с типовыми версиями при прошивке прибора **принудительно**, **без возможности восстановления**, уменьшается размер eMMC памяти в два раза с целью увеличения ресурса её работы.

Данная версия контроллера работает со Средой Разработки Мастерскада 4Д версии не ниже 1.3.6.22394.

Список принятых определений и сокращений:

Для просмотра всех индексов и кодовых обозначений разъёмов и клеммных колодок – читать Приложение Б.

ЛКМ – левая клавиша мыши;
ПКМ – правая кнопка мыши;
АРМ – автоматизированное рабочее место;
ПК – персональный компьютер;
ПО – программное обеспечение;
ModBus – открытый протокол обмена по сети RS-485, разработан компанией ModiCon, в настоящий момент поддерживается независимой организацией ModBus-IDA (www.ModBus.org);
ModBus-TCP – версия протокола ModBus, адаптированная к работе в сети TCP/IP;
ПЛК – программируемый логический контроллер;
Рабочий режим – штатная работа запрограммированного контроллера;
FBD (англ. **F**unction **B**lock **D**iagram) – графический язык программирования стандарта МЭК 61131-3 для программирования программируемых логических контроллеров;
SFC (англ. **S**equential **F**unction **C**hart) – графический язык стандарта МЭК 61131-3 последовательного функционального управления, позволяющий однозначно определить поведение системы управления;
LD (англ. **L**adder **D**iagram) – графический язык релейной (лестничной) логики стандарта МЭК 61131-3;
ST (англ. **S**tructured **T**ext) – не графический язык высокого уровня (типа Паскаля) стандарта МЭК 61131-3;
IL (англ. **I**nstruction **L**ist) – не графический язык низкого уровня (типа Ассемблера) стандарта МЭК 61131-3;
Host – устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах;
DHCP (англ. **D**ynamic **H**ost **C**onfiguration **P**rotocol / рус. «Протокол Динамической Настройки Узла») – технология, предназначенная для автоматического присвоения IP-адресов сетевым устройствам;
DNS (англ. **D**omain **N**ame **S**ystem «система доменных имён») – компьютерная распределённая система для получения информации о доменах;
NTP (англ. **N**etwork **T**ime **P**rotocol) – протокол синхронизации внутренних часов компьютера и сетевого оборудования внутренней сети;

NTP-сервер – сервер точного времени, предназначенный для синхронизации внутренних часов компьютеров и сетевого оборудования по протоколу NTP;

WPA2 (англ. **W**i-Fi **P**rotected **A**ccess **2**) **–** обновлённая программа сертификации устройств беспроводной связи;

PSK (англ. **P**re-**S**hared **K**ey) – это согласованный ключ (идентификационная фраза) в формате ASCII на обоих концах беспроводного соединения. Идентификационная фраза должна быть от 8 до 63 символов;

WPA2-PSK – упрощённый режим работы сети, позволяющий использовать один пароль, хранящийся непосредственно в маршрутизаторе;

SSID (англ. **S**ervice **S**et **I**dentifier) – идентификатор (название, имя) беспроводной сети;

HTTPS (англ. **H**yper **T**ext **T**ransfer **P**rotocol **S**ecure) – расширение протокола HTTP для шифрования в целях безопасности;

FTP (англ. **File T**ransfer **P**rotocol) – протокол передачи файлов по сети;

PuTTY – свободно распространяемый клиент для различных протоколов удалённого доступа включая SSH, Telnet, rlogin и предоставляющий возможность связи по последовательному порту;

SSL (англ. **S**ecure **S**ockets **L**ayer / рус. Уровень защищённых сокетов) – криптографический протокол защиты связи;

TLS (англ. **T**ransport **L**ayer **S**ecurity**)** – протокол защиты транспортного уровня – улучшенный вариант SSL;

WSS (от англ. **W**eb**S**ocket **S**ecurity**)** – протокол защиты соединения;

PKI (англ. **P**ublic **K**ey **I**nstruction) – инфраструктура открытых ключей. Совокупность сервисов для управления ключами и цифровыми сертификатами пользователей, программ и систем;

CSR (англ. **C**ertificate **S**igning **R**equest**)** – запрос на получение сертификата;

RSA (англ. фамилии авторов **R**ivest, **S**hamir и **A**dleman**)** – криптографический алгоритм с открытым ключом;

SSH (англ. **S**ecure **S**hell **/** рус. Безопасная оболочка), сетевой протокол прикладного уровня передачи данных, позволяющий производить удалённое управление операционной системой и туннелирование.

1. ОБЩИЕ СВЕДЕНИЯ

Контроллер, программируемый логический «М3000-Т Инсат» АЦДР.421455.003 (в дальнейшем – контроллер или ПЛК), предназначен для:

- совместного использования с подчиненными устройствами, работающими по протоколу ModBus RTU;
- для создания систем автоматизированного управления технологическим оборудованием и диспетчеризации.

1. Логика работы ПЛК определяется потребителем в процессе программирования контроллера. Программирование осуществляется с помощью программного обеспечения MasterSCADA 4D. При этом поддерживаются все языки программирования, указанные в МЭК 61131-3.
2. Область применения ПЛК: системы автоматизированного управления технологическим оборудованием в энергетике, на транспорте, в различных областях промышленности, жилищно-коммунального и сельского хозяйства.

Конструкция контроллера не предусматривает его использование в условиях воздействия агрессивных сред, пыли, а также во взрывопожароопасных помещениях.

2. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Основные технические характеристики контроллера приведены в таблице 1.

Таблица 1. Основные технические характеристики контроллера

Наименование характеристики	Значение
Аппаратные характеристики	
Центральный процессор	Cortex™-A7 4Core 1.2 GHz
Объем оперативной памяти (тип памяти)	1GB DDR4
Объем встроенной энергонезависимой памяти	8 GB MLC
Объем энергонезависимой памяти доступно пользователю (тип памяти)	4 GB
Дополнительное оборудование	– держатель SD-карты – часы реального времени – элемент питания
Программные характеристики	
Операционная система	Linux
Среда разработки	MasterSCADA 4D
Встроенная среда исполнения	MasterSCADA 4D
Языки программирования	FBD/SFC/LD/ST/IL (Стандарт МЭК 61131-3)
Электропитание контроллера	
Количество входов питания	2
Диапазон напряжения питания, В	от 10,2 до 28,4 постоянного тока
Минимальное напряжение батарейки часов контроллера CR2032 для исправной работы, В	2,2
Потребляемый ток, без подключенных устройств, мА - при напряжении питания 12В - при напряжении питания 24В	 не более 260 не более 140
Интерфейсы передачи данных	
Электрическая прочность изоляции линий RS-485 (как между линиями RS-485 и остальной частью схемы, так и между разными каналами линии RS-485), Вольт в течение минуты (АС 50 Гц).	1000 (в нормальных условиях) 500 (в условиях предельной/повышенной влажности и/или повышенной запылённости)
Количество интерфейсов RS-485 (гальванически развязаны)	4
Сопротивление оконечных резисторов RS-485, Ом	120
Количество интерфейсов RS- 232 для подключения устройств	1
Количество интерфейсов Ethernet с поддержкой стандартов 10BASE-T и 100BASE-TX (10/100)	1
Количество интерфейсов USB	USB Host (USB-A) – 1 шт. Micro USB (ограниченная поддержка режима USB OTG) – 1 шт.
Технические характеристики корпуса	
Габаритные размеры контроллера, мм	156x107x39
Степень защиты оболочки по ГОСТ 14254-96	IP30
Масса контроллера, кг	не более 0,3

Эксплуатационные параметры	
Диапазон температур, °С	от минус 20 до плюс 55
Время непрерывной работы контроллера	круглосуточно
Время выполнения пустого цикла, миллисекунд	1 (настраивается в основной задаче) ПО MasterScada4D.
Средняя наработка контроллера на отказ в дежурном режиме работы, ч	не менее 80000
Вероятность безотказной работы за 1000 ч	0,98758
Средний срок службы контроллера, лет	10
Срок работы батарейки часов контроллера CR2032, лет	1
Время технической готовности контроллера к работе, с	не более 30
Индустриальные радиопомехи, создаваемые контроллером по ГОСТ Р 51318.22 (СИСПР22—2006) п. 5.1, 6.1	не ниже третьей степени жёсткости
Устойчивость к механическим воздействиям по ОСТ 25 1099-83	категория размещения 03
Устойчивость к климатическим воздействиям по ОСТ 25 1099-83	исполнение О3

*в зависимости от исполнения контроллера

3. КОМПЛЕКТНОСТЬ

Наименование	Количество, шт.	Примечание
Контроллер «М3000-Т Инсат» АЦДР.421455.003	1	
Комплект запасных частей и принадлежностей (ЗИП): Шуруп 1-3х25.016 ГОСТ 1144-80 Дюбель 6х30 Винт-саморез 2,2 х 6,5 оц. DIN 7982	 3 3 1	
«М3000-Т Инсат» АЦДР.421455.003 РЭ. Руководство по эксплуатации	1	

4. КОНСТРУКЦИЯ, МОНТАЖ, ПОДКЛЮЧЕНИЕ

4.1 Меры безопасности

Меры безопасности при подготовке изделия:

– конструкция контроллера удовлетворяет требованиям электро- и пожарной безопасности по ГОСТ 12.2.007.0-75 и ГОСТ 12.1.004-91;

– контроллер не имеет цепей, находящихся под опасным напряжением;

– конструкция контроллера обеспечивает его пожарную безопасность в аварийном режиме работы и при нарушении правил эксплуатации согласно ГОСТ 12.1.004-91;

– монтаж, установку, техническое обслуживание производить при отключенном напряжении питания контроллера;

– обслуживание контроллера (замену батарейки часов и т.д.) производить **исключительно** при соблюдении мер защиты от статического электричества в соответствии с ГОСТ 12.1.018-93;

– монтаж и техническое обслуживание контроллера должны производиться лицами, имеющими квалификационную группу по технике безопасности не ниже второй.

4.2 Конструкция

Внешний вид контроллера, а также габаритные и установочные размеры контроллера показаны в Приложении А.

4.3 Монтаж контроллера

Монтаж контроллера проводится следующим образом:

- контроллер устанавливается на стенах или в специальных шкафах, также в других конструкциях в местах, защищённых от воздействия атмосферных осадков и механических повреждений;
- контроллер закрепляется на стене в удобном месте или в шкафу с установленной DIN-рейкой. Если контроллер устанавливается в неохраняемом помещении, рекомендуется устанавливать его на высоте не менее 2,2 м от пола;

4.4 Подключение контроллера

Схема внешних подключений приведена в Приложении Б.

4.4.1 Подключение линий интерфейса RS-485.

Для подключения к сетевому контроллеру по магистральному интерфейсу RS-485 необходимо:

а) контакты "A" и "B" клемм XT3/XT4/XT5/XT6/XT7 подключить соответственно к линиям A и B интерфейса RS-485;

б) подключить цепь GND – "0В" («земля») контроллера к аналогичной цепи предыдущего и последующего контроллеров в магистрали RS-485 (если контроллеры подключены к одному источнику питания, то это делать не обязательно).

При прокладке провода интерфейса RS-485 рекомендуется соединять контроллеры "в цепочку". Если из каких-либо соображений требуется сделать ответвление значительной протяженности (более 50 м) от общей магистрали RS-485 (например, для уменьшения длины кабеля), то в месте ответвления рекомендуется установить повторитель интерфейса "С2000−ПИ".

4.4.2 Включение контроллера.

Перед подачей питания на контроллер следует проверить правильность подключения напряжения и его уровень:

- при напряжении ниже 10В работа контроллера не гарантируется (контроллер прекращает функционировать, однако, из строя не выходит);
- при превышении напряжения питания уровня 28В возможен выход контроллера из строя.

При подаче на ПЛК напряжения питания допустимого диапазона на лицевой стороне корпуса загорается индикатор «Работа».

5. ОПИСАНИЕ И РАБОТА ИЗДЕЛИЯ

5.1 Световая индикация

Контроллер формирует визуальные сигналы на световые индикаторы (светодиоды), расположенные на лицевой панели, отражающие состояние контроллера и его интерфейсов.

Извещения, выдаваемые на светодиоды "Работа" и светодиоды интерфейсов контроллера приведены в таблицах 2 и 3 соответственно.

Таблица 2. Светодиод «Работа»

Состояние контроллера	Содержание извещения
Рабочий режим	Индикатор включен

Таблица 3. Светодиоды интерфейсов

Состояние интерфейса контроллера	Режим свечения
Передача пакета на интерфейсе	Мигает зелёный
Приём пакета на интерфейсе	Мигает желтым

5.2 Подключение контроллера к компьютеру

По перечисленным ниже интерфейсам предоставляется доступ к Linux-консоли.

Подключение контроллера к компьютеру производится с использованием «HyperTerminal», «PuTTY» и других программ по следующим интерфейсам:

– USB интерфейса (разъём MicroUSB (индекс на схеме – **X1**) с поддержкой спецификации USB OTG);

– по интерфейсу Ethernet (индекс разъёма на схеме – **XS2**) с использованием программ «HyperTerminal», «PuTTY» или их аналогами.

Логин пользователя по умолчанию: «**root**».
Пароль пользователя по умолчанию: «**p@ssw0rd1234**».

5.3 Настройка контроллера через браузер

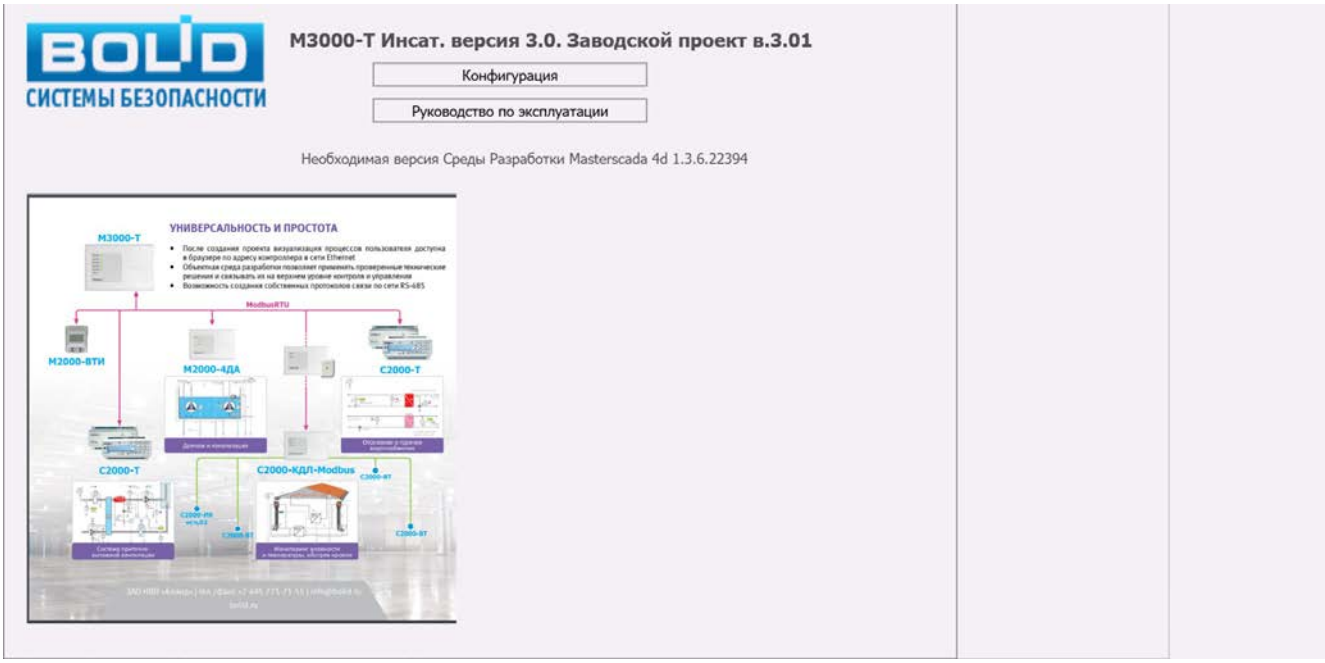
Доступ к настройке контроллера в веб-браузерах возможен через браузеры на мобильных устройствах (iOS, Android выше 8 версии) и через версии настольные веб-браузеры: браузеров Chromium (136.0.7103.48 от 24 апреля 2025 года), Firefox, а также Safari (в ограниченном виде).

Внимание!

Работа веб-конфигуратора осуществляется в браузере только на одной вкладке! При попытке вторичной авторизации в конфигураторе на другой вкладке этого же браузера будет отображаться ошибка!

Веб-интерфейс контроллера сочетает в себе два проекта: заводской и пользовательский (создаётся непосредственно пользователем в среде разработки MasterSCADA и в РЭп не описывается).

Заводской проект доступен по ссылке http://ip_device (где «ip_device» – текущий сетевой адрес контроллера (по умолчанию - 192.168.0.50; в случае подключения по спецификации USB OTG, ПЛК становится сетевым устройством, сетевой адрес - 10.255.127.5)) и имеет внешний вид, представленный на рисунке ниже.



Веб-интерфейс. Заводской проект контроллера.

Есть возможность перейти в веб-конфигуратор или прочитать текущее Руководство по эксплуатации контроллера.

Заводской проект позволяет пользователю увидеть необходимую версию среды разработки MPLC для создания пользовательского проекта, а также позволяет перейти к Руководству по эксплуатации и зайти в веб-конфигуратор для непосредственной настройки контроллера.

Открытие веб-конфигуратора производится переходом из заводского/пользовательского проекта или же записью в адресной строке браузера URL-адреса: http://ip_device/bolid_web_cfg, где «**ip_device**» – текущий сетевой адрес контроллера (по умолчанию - 192.168.0.50; в случае подключения по спецификации USB OTG, ПЛК становится сетевым устройством, сетевой адрес - 10.255.127.5).

После выполнения этой команды появляется окно авторизации, представленное на Рисунке 1.

Логин при входе через браузер: **«admin»**,
пароль пользователя по умолчанию: «**p@ssw0rd1234**».

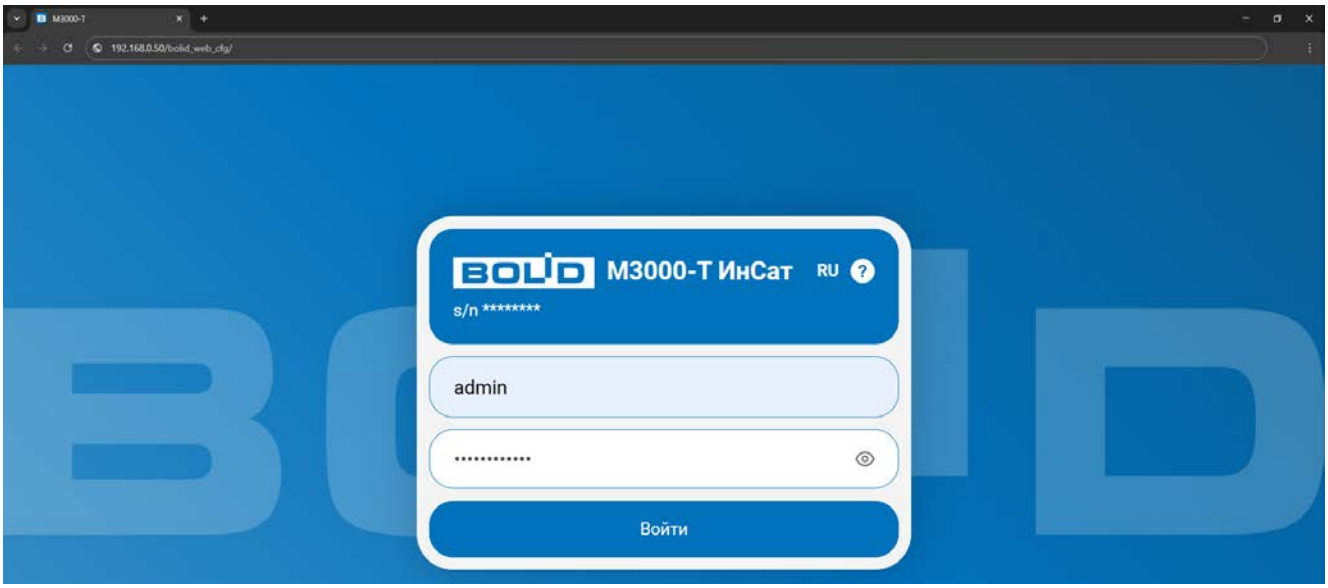


Рисунок 1. Приветственное окно веб-конфигуратора.
Окно авторизации.

5.3.1 Верхняя панель веб-конфигуратора

Общий вид верхней панели конфигуратора представлен на Рисунке 2.

Верхняя панель веб-конфигуратора позволяет администратору переходить на страницы, связанные с просмотром и изменением настроек контроллера.

Всего в веб-конфигураторе имеется 6 страниц для настройки систем контроллера: «MPLC», «Пользователи», «Настройки сети», «SSL-сертификаты», «Настройки времени» и «Сервисное обслуживание» - они указаны на центральной части панели; выбранная страница отмечается округленным прямоугольником.

В левой части панели присутствует обособленная плашка, на которой можно увидеть:

— серийный номер устройства (под логотипом компании, после слова «**s/n**» (англ. «**serial number**»);

— возможность смены языка интерфейса (представленного на русском и английском языках);

— а также кнопку с символом вопроса, при нажатии на которую появляется окно с основной информацией о контроллере (*читать п. 5.3.2 «Окно с основной информацией о контроллере»).*

Справа расположено имя текущего пользователя, и кнопка выхода из веб-конфигуратора.

Рисунок 2. Верхняя панель веб-конфигуратора.

5.3.2 Окно с основной информацией о контроллере

Данное окно вызывается нажатием на иконку вопроса на обособленной плашке в верхней панели веб-конфигуратора. В нем отображена следующая информация об устройстве (*см. Рис. 3*):

- дата сборки прошивки устройства;
- отображаемое имя устройства;
- модель системы («М3000-Т-InSat»);
- аппаратная версия устройства;
- дата изготовления устройства;
- серийный номер устройства;
- версия программного обеспечения.

Рисунок 3. Окно с дополнительной информацией о контроллере на верхней панели конфигуратора.

5.3.3 Страница «MPLC»

Общий вид страницы представлен на Рисунке 4. Страница предназначена для предоставления пользователю дополнительной информации о среде разработки, а также обладает возможностью резервного копирования и восстановления проекта MasterSCADA (подробно о восстановлении проекта *читать п. 5.3.8 «Информация о памяти»*).

В нижней части страницы присутствует окно «Операции»: оно позволяет пользователю создавать резервные копии созданного пользовательского проекта в среде разработки MasterSCADA 4D, а также загружать их при необходимости (в случае обновления, сдачи ПЛК в ремонт).

Скачивание и восстановление резервных копий происходит при помощи соответствующих кнопок ниже предупреждения:

- «Скачать резервную копию» - позволяет администратору скачать резервную копию загруженного в контроллер проекта MasterSCADA с желаемым расширением;
- Восстановить из резервной копии – позволяет администратору записать сохраненную резервную копию проекта в контроллер;
- Удалить data.db – даёт возможность удалить базу данных контроллера, что приведёт к удалению всех данных контроллера, включая и текущий пользовательский проект. После этого, ПЛК будет необходимо восстановить.

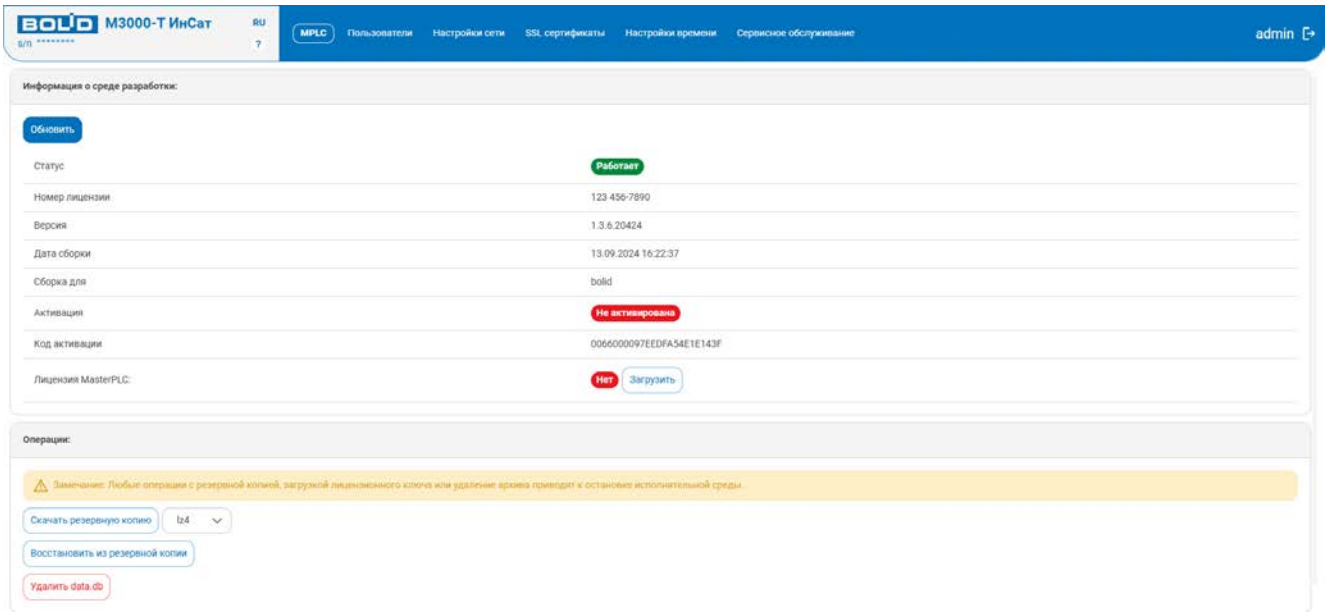


Рисунок 4. Страница «MPLC».
Окно с показом информации о среде разработки контроллера.

5.3.4 Страница «Пользователи»

Общий вид страницы представлен на Рисунках 5 и 6. Страница предназначена для добавления и удаления пользователей, смены паролей, а также просмотра подключений к веб-конфигуратору (рисунки предоставлены соответственно).

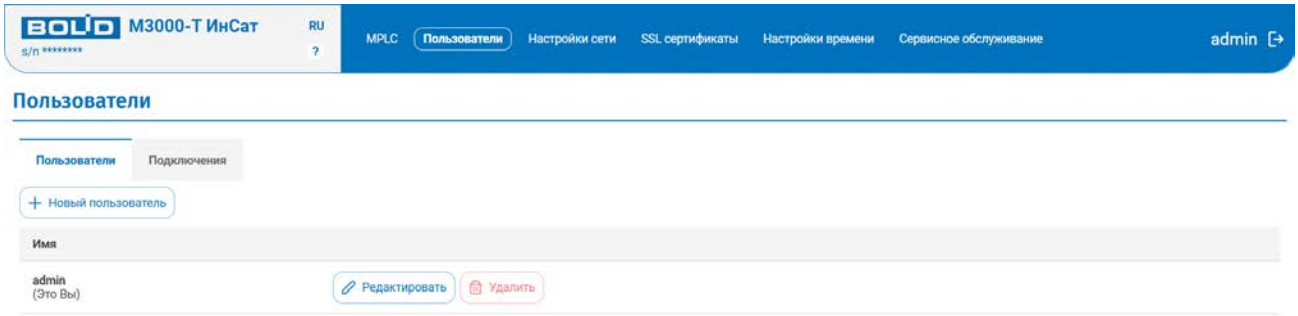


Рисунок 5. Страница «Пользователи».
Вкладка добавления и удаления пользователей.

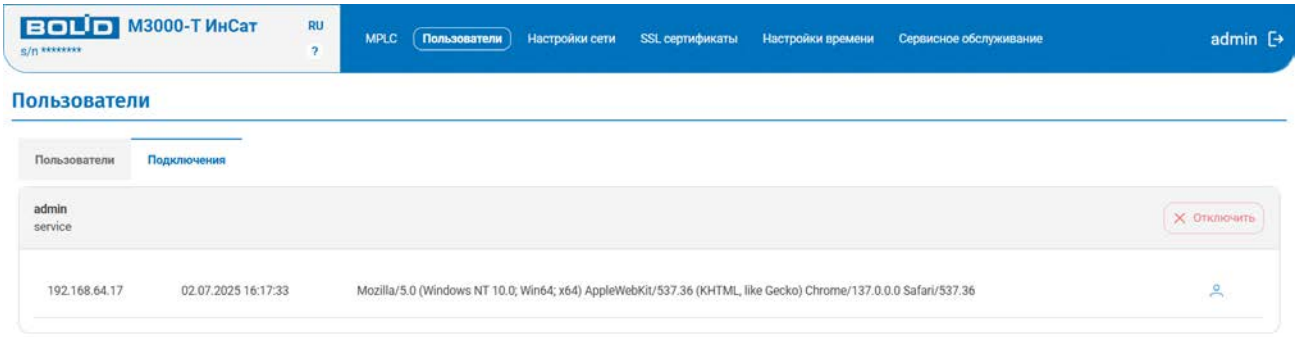


Рисунок 6. Страница «Пользователи».
Вкладка подключений к контроллеру.

5.3.5 Страница «Настройки сети»

Страница разделена на 4 вкладки: «Общие», «Wi-Fi», «Модем», и «Ethernet» (пункты по данным вкладкам отмечаются цифрами 1, 2, 3, 4 после написания номера пункта 5.3.5 соответственно).

Общий вид страниц представлен на рисунках 7, 8, 9 и 10 соответственно:

Параметры вкладки «Общие» описаны в таблице 4;
параметры вкладки Wi-Fi – в таблице 5;
параметры настройки интернет-протокола IPv4 – в таблице 6;
параметры вкладки «Модем» – в таблице 7;
параметры вкладки Ethernet – в таблице 8.

5.3.5 – 1 – Вкладка «Общие» и её настройка

Данная вкладка позволяет настроить имя устройства при подключении к нему при помощи интернет технологий (Ethernet, Wi-Fi и режим модема).

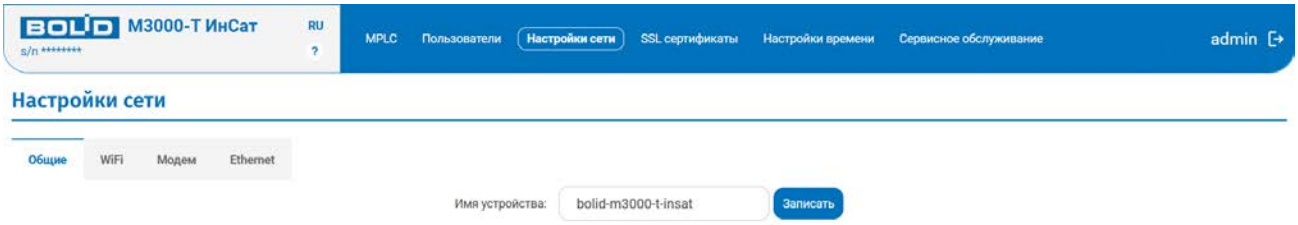


Рисунок 7. Настройки сети, вкладка «Общие».

Таблица 4. Описание параметров настройки сети, вкладка «Общие»

Вкладка «Общие»		
Название параметра	**Значение по умолчанию**	**Описание**
Имя устройства	bolid-m3000t-insat	Hostname устройства

5.3.5 – 2 – Вкладка «Wi-Fi» и её настройка (в случае если к контроллеру подключен поддерживаемый USB-Wi-Fi адаптер)

Вкладка «Wi-Fi» страницы «Настройки сети» располагает тремя возможностями настройки режима работы контроллера по беспроводной технологии Wi-Fi:

1) технология выключена (невозможность беспроводного подключения) (*читать п. **5.3.5 – 2.1** см. Рис. 8, поз. 1*);

2) технология включена и выступает в виде клиента для точки доступа Wi-Fi (*читать п, **5.3.5 – 2.2**, см. Рис. 8, поз. 2, поз. 3, поз. 4 – автоматическое подключение; см. Рис 8, поз. 5 – ручное подключение*);

3) технология включена и выступает в виде точки доступа для подключения к контроллеру (*читать п. **5.3.5 – 2.3**, см. Рис. 8, поз. 6*).

5.3.5 – 2.1 – Вкладка «Wi-Fi»; Wi-Fi модуль выключен

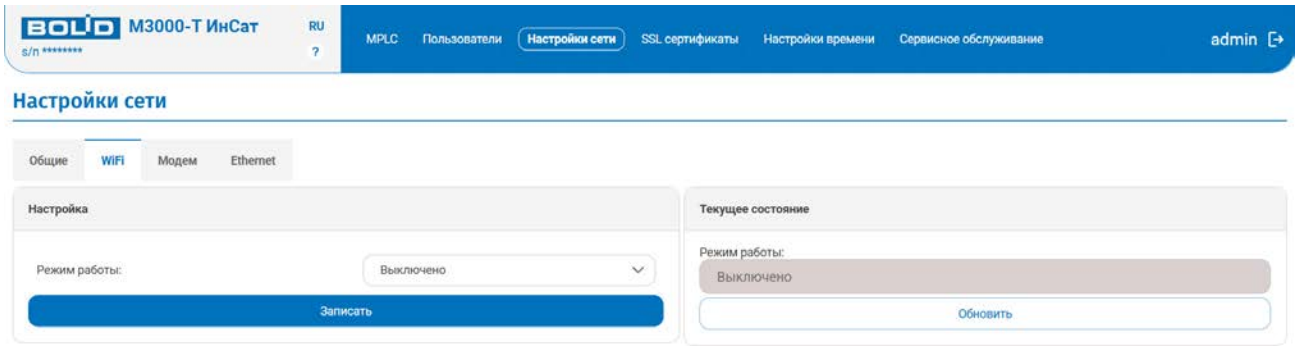


Рисунок 8, позиция 1. Настройки сети, вкладка «Wi-Fi».
Wi-Fi модуль ПЛК выключен.

5.3.5 – 2.2 – Вкладка «Wi-Fi»; ПЛК представлен в виде клиента

Данная настройка позволяет администратору изменять режим работы Wi-Fi модуля ПЛК, просматривать список точек Wi-Fi и подключаться к ним.

– Для осуществления подключения к отображаемой Wi-Fi точке, следует перевести режим работы модуля из состояния «Выключено» в состояние «Клиент», после чего нажать на нужную точку Wi-Fi среди списка доступных (*см. Рис. 8, поз. 2*). Затем следует ввести пароль и выбрать способ настройки IPv4 (автоматически через DHCP или вручную*, *см. Рис. 8, поз. 3* и *Рис. поз.4* соответственно).

***смотреть Таблицу 6.**

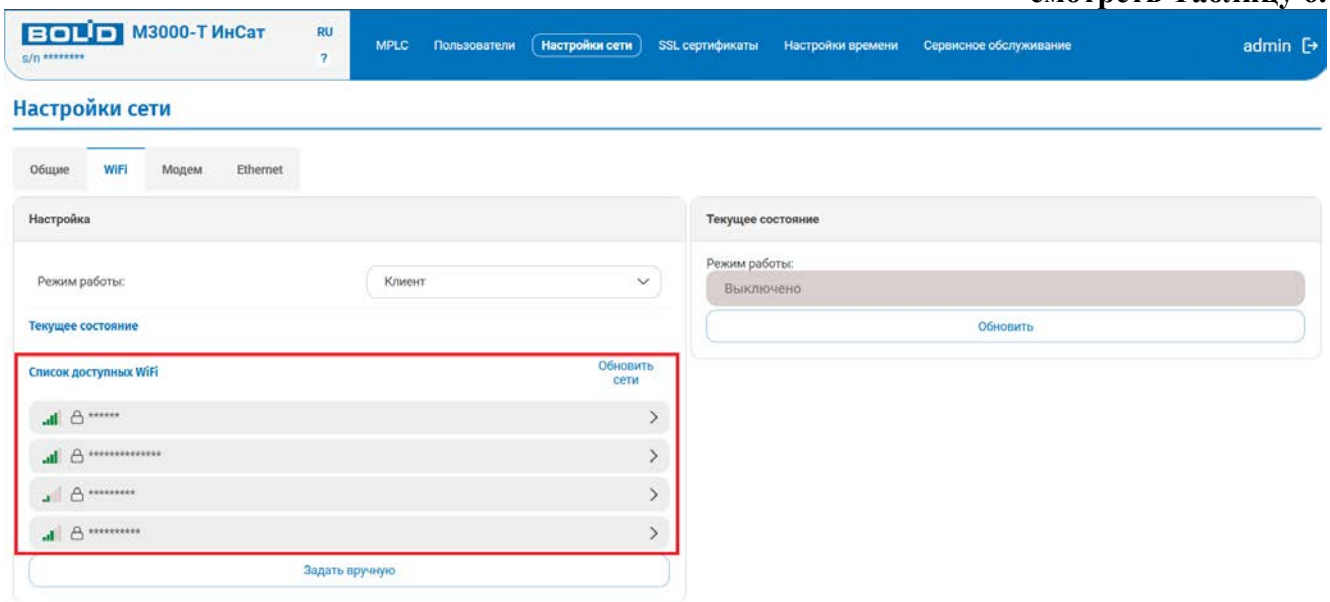


Рисунок 8, позиция 2.
Настройки сети, вкладка"Wi-Fi". Подключение к открытой Wi-Fi точке.
Список доступных подключений выделен красным прямоугольником.

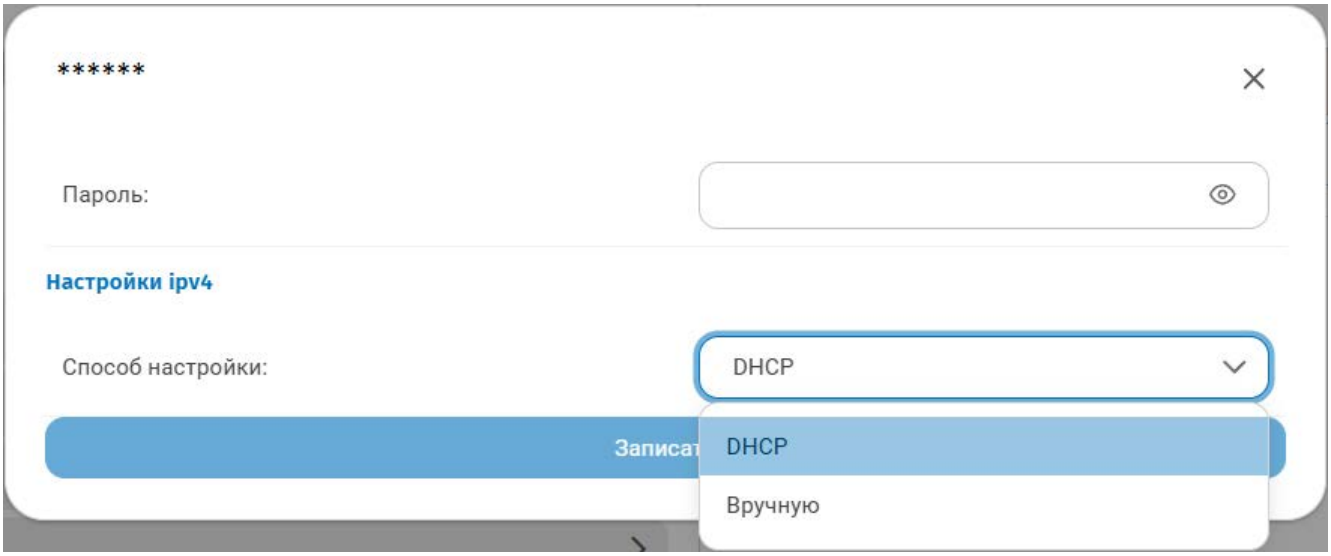


Рисунок 8, позиция 3.
Настройки сети, вкладка "Wi-Fi". Подключение к открытой Wi-Fi точке.
Настройка IPv4 путём DHCP.

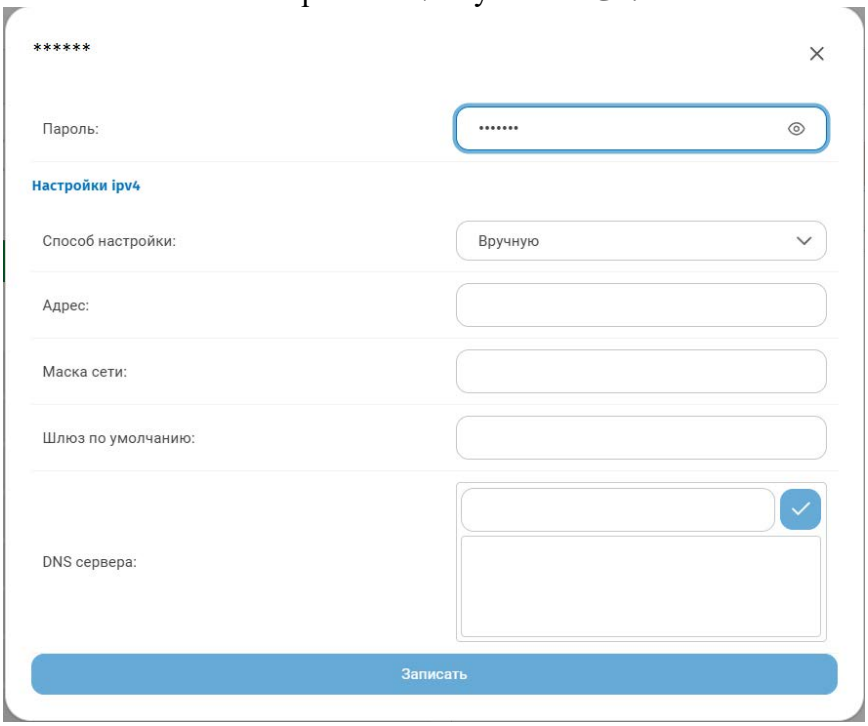


Рисунок 8, позиция 4. Настройки сети, вкладка "Wi-Fi".
Подключение к открытой Wi-Fi точке.
Настройка IPv4 путём ручного выставления параметров.

– Для осуществления подключения к неотображаемой Wi-Fi точке, следует перевести режим работы модуля из состояния «Выключено» в состояние «Клиент», после чего нажать на параметр «**задать вручную**»* (находится ниже списка доступных точек Wi-Fi) и вписать нужные характеристики подключения (*см. Рис. 8, поз. 5)*.

***параметры данного подключения показаны в таблицах 6 и 7.**

Внимание!

В режиме ручного подключения к Wi-Fi точке IPv4 может настраиваться как автоматически (при помощи DHCP-сервера), так и вручную. Этот процесс ничем не отличается от того, что показан на рисунке 8, позиции 4.

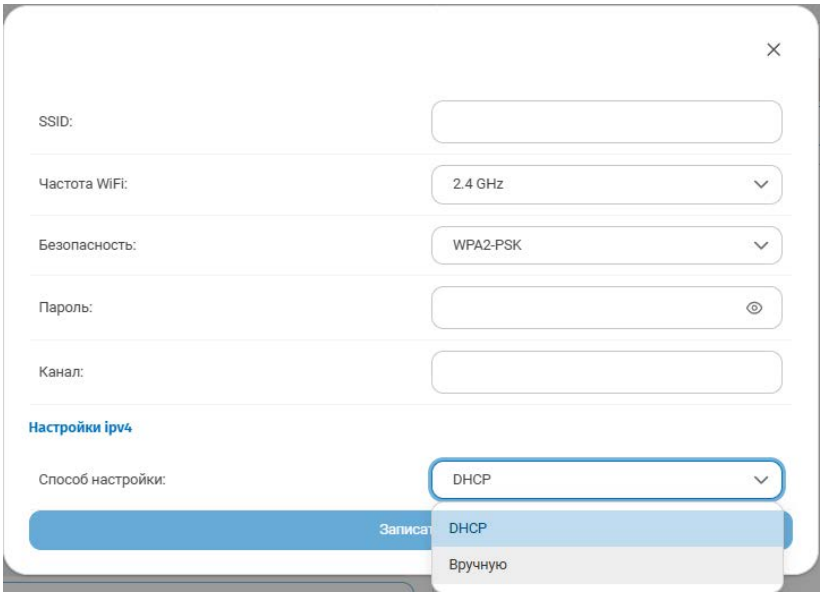


Рисунок 8, позиция 5. Настройки сети, вкладка "Wi-Fi". Ручное подключение к точке.
Ручное выставление параметров подключения к Wi-Fi точке.

Таблица 5. Описание параметров, вкладка «Wi-Fi»

Вкладка «Wi-Fi», работа модуля Wi-Fi представлена как «Точка доступа»		
Название параметра	**Значение по умолчанию**	**Описание**
Частота Wi-Fi	2.4 GHz	Частота работы Wi-Fi соединения Возможные значения: • 2.4 GHz • 5 GHz
SSID	Bolid-C3000Hub	Идентификатор сети
Безопасность	WPA2-PSK	Тип безопасности беспроводной сети
Пароль	C3000hub-серийный номер прибора (буквы латинские)	Пароль для подключения к беспроводной сети
Канал	1	Номер канала Wi-Fi

Таблица 6. Описание параметров настройки IPv4

<table>
<tr><th colspan="3">Настройки IPv4</th></tr>
<tr><td>Параметр настройки</td><td>Стандартное значение</td><td>Тип задания IP-адреса, маски сети, шлюза
Возможные значения:
• DHCP
• Вручную</td></tr>
<tr><td>Адрес</td><td>172.20.0.50</td><td rowspan="4">Сетевые настройки Wi-Fi доступны для редактирования, в случае если режим работы указан «Вручную».</td></tr>
<tr><td>Маска</td><td>255.255.255.0</td></tr>
<tr><td>Шлюз</td><td>-</td></tr>
<tr><td>DHCP-сервер</td><td>Включен

Диапазон адресов:
с 172.20.0.50
по 172.20.0.75</td></tr>
<tr><td colspan="3">На вкладке «Wi-Fi» параметры размещены в двух областях: в области справа отображаются текущие выставленные настройки, которые работают в данный момент времени (работающие настройки). В области слева «Настройка» параметры конфигурации можно изменять. Эти параметры применяются после нажатия на кнопку «Записать».</td></tr>
</table>

5.3.5 – 2.3 – Вкладка «Wi-Fi»; ПЛК представлен в виде точки доступа

Данная вкладка позволяет администратору изменять режим работы Wi-Fi модуля, и превращать ПЛК в точку доступа Wi-Fi для последующего подключения к нему устройств.

– Для осуществления работы данного режима работы модуля, необходимо перейти в настройку «Точка доступа» во вкладке «Wi-Fi» и выставить параметры, соответствующие параметрам, заданным в таблицах 5 и 6.

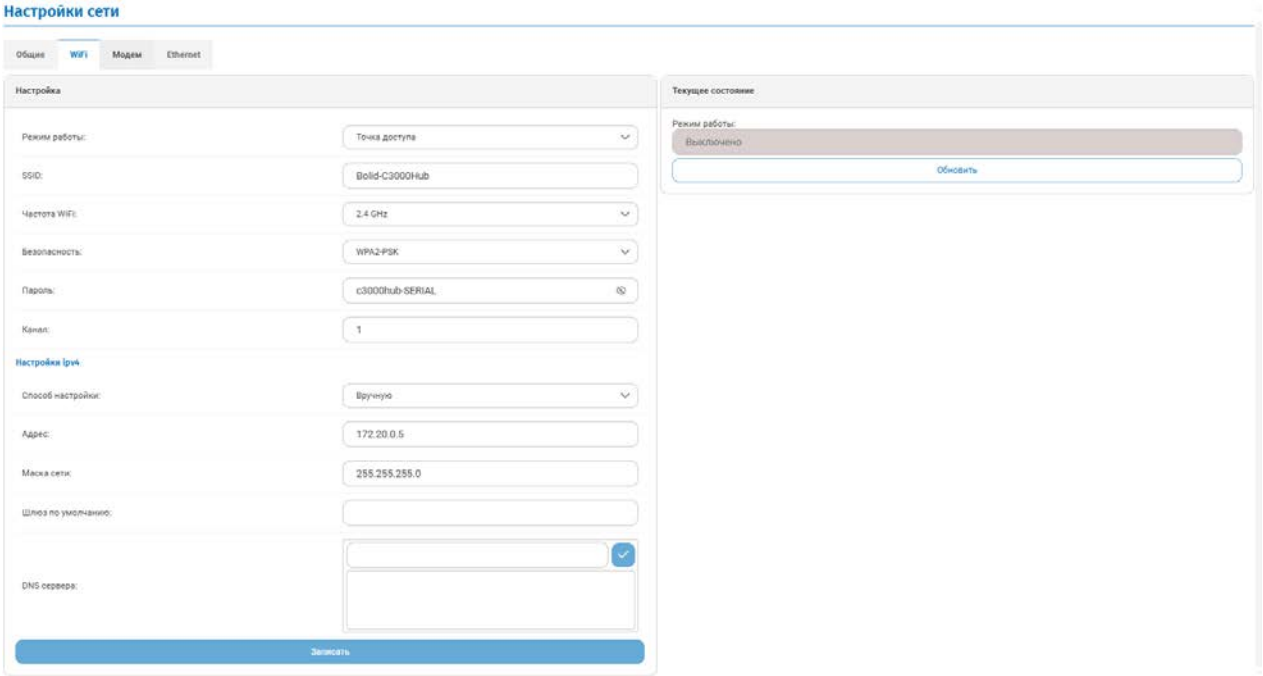


Рисунок 8, позиция 6. Настройки сети, вкладка «Точка доступа».

5.3.5 – 3 – Вкладка «Модем» и её настройка

Вкладка «Модем» страницы «Настройки сети» располагает возможностью настраивать подключение ПЛК к интернету через сеть мобильного оператора, при помощи внешнего модема с антенной.

– Для осуществления работы данного метода подключения, необходима настройка следующих трех изменяемых параметров (*см. Рис 9, Таблицу 7*):

1. Точка доступа, имя точки доступа: уникальное имя, которое используется для идентификации точки доступа в сети оператора;
2. Имя пользователя: некоторые сотовые операторы требуют аутентификации для доступа к сети. В данном случае, имя пользователя используется в качестве логина для проверки подлинности абонента SIM-карты.
3. Пароль: код подтверждения подлинности абонента для доступа к сети.

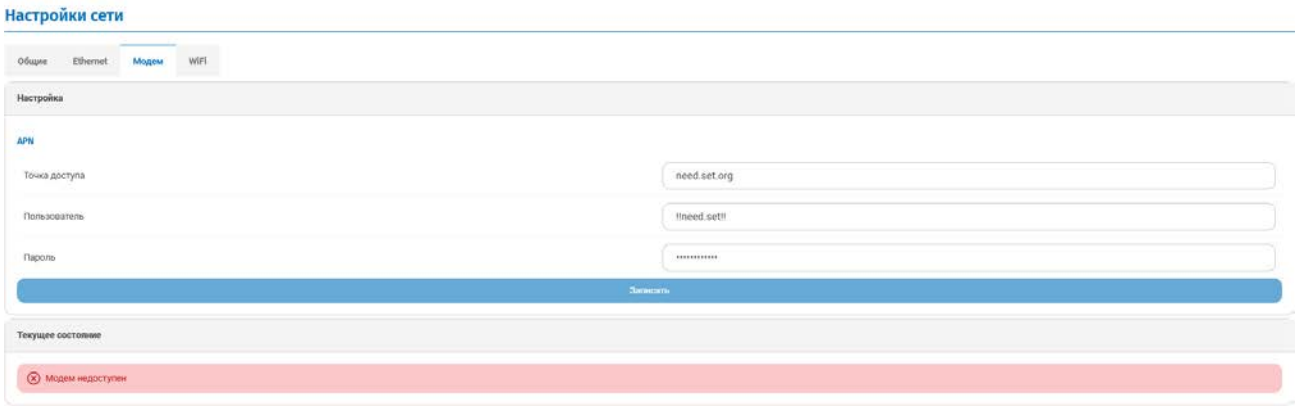


Рисунок 9. Настройки сети, вкладка «Модем».

Таблица 7. Описание параметров настройки сети, вкладка «Модем»

Вкладка «Модем»		
Название параметра	**Значение по умолчанию**	**Описание**
Точка доступа (имя точки доступа)	Отсутствует, присваивается пользователем	Идентификатор точки доступа в сети оператора
Пользователь	Отсутствует, присваивается пользователем	Логин для проверки подлинности абонента SIM-карты в сети оператора связи
Пароль	Отсутствует, присваивается пользователем	Код подтверждения подлинности абонента
Эти параметры применяются после нажатия на кнопку «Записать».		

5.3.5 – 4 – Вкладка «Ethernet» и её настройка

Внешний вид вкладки отображен на Рисунке 10.

Вкладка «Ethernet» позволяет администратору редактировать параметры интернет-подключения при подключении ПЛК к Ethernet-сети через витую пару (возможно при подключении витой пары, обжатой в штекере 8P8C, к интерфейсу Ethernet (разъём XS2 – *см. Приложение Б*), расположенному на контроллере).

Параметры подключения контроллера через интерфейс Ethernet отображены в таблице 8.

Таблица 8. Описание параметров настройки сети, вкладка «Ethernet»

Вкладка Ethernet		
Название параметра	**Значение по умолчанию**	**Описание**
Способ настройки	Вручную	Способ задания IP-адреса, маски и шлюза. Возможные значения: • вручную • DHCP
Остальные параметры доступны для редактирования только в случае, если указан способ настройки «Вручную»		
Адрес	192.168.0.50	IP-адрес контроллера
MAC	Присваивается производителем	Уникальный идентификатор контроллера. Значение не редактируется
Статус	Статус контроллера	Статус работы
Маска сети	255.255.255.0	Маска локальной сети
Шлюз по умолчанию	–	IP-адрес шлюза, через который осуществляется доступ в подсеть
DNS сервера	–	IP-адреса DNS-серверов
На вкладке «Ethernet» параметры размещены в двух областях: в области справа отображаются нередактируемые текущие настройки, которые работают в данный момент времени (работающие настройки). В области слева параметры конфигурации можно изменять. Эти параметры применяются после нажатия на кнопку «Записать».		

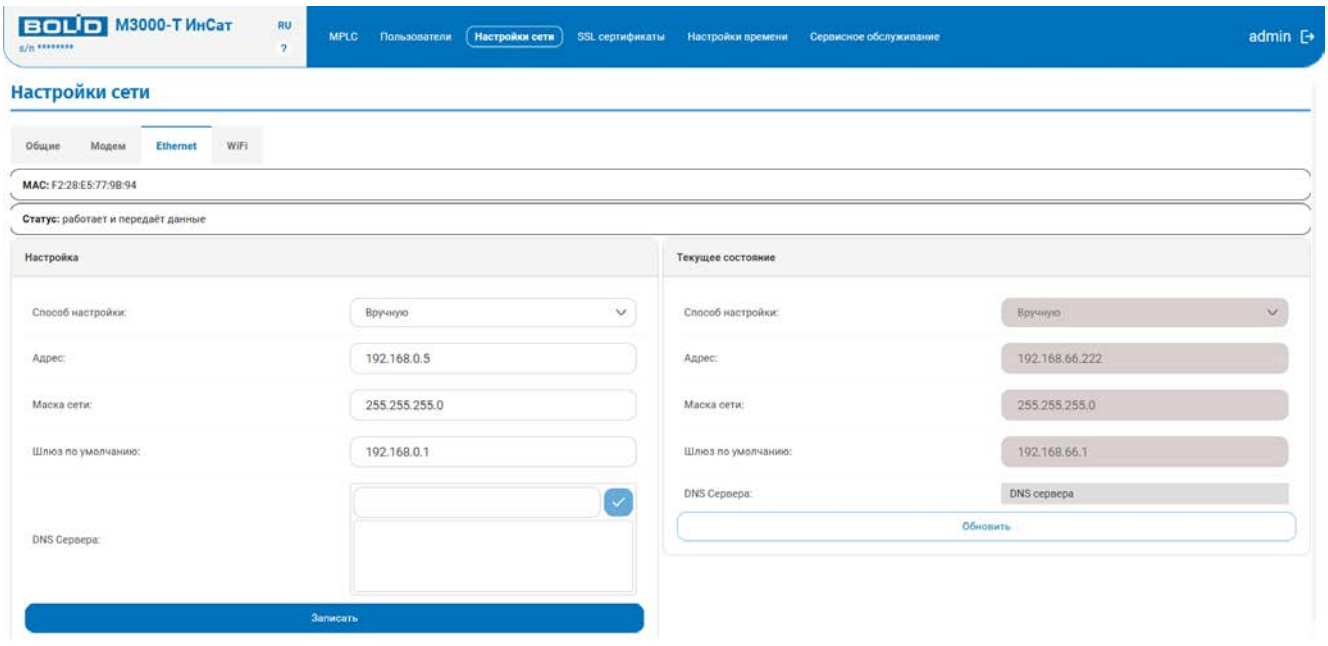


Рисунок 10. Настройки сети, вкладка «Ethernet».

5.3.6 Страница «SSL-сертификаты»

Страница разделена на 4 вкладки: «Самоподписанный сертификат», «Запрос на сертификат», «Загрузить сертификат», и «Установленный» (пункты по данным вкладкам отмечаются цифрами 1, 2, 3, 4 после написания номера пункта 5.3.6 соответственно).

Необходимые параметры ввода для генерации/запроса сертификата на вкладках «Самоподписанный сертификат» и «Запрос на сертификат» описаны в таблице 9.

Общий вид вкладок представлен на рисунках 11, 12, 13 и 14 соответственно.

Для обеспечения криптографической защиты передаваемого трафика (а также аутентичности прибора, защита от атак «Человек посередине») в контроллере предусмотрена возможность установления защищённого соединения посредством протокола HTTPS/WSS (HTTP и WS (WebSocket) поверх TLS/SSL). Для работы требуется настройка PKI (установка сертификатов), а также включение безопасного соединения на странице «Сервисное обслуживание > Вкладка «Системные настройки» > Два параметра «Доступ к устройству по протоколу HTTP/HTTPS»».

Для установки сертификата SSL реализовано 2 схемы:

1. Генерация цепочки самоподписанных SSL сертификатов. Подходит для одиночных устройств или когда нет инфраструктуры PKI на предприятии – создание сертификата данного типа происходит на вкладке «Самоподписанный сертификат».
2. Генерация запроса на получение сертификата (CSR) и последующий импорт SSL сертификата. Данный механизм подходит для предприятий, у которых есть развернутая инфраструктура PKI и требуется, чтобы сертификат устройства был в цепочки доверия предприятия – создание сертификата данного типа происходит на вкладке «Запрос на сертификат».

Все операции с сертификатами рекомендуется проводить «на столе» в безопасной среде (чтобы исключить вмешательство извне).

Из контроллера не предусмотрен экспорт закрытых ключей стандартными средствами.

При этом возможно скачать ключ с использованием программы PuTTY, либо с использованием доступа по протоколу Sftp. Внутри контроллера ключи расположены в файлах:

etc/bolid/ssl/cert.pem – цепочка сертификатов
etc/bolid/ssl/private.pem – приватный ключ.

Для работы допускается использование только RSA ключей.

Таблица 9. Параметры сертификатов

Название параметра	**Ограничения**	**Значение по умолчанию**	**Влияние на Root CA сертификат 1-й схемы**	**Влияние на Device сертификат 1-й схемы**	**Влияние на CSR**
Битность RSA ключа	Допустимы только: 1024, 2048, 4096	2048	Определяет размер закрытого ключа Root CA	Определяет размер закрытого ключа контроллера	Определяет размер закрытого ключа контроллера
Имя сертификата - Common Name (CN)	Любая строка латиницей до 64-х символов	Пусто, но устройство тогда автоматически сделает «M3000-T-InSat SN:серийный номер»	Компонент CN субъекта и издателя с добавление префикса “Root CA“	Компонент CN субъекта. Компонент CN издателя с добавление префикса “Root CA“	Компонент CN субъекта
Страна - Country name (C)	Двухбуквенное обозначение страны ISO-3166	Пусто	Если не пусто компонент C субъекта и издателя.	Если не пусто компонент C субъекта и издателя.	Если не пусто компонент C субъекта.
Область или регион - State or province (ST)	Любая строка латиницей до 64-х символов	Пусто	Если не пусто компонент ST субъекта и издателя.	Если не пусто компонент ST субъекта и издателя.	Если не пусто компонент ST субъекта.
Город - Locality (L)	Любая строка латиницей до 64-х символов	Пусто	Если не пусто компонент L субъекта и издателя.	Если не пусто компонент L субъекта и издателя.	Если не пусто компонент L субъекта.
Название - Organization (O)	Любая строка латиницей до 64-х символов	Пусто	Если не пусто компонент O субъекта и издателя.	Если не пусто компонент O субъекта и издателя.	Если не пусто компонент O субъекта.
Контактный e-mail адрес - Email (E)	Любая строка латиницей до 256-х символов	Пусто	Если не пусто компонент E субъекта и издателя.	Если не пусто компонент E субъекта и издателя.	Если не пусто компонент E субъекта.
Название отдела организации - Organization Unit (OU)	Любая строка латиницей до 64-х символов	Пусто	Если не пусто компонент OU субъекта и издателя.	Если не пусто компонент OU субъекта и издателя.	Если не пусто компонент OU субъекта.
Дата начала	Дата начала времени действия сертификата	0	Дата начала времени действия сертификата	Дата конца времени действия сертификата	Не влияет

Название параметра	Ограничения	Значение по умолчанию	Влияние на Root CA сертификат 1-й схемы	Влияние на Device сертификат 1-й схемы	Влияние на CSR
Дата конца	Дата конца времени действия сертификата	0	Дата конца времени действия сертификата	Дата конца времени действия сертификата	Не влияет
Срок действия сертификата (дни)	От 7 дней до 25 лет	365	Срок действия сертификата (от текущего времени конвертера)	Срок действия сертификата (от текущего времени конвертера)	Не влияет
IP адрес	Любой допустимый IP адрес	IP адрес из адресной строки браузера (если входили по IP адресу)	Не влияет	Каждый IP добавляет компонент CN субъекта. Компонент поля Subject Alternative Names	Каждый IP добавляет компонент CN субъекта. Компонент поля Subject Alternative Names
DNS-имя	Любое допустимое DNS имя	Доменное имя хоста из адресной строки браузера (если входили по DNS имени)	Не влияет	Каждый DNS добавляет компонент CN субъекта. Компонент поля Subject Alternative Names	Каждый DNS добавляет компонент CN субъекта. Компонент поля Subject Alternative Names

5.3.6 – 1 – Вкладка «Самоподписанный сертификат»

Один из двух возможных путей генерации сертификата (генерация цепочки самоподписанных сертификатов) осуществляется на вкладке «Самоподписанный сертификат».

Чтобы сгенерировать самоподписанный сертификат, необходимо заполнить параметры будущего сертификата в соответствии с таблицей 9.

После заполнения этих параметров (*см. Рис. 11.1*) следует нажать кнопку «**Сгенерировать**».

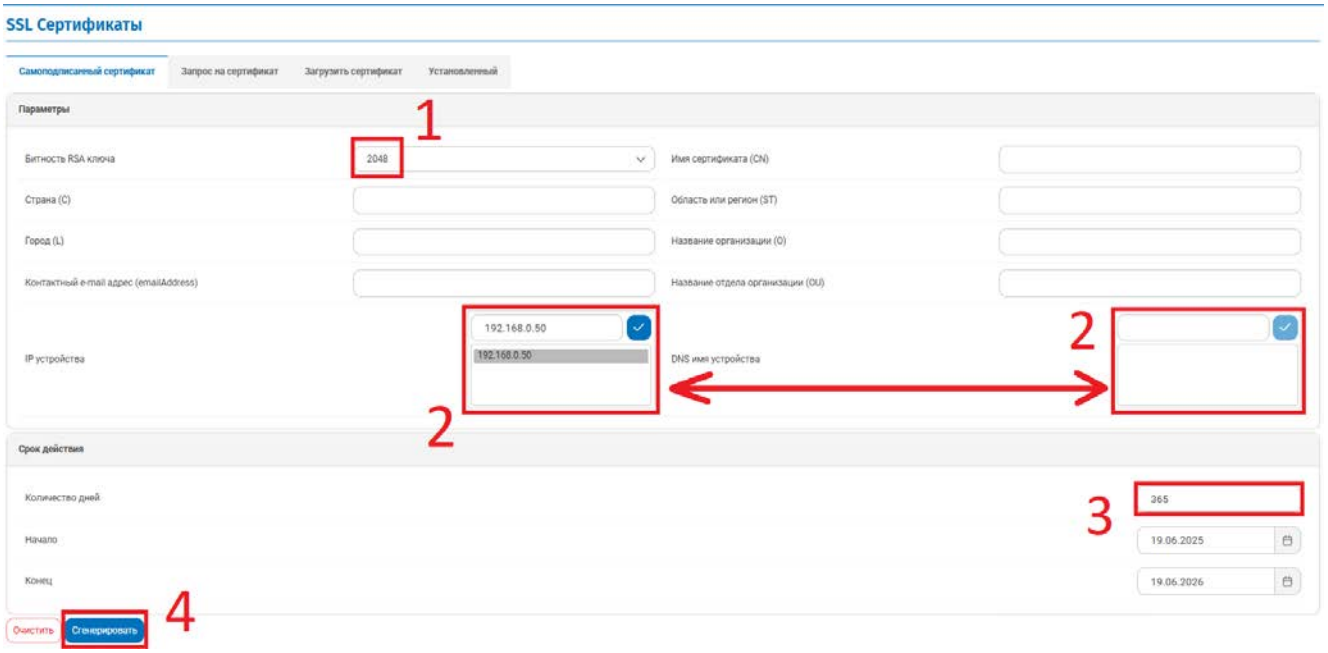


Рисунок 11.1. Страница SSL Сертификаты. Вкладка «Самоподписанный сертификат».

Отмечены поля и нумерация по заполнению параметров сертификатов.

На экран будет выведено сообщение о генерации сертификата (*см. Рис. 11.2*).

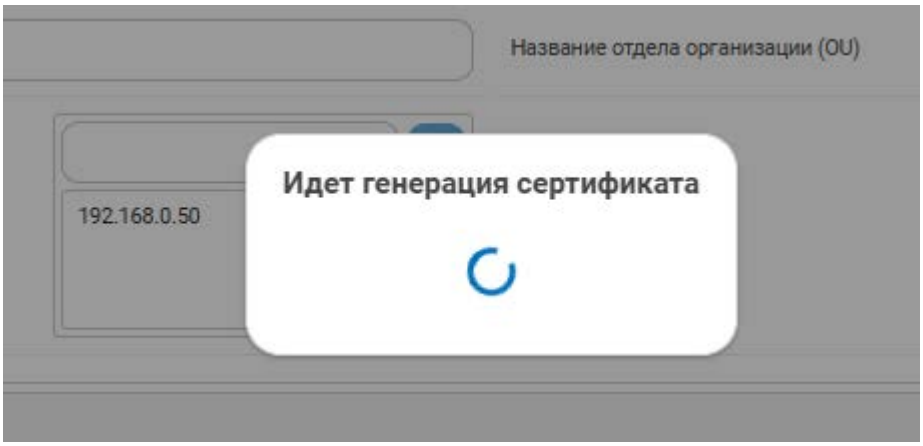


Рисунок 11.2. Сообщение о генерации сертификата.

После генерации сертификат применяется автоматически. То есть, происходит установка сертификата в веб-сервер и на протокол JSON RPC. Дождитесь появления сообщения в правом нижнем углу экрана о том, что сертификат применён (*см. Рис. 11.3*).

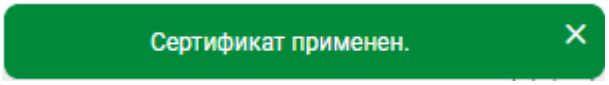


Рисунок 11.3. Сообщение о применении сертификата.

Далее можно включить доступ к контроллеру по протоколу HTTPS на вкладке «Сервисное обслуживание» (наличие применённого сертификата – обязательное условие работы по протоколу HTTPS).

При открытии страницы с новым сертификатом, необходимо добавить его в доверенные в браузере.

5.3.6 – 2 – Вкладка «Запрос на сертификат»

Второй из двух возможных путей генерации сертификата – генерация запроса на получение сертификата (CSR) и последующий импорт SSL сертификата – осуществляется на вкладке «Запрос на сертификат».

Создание сертификата по запросу осуществляется следующим образом:

1. Генерация запроса на сертификат;
2. Подготовка непосредственно сертификата в центре сертификации (CA);
3. Загрузка сертификата на устройство.

Чтобы создать запрос на сертификат, необходимо заполнить параметры будущего сертификата в соответствии с таблицей 9.

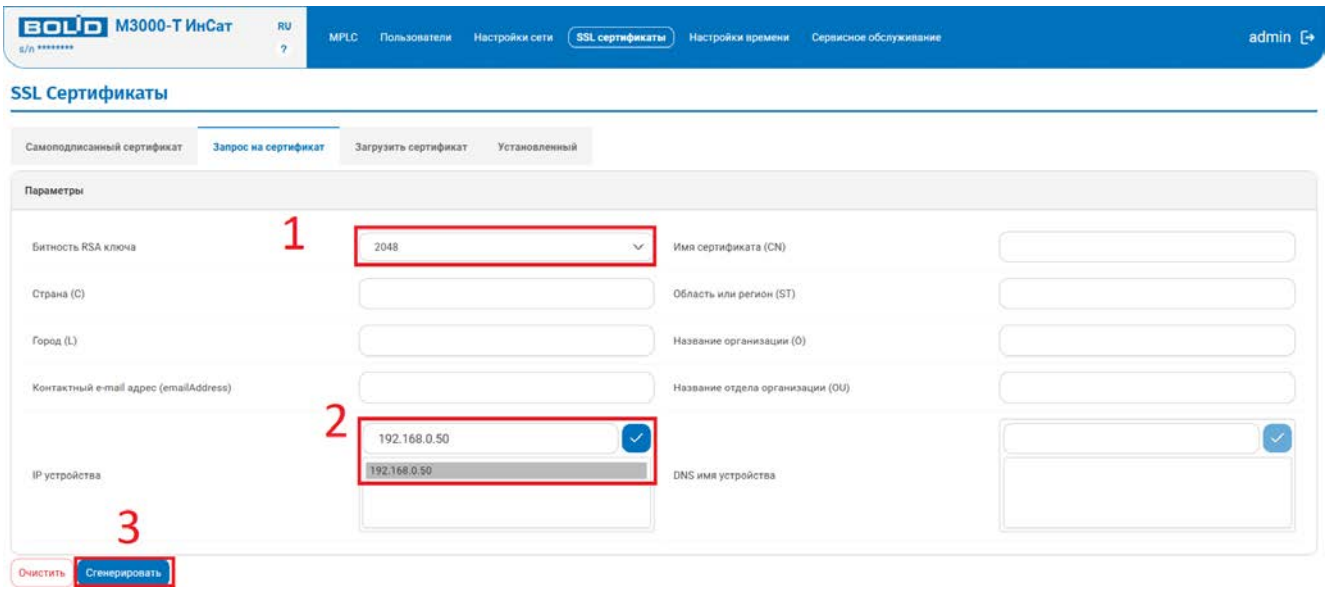


Рисунок 12. Страница SSL Сертификаты. Вкладка «Запрос на сертификат».

После заполнения этих параметров (*см. Рис. 12*) следует нажать кнопку «**Сгенерировать**».

Далее на основе CSR и корневого сертификата подготовьте сертификат устройства. Полученный сертификат должен быть в формате PKSC7 в кодировке PEM (содержит цепочку доверия).

Затем на вкладке «Загрузить сертификат» нажмите кнопку «Выберите файл», выберите файл на своем компьютере и нажмите кнопку «Загрузить» (*подробнее - читать пункт 5.3.6 – 3 – Вкладка «Загрузить сертификат», также см. Рис. 13*):

Дождитесь сообщения о том, что файл загружен и примените сертификат, нажав кнопку «Загрузить». Изменения вступят в силу после перезагрузки устройства.

5.3.6 – 3 – Вкладка «Загрузить сертификат»

Данная вкладка позволяет загрузить администратору сертификат в ПЛК. Общий вид вкладки отображен на Рисунке 13.

На вкладке имеются две кнопки:

- «Выберите файл» - позволяет выбрать необходимый файл-сертификат в файловой системе пользователя ПК;

- «Загрузить» - позволяет загрузить сертификат в систему контроллера и применить изменения.

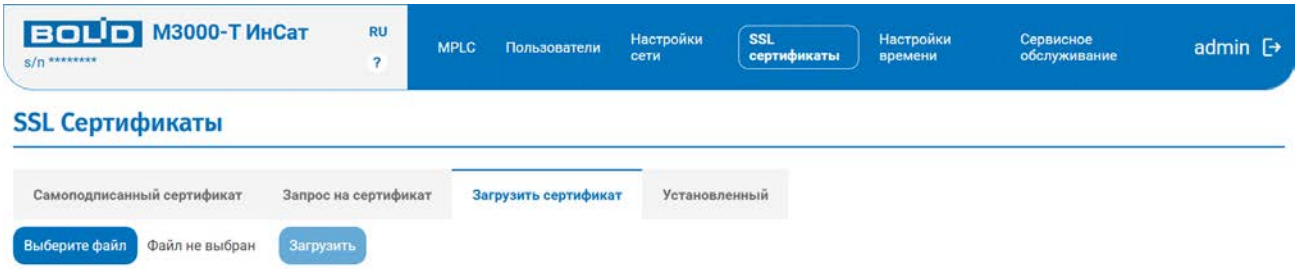


Рисунок 13. Вкладка загрузки сертификата.

5.3.6 – 4 – Вкладка «Установленный сертификат»

Данная вкладка предназначена для просмотра установленного сертификата прибора. Общий вид вкладки предоставлен на Рисунке 14.

Данная вкладка располагает тремя функциями:

- Кнопка «**Скачать**» - скачать действующий сертификат;
- Кнопка «**Скачать цепочку**» - скачать цепочку действующих сертификатов;
- Кнопка «**Сбросить**» - удаляет сертификат из устройства.

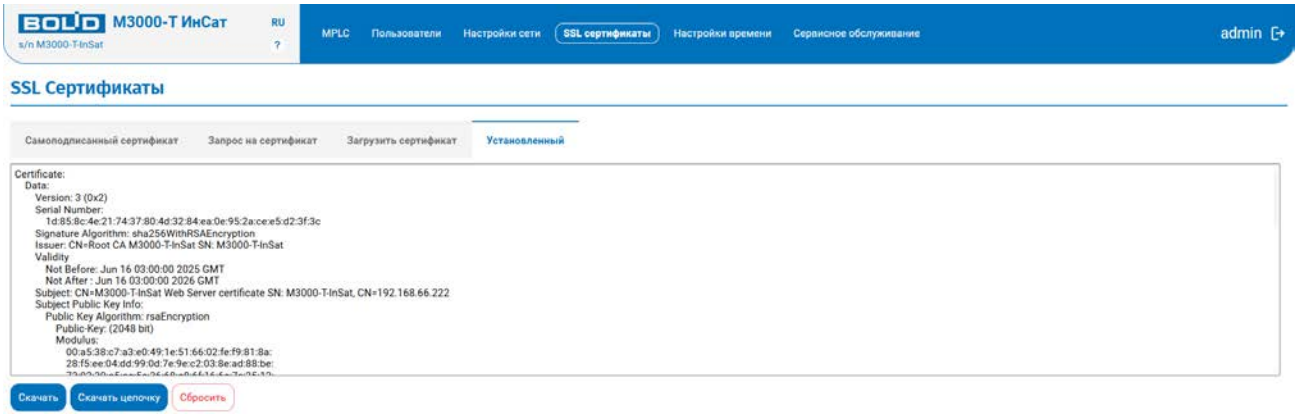


Рисунок 14. Вкладка просмотра и сброса сертификата.

Внимание!

В конвертере хранится только один закрытый ключ.
Генерация (нажатие на кнопку «**Сгенерировать**») нового ключа удаляет старый предыдущий ключ.

Импорт сертификатов в ОС Windows

В операционной системе семейства Windows предусмотрено глобальное хранилище сертификатов. Это хранилище используют браузеры Chrome, Opera, Microsoft Edge, Microsoft Internet Explorer.

Внимание!

Добавление сертификата для браузера Mozilla Firefox, описано отдельно, в пункте «Импорт сертификатов Mozilla Firefox».

Для импорта сертификатов необходимо:

1. Перейти в веб-конфигураторе на вкладку «Установленный» (*см. Рис. 14*) и нажать кнопку «**Скачать цепочку**»:

2. Перейти в папку загрузок (*см. Рис. 15*) и кликнуть два раз левой кнопкой мыши по скачанному файлу.

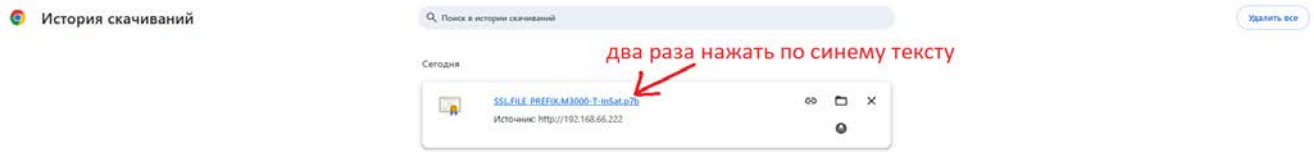


Рисунок 15. Папка загрузок

Откроется окно со списком содержащихся в нём сертификатов (*см. Рис. 16*):

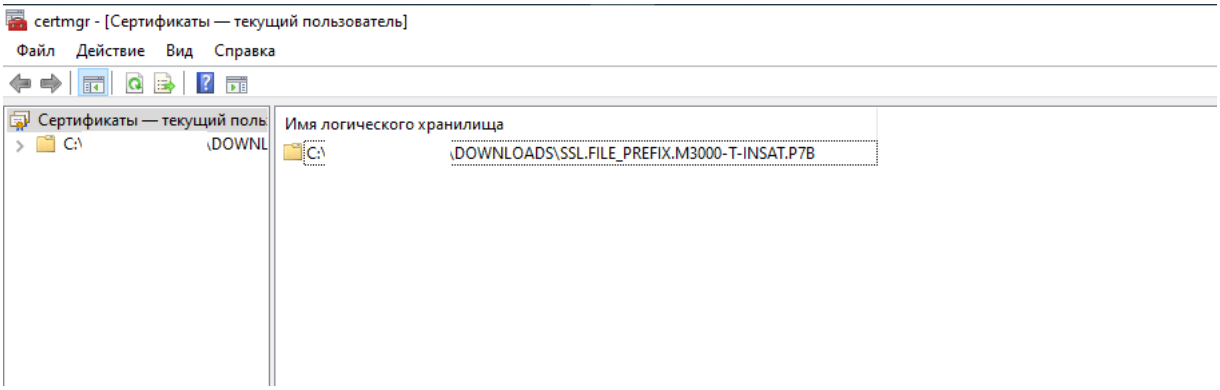


Рисунок 16. Список сертификатов, хранящихся в файле цепочки сертификатов.

3. Необходимо дважды нажать на скачанную цепочку сертификатов, после чего зайти в папку «**Сертификаты**». В списке сертификатов выбрать сертификат, начинающийся с символов «Root CA…» и щелкнуть по нему два раза. Откроется окно (*см. Рис. 17*), в котором нужно нажать кнопку «Установить сертификат»:

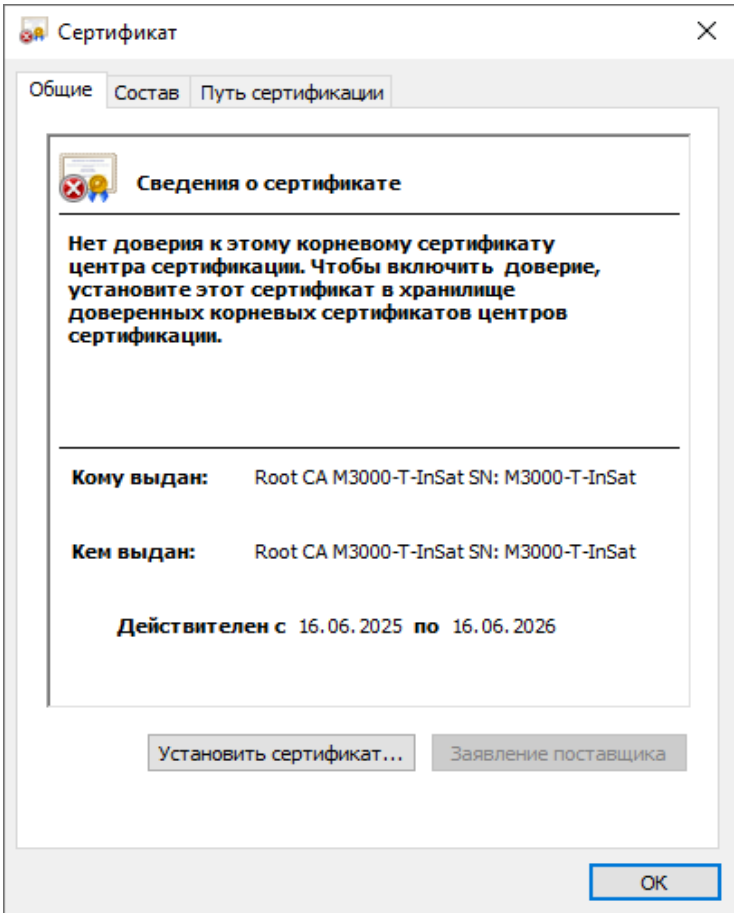
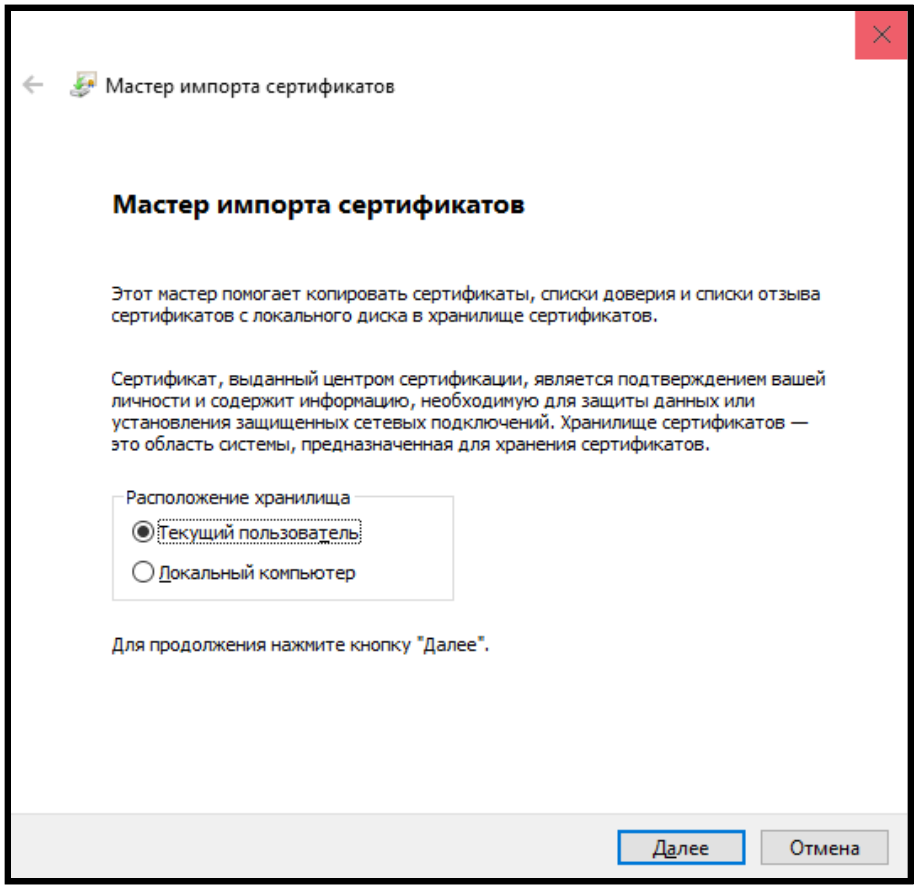


Рисунок 17. Окно установки сертификата.

В появившемся «Мастере импорта сертификатов» перейти на вторую страницу, нажав кнопку «Далее». Выбрать пункт «Поместить все сертификаты в выбранное хранилище» и нажать кнопку «Обзор» (*см. Рис. 18, поз. 2*).



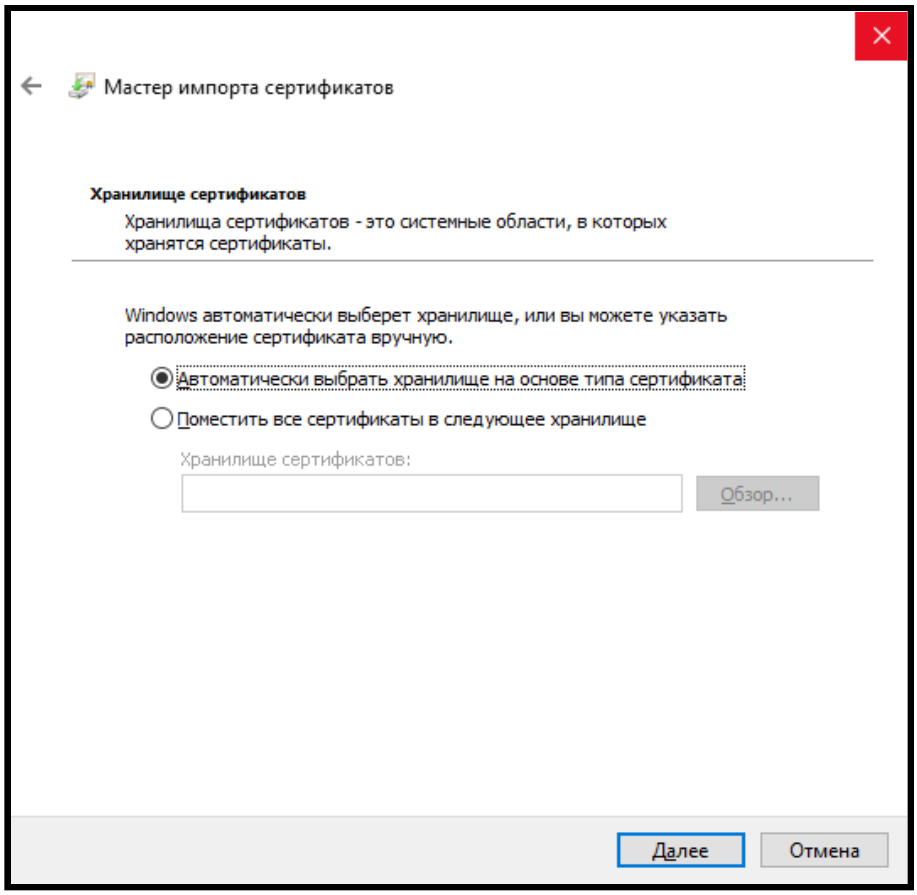


Рисунок 18, позиция 1 и 2 соответственно. Выбор хранилища сертификатов.

В диалоговом окне (*см. Рис. 19*) выбрать папку «Доверенные корневые центры сертификации» и нажать «Далее».

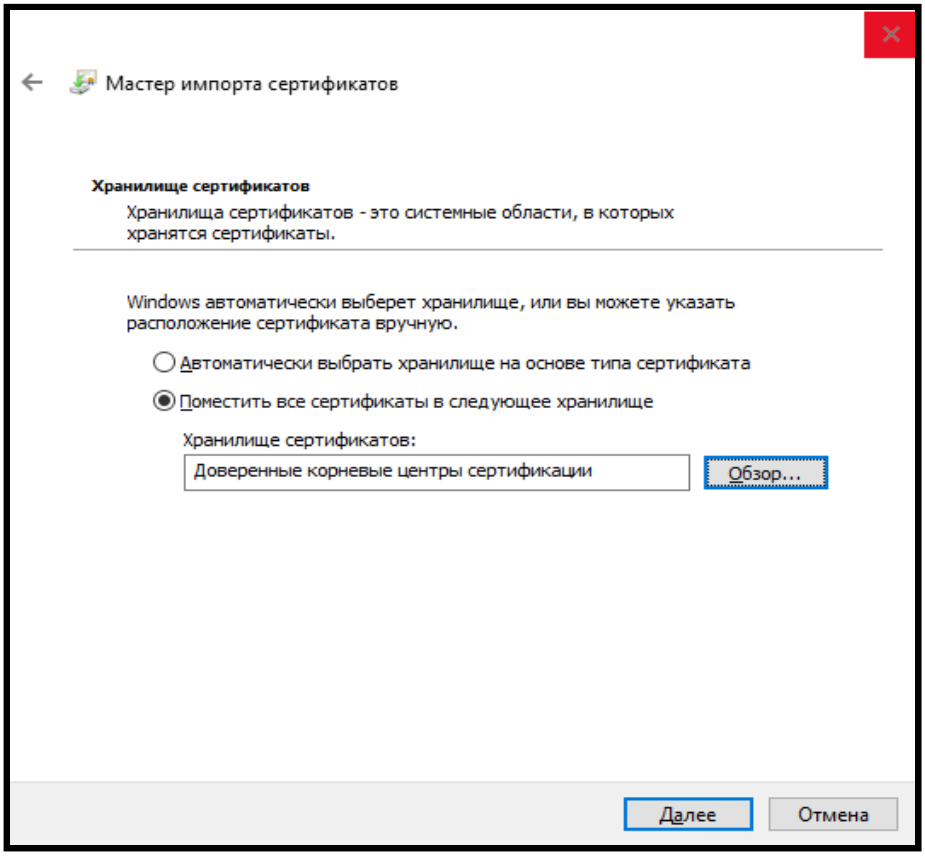


Рисунок 19. Выбор хранилища сертификатов.

После выбора хранилища завершить импорт, нажав кнопку «Далее», «Готово». В появившемся предупреждении безопасности, нажать «Да», после чего должно появиться завершающее окно (*см. Рис. 20*) с подтверждением выполнения импорта.

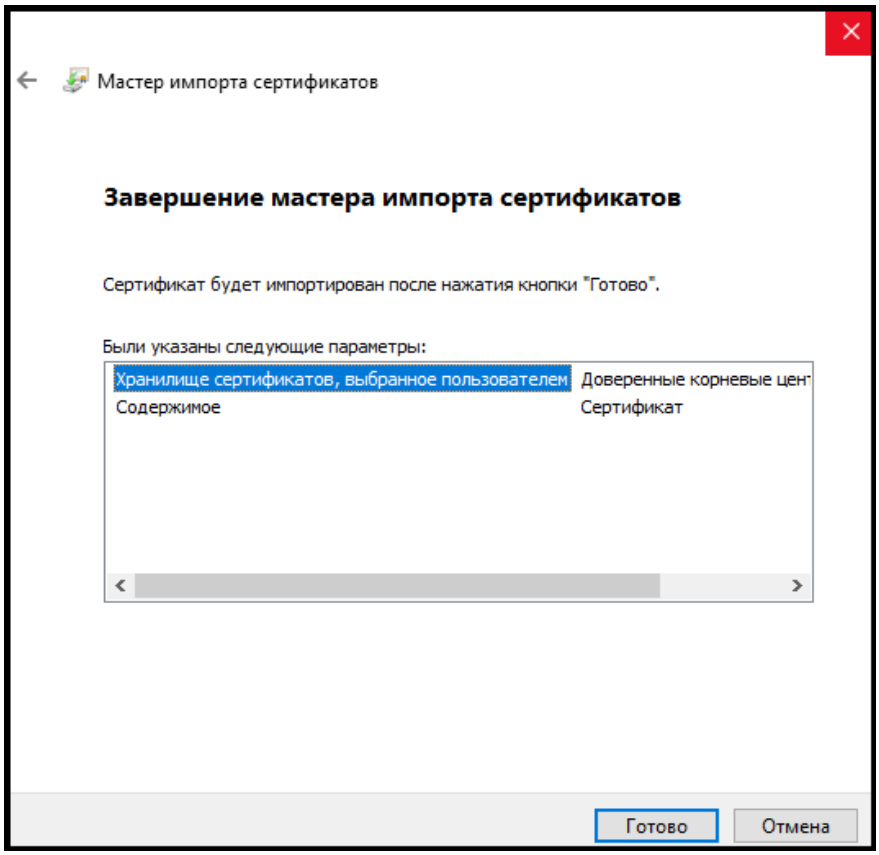


Рисунок 20. Завершение импорта.

Импорт сертификата Mozilla Firefox

Импорт сертификата Mozilla Firefox версии 57 и выше для платформ Windows и Linux. Сертификат будет добавлен во внутреннее хранилище Firefox и понадобится только при взаимодействии через веб-конфигуратор.

Для добавления сертификата нужно запустить браузер и в основном меню (*см. Рис. 21*) выбрать пункт «Настройки»:

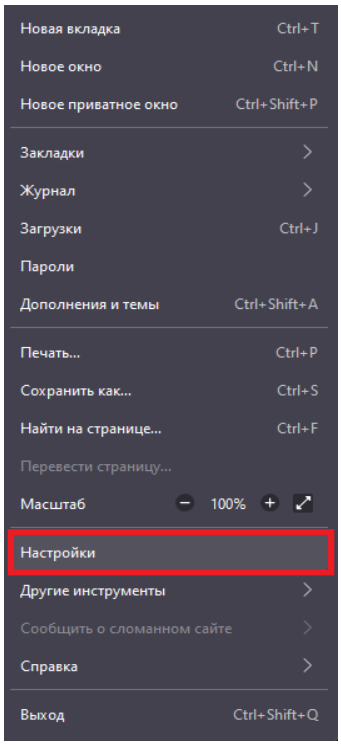


Рисунок 21. Меню настроек Mozilla Firefox

В настройках следует зайти в раздел «**Приватность и защита**», подраздел «**Защита - Сертификаты**», затем нажать кнопку «**Просмотр сертификатов**» (*см. Рис 22, поз. 1*); или же вписать в поисковую строку слово «сертификаты» и нажать на кнопку «**Просмотр сертификатов**» (*см. Рис. 22, поз. 2*).

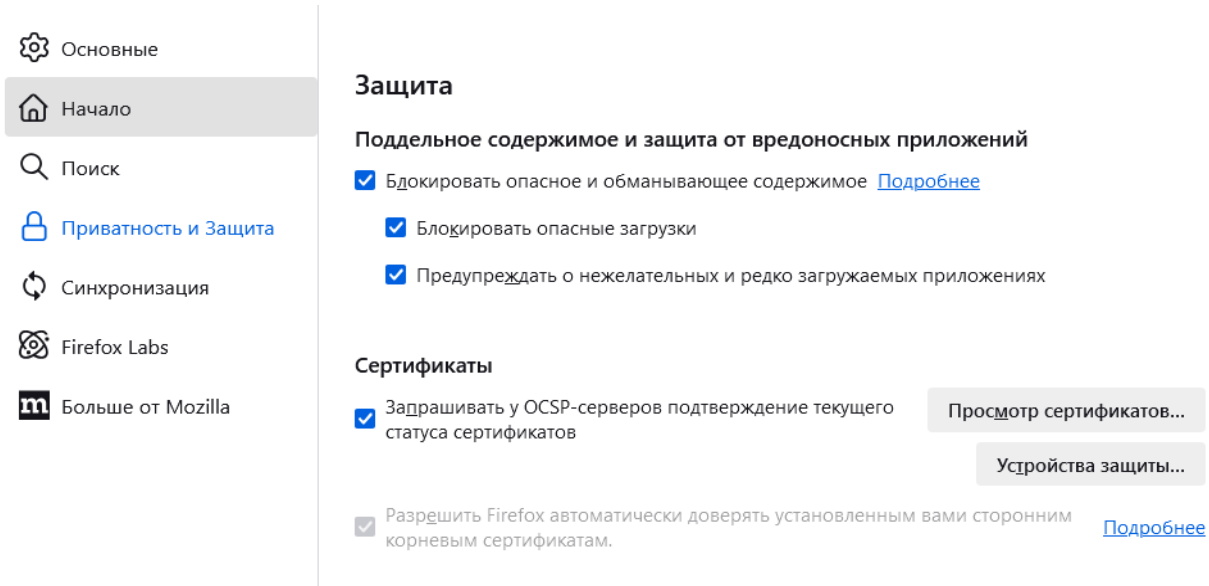


Рисунок 22, позиция 1.
Раздел «Приватность и защита» в настройках Mozilla Firefox.

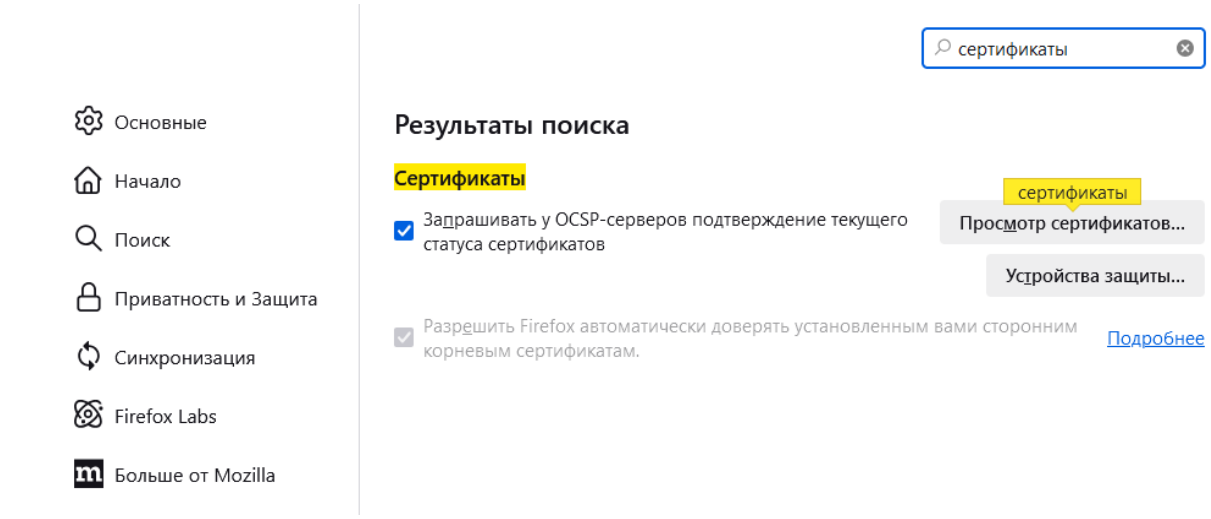


Рисунок 22, позиция 2.
Выданный результат в поисковой строке окна настроек в Mozilla Firefox.

Откроется окно «Управление сертификатами» (*см. Рис. 23*):

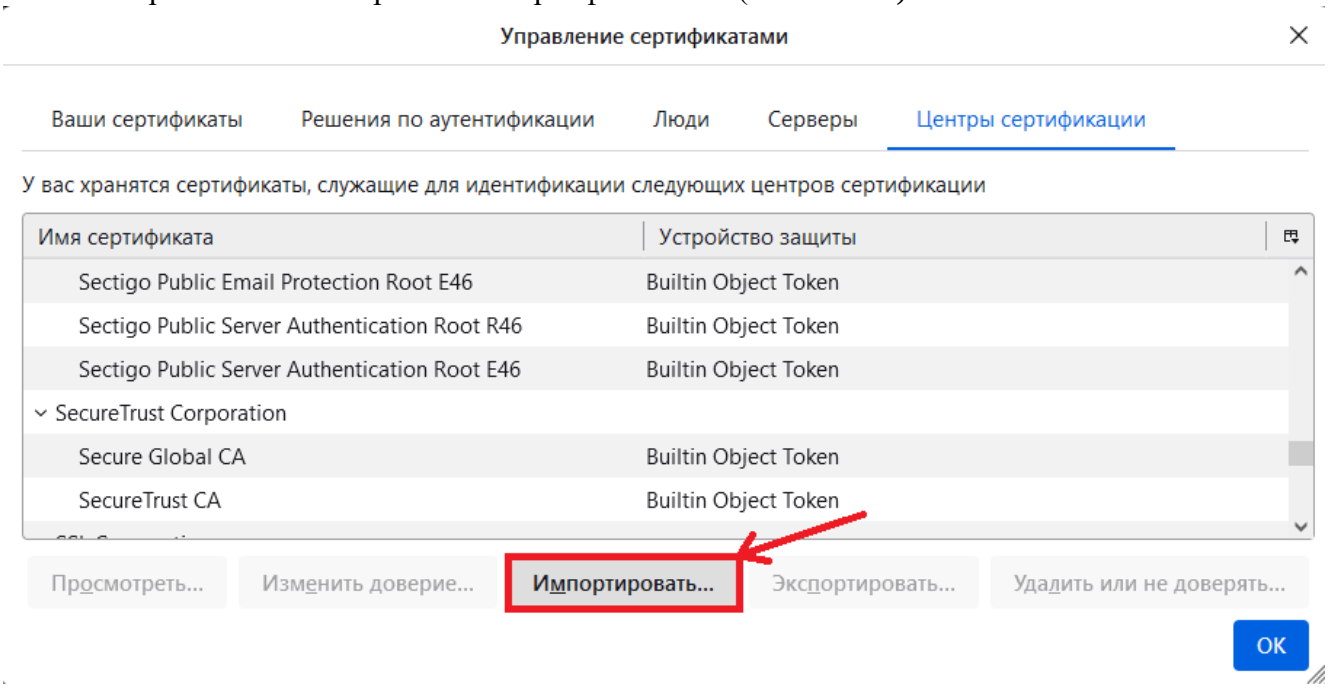


Рисунок 23. Импорт сертификата в Mozilla Firefox.

Выбрать вкладку «Центры сертификации», нажать кнопку «Импортировать». В открывшемся диалоговом окне выбрать загруженный сертификат. Нажать кнопку «ОК».

Появится окно «Загрузка сертификата» (*см. Рис. 24*):

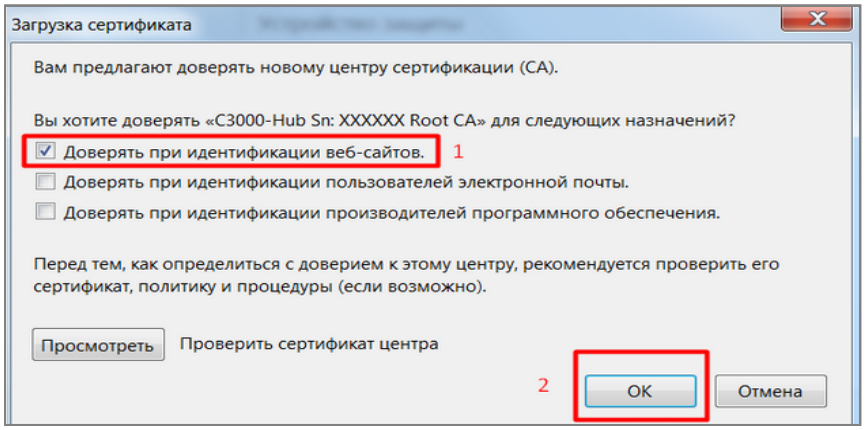


Рисунок 24. Завершение импорта сертификата в Mozilla Firefox.

Отметить пункт «Доверять при идентификации веб-сайтов». Нажать кнопку «ОК». Убедиться, что сертификат появился в списке (*см. Рис. 25*):

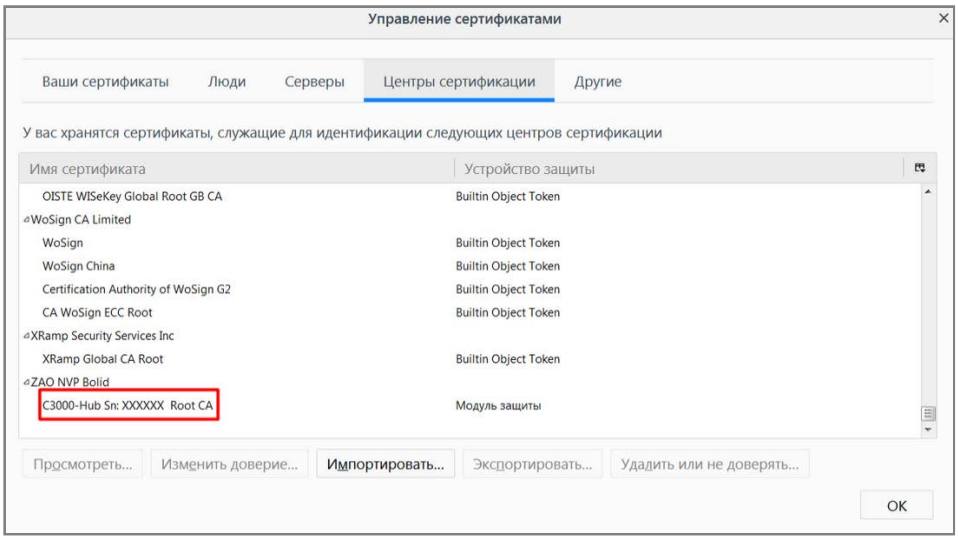


Рисунок 25. Окно отображения сертификатов в Mozilla Firefox

Импорт сертификатов в ОС Linux

Данная инструкция подходит для веб-браузеров Chromium и Opera.

Необходимо установить пакет libnss3-tools. Необходимо выполнить следующую команду:

certutil -d sql:$HOME/.pki/nssdb -A -t «C,,» -n «<Алиас сертификата>« -i <Путь к файлу сертификата>

Удостовериться, что сертификат появился в списке (появится с указанным алиасом):

certutil -d sql:$HOME/.pki/nssdb –L

5.3.7 Страница «Настройки времени»

Данная страница предназначена для настройки даты и времени устройства. Общий вид страницы представлен на Рисунке 26.1.

В зависимости от требований конкретного пользовательского приложения или в целях отладки, можно установить дату и время непосредственно указав или синхронизировав с компьютером.

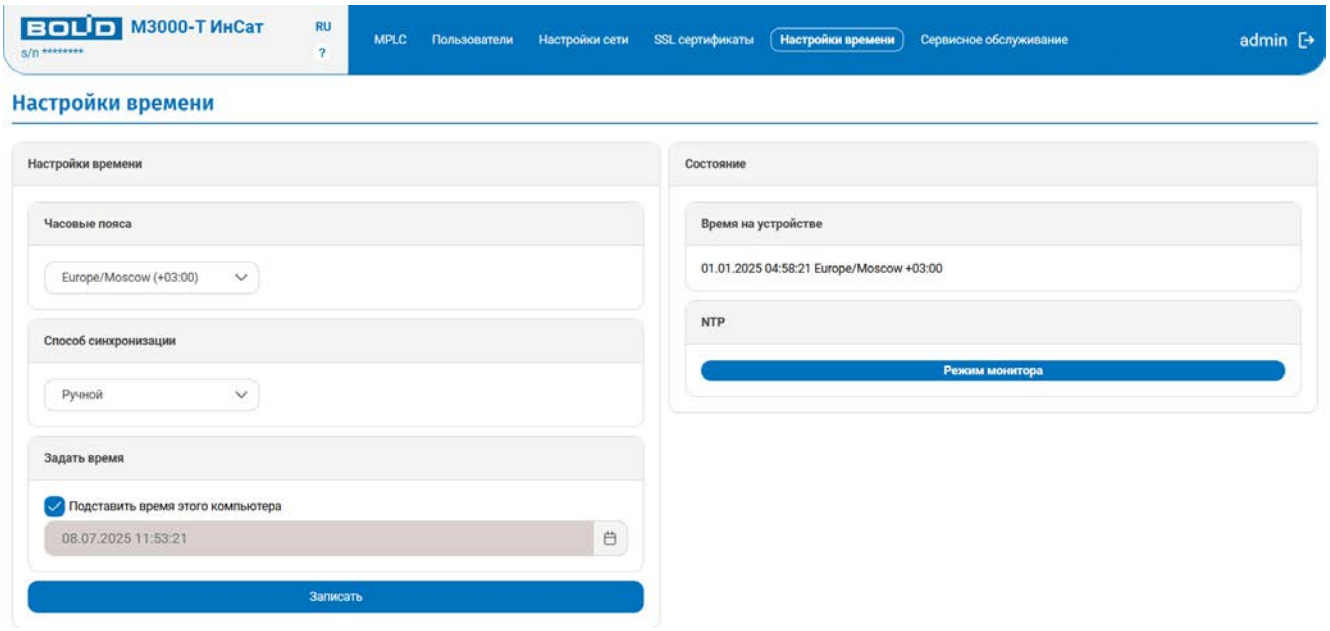


Рисунок 26.1. Общий вид страницы настройки времени.

При нажатии ЛКМ по параметру «**Подставить время этого компьютера**» пропадает возможность изменять время на ПЛК самостоятельно, а также происходит синхронизация времени с ПК, на котором открыт веб-конфигуратор (*см. Рис. 26.2*). Дата и время в этом окне изменяется синхронно с датой и временем компьютера.

Текущие дата и время записываются в контроллер и вступают в силу **только** после нажатия синей кнопки «**Записать**» в левой нижней части экрана.

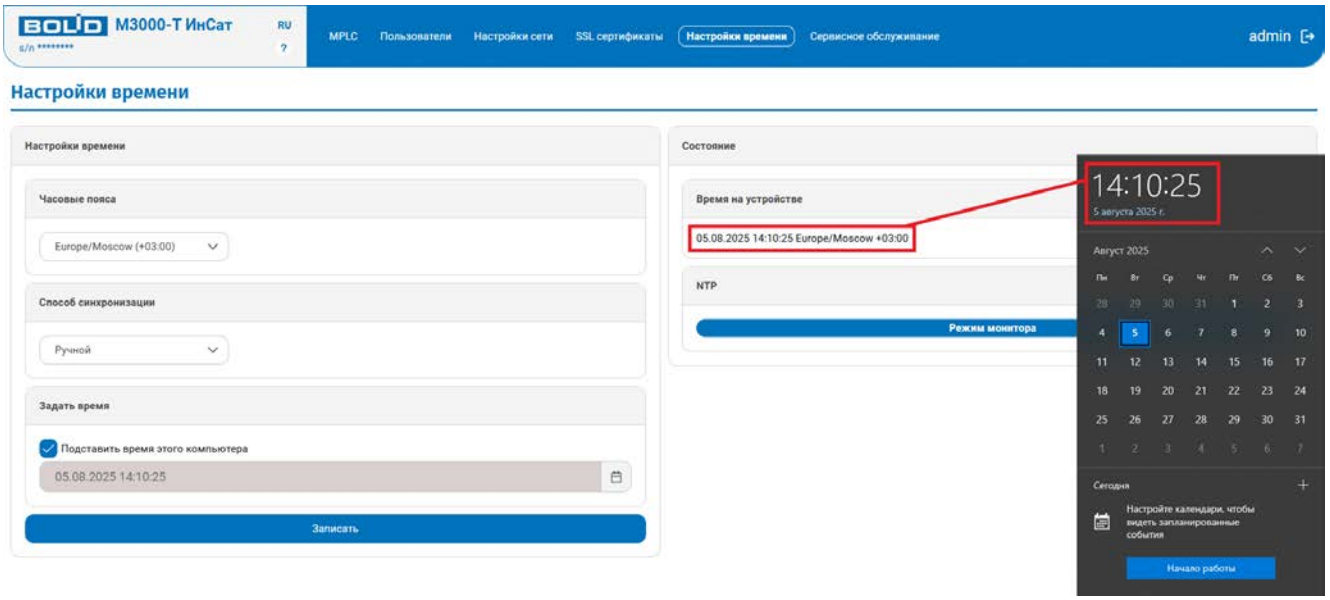


Рисунок 26.2. Страница настройки времени. Синхронизация даты и времени с компьютером.

В случае снятия галочки с параметра «Подставить время этого компьютера», время ПЛК будет выставляться пользователем вручную – по нажатию на иконку отрывного календаря справа от остановившегося счётчика времени появится возможность выбрать число месяца, а также время *(см. Рис. 26.3 поз. 1 и поз. 2*).

При необходимости, время может быть прописано вручную пользователем в соответствии с правильным выставлением параметров – дата, месяц и год (ДД.ММ.ГГГГ) и время суток по часам, минутам и секундам соответственно.

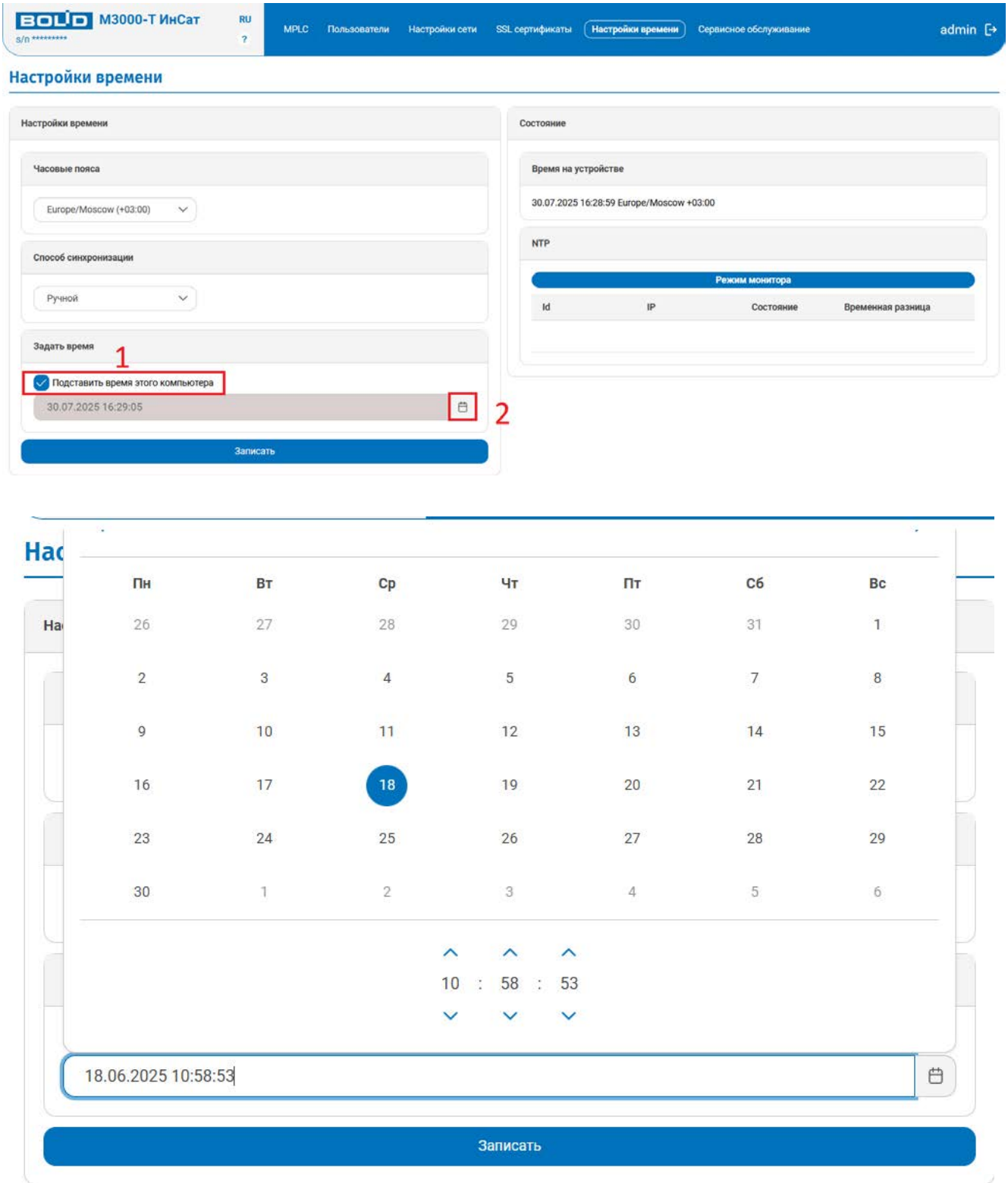


Рисунок 26.3, позиция 1 и 2 соответственно. Страница настройки времени.
Задание времени вручную.

Выставленные вручную параметры вступают в силу после записи в контроллер – при нажатии синей кнопки «**Записать**» в правой нижней части экрана.

Контроллер поддерживает протокол NTP и может автоматически синхронизироваться в процессе работы. Для синхронизации в сети необходим(ы) NTP-сервер(ы). Для задания IP-адресов NTP-серверов, включения и отключения протокола NTP и отражения его статуса предназначен набор полей и кнопок в рамке с названием NTP в левой части текущего окна.

На Рисунке 26.4 показан контроллер с активированным NTP протоколом и NTP-сервером, имеющим адрес 192.168.0.50.

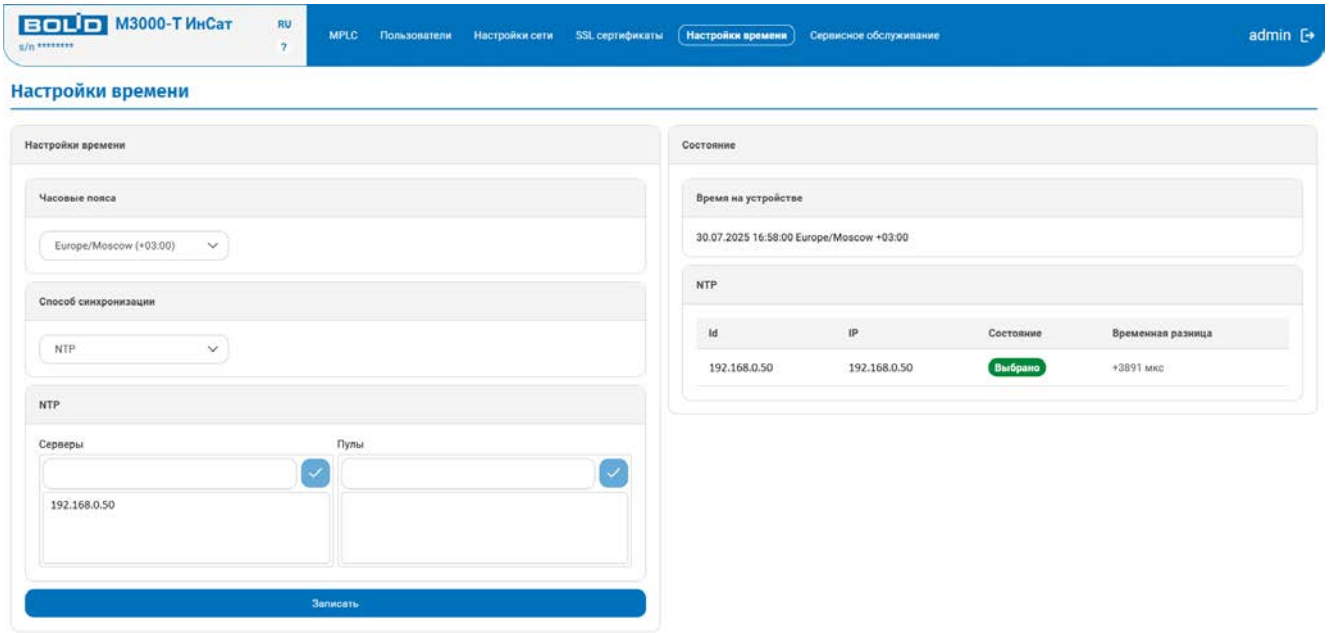


Рисунок 26.4. Страница настройки времени. Настройка NTP.

5.3.8 Страница «Сервисное обслуживание»

Страница разделена на три вкладки: «Прочие настройки», «Информация о памяти» и «Обновление» (пункты по данным разделам отмечаются цифрами 1, 2, 3 написания номера 5.3.8 соответственно).

5.3.8 – 1 – Вкладка «Системные настройки»

Дополнительные настройки контроллера. Внешний вид вкладки представлен на Рисунке 27. Описание приведено в таблице 10.

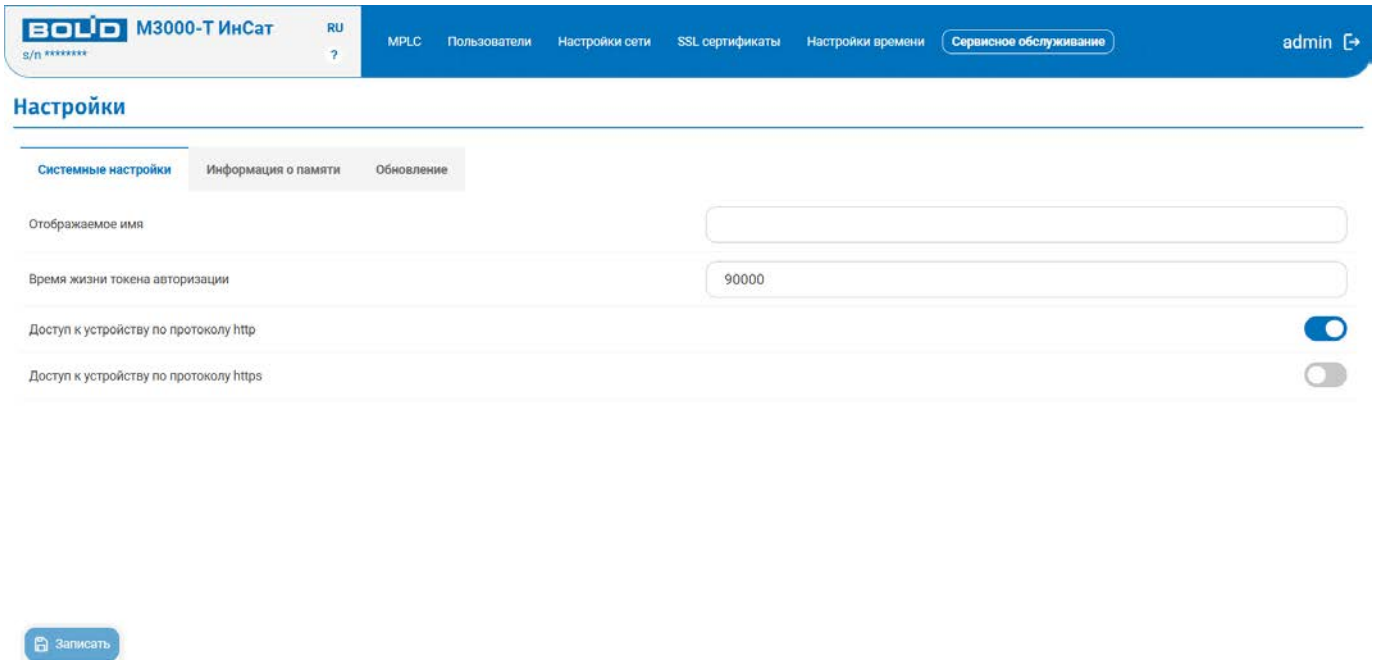


Рисунок 27. Страница «Сервисное обслуживание», вкладка «Системные настройки»

Таблица 10 – Параметры вкладки «Системные настройки»

Параметр	Описание	Возможные значения	Значение по умолчанию
Время жизни токена авторизации	Время, после которого заново нужно будет проходить аутентификацию	0….	90000
Доступ к устройству по протоколу HTTP	Доступ к устройству по протоколу http без надстройки шифрования	Вкл/выкл	Включен
Доступ к устройству по протоколу HTTPS	Доступ с надстройкой шифрования. Данная опция будет принудительно отключена, если сертификат на устройстве отсутствует или некорректен	Вкл/выкл	Выключен

5.3.8 – 2 – Вкладка «Информация о памяти»

Во вкладке "Информация о памяти" веб-конфигуратора представлена информация о внутренней памяти устройства, включая объём занятой и свободной памяти, виды хранилищ и их статус (заполненное и свободное место). Внешний вид вкладки представлен на Рисунке 28.

Внутренняя память контроллера (SD-накопитель) реализована по технологии, имеющей ограничения по количеству циклов записи, которые фиксируются внутренним ПО контроллера, постоянно вычисляется контроллером и выводится с шагом 10 % в отдельное поле.

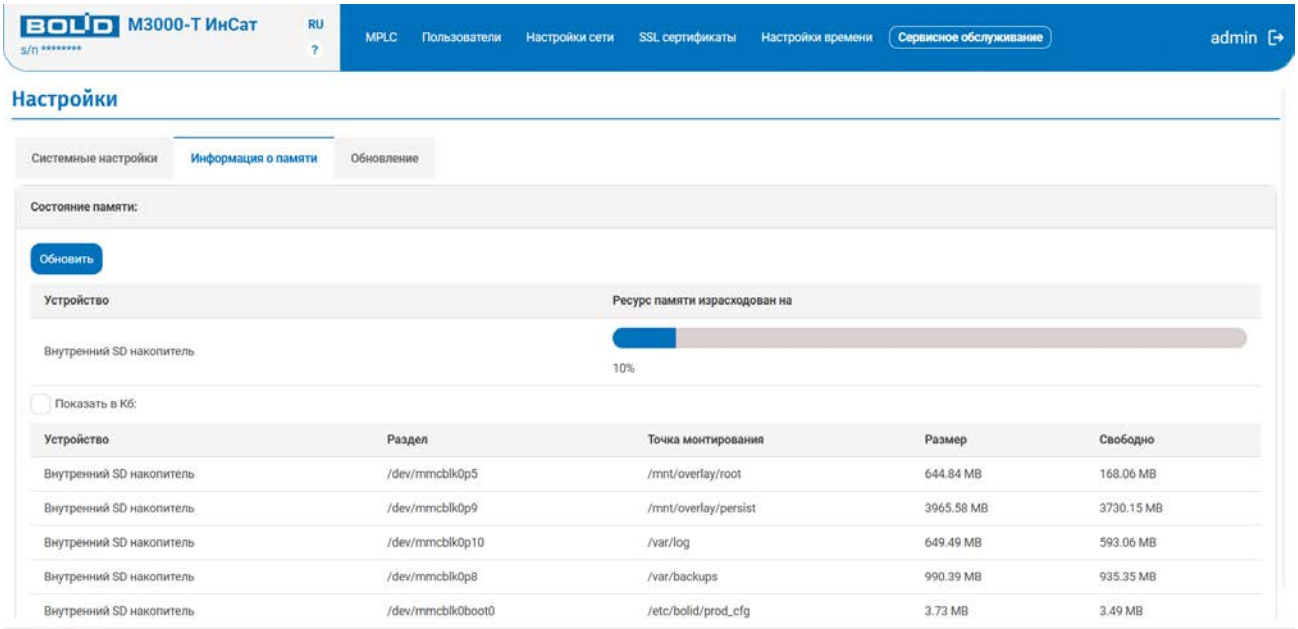


Рисунок 28. Страница «Сервисное обслуживание», вкладка «Информация о памяти»

Начальная цифра ресурса (даже у нового контроллера) всегда 10%. Максимально выработанный ресурс – 90%. Следует учитывать, что ресурс тратится в моменты записи. В случае если производится интенсивная запись больших объёмов во встроенную память контроллера, может произойти «затирание» этой памяти, **что повлечет снятие с гарантии!**

Типичная ошибка, приводящая к расходу ресурса памяти - это **архивирование процесса пользователем со временем цикла Задачи**, в которой объявлены переменные с атрибутом «**архивирование**».

То есть, если время цикла такой Задачи, составляет 100 мс, то при архивировании в этой Задаче только одной переменной типа «вещественное», ячейка памяти в 8 байт будет записываться 10 раз в секунду, 600 раз в минуту, 36000 раз в час, 864000 циклов записи в сутки. За это время записанный архив (лишь одной вещественной переменной без меток времени) составит 6912000 байт. Используемый тип памяти – eMMC – имеет ресурс порядка 3 000 циклов перезаписи. Очевидно, что запись во встроенную память контроллера с такой интенсивностью приведёт к её преждевременному «затиранию».

Контроллер сам перераспределяет уже стёршиеся блоки памяти как неиспользуемые, в связи с чем, оставшийся объём будет постоянно уменьшаться.

При необходимости сохранения архивов оперативных параметров необходимо:

- архивирование производить на внешние носители информации – SD-карты и USB-накопители;
- архивировать промежуточные переменные, которые объявлены в Задаче с большим временем цикла, к примеру - 1 минута;
- архивировать медленно меняющиеся переменные (параметры), только тогда, когда они изменяются или существенно изменяются (запись по изменению).

Окно среды разработки MasterSCADA 4D с элементами настройки архива представлено на Рисунках 29.1 и 29.2.

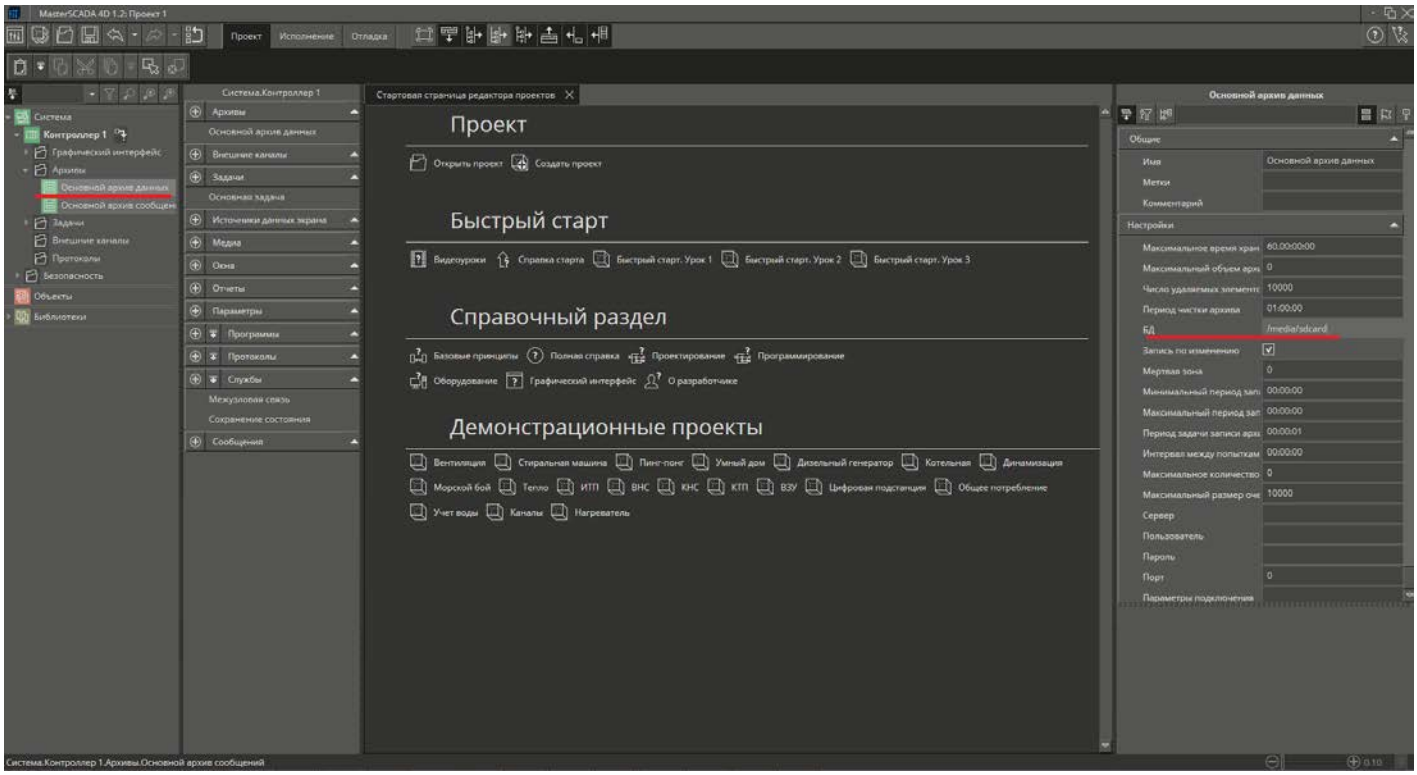


Рисунок 29.1. Окно среды разработки MasterSCADA 4D с элементами настройки архива (общий вид окна).

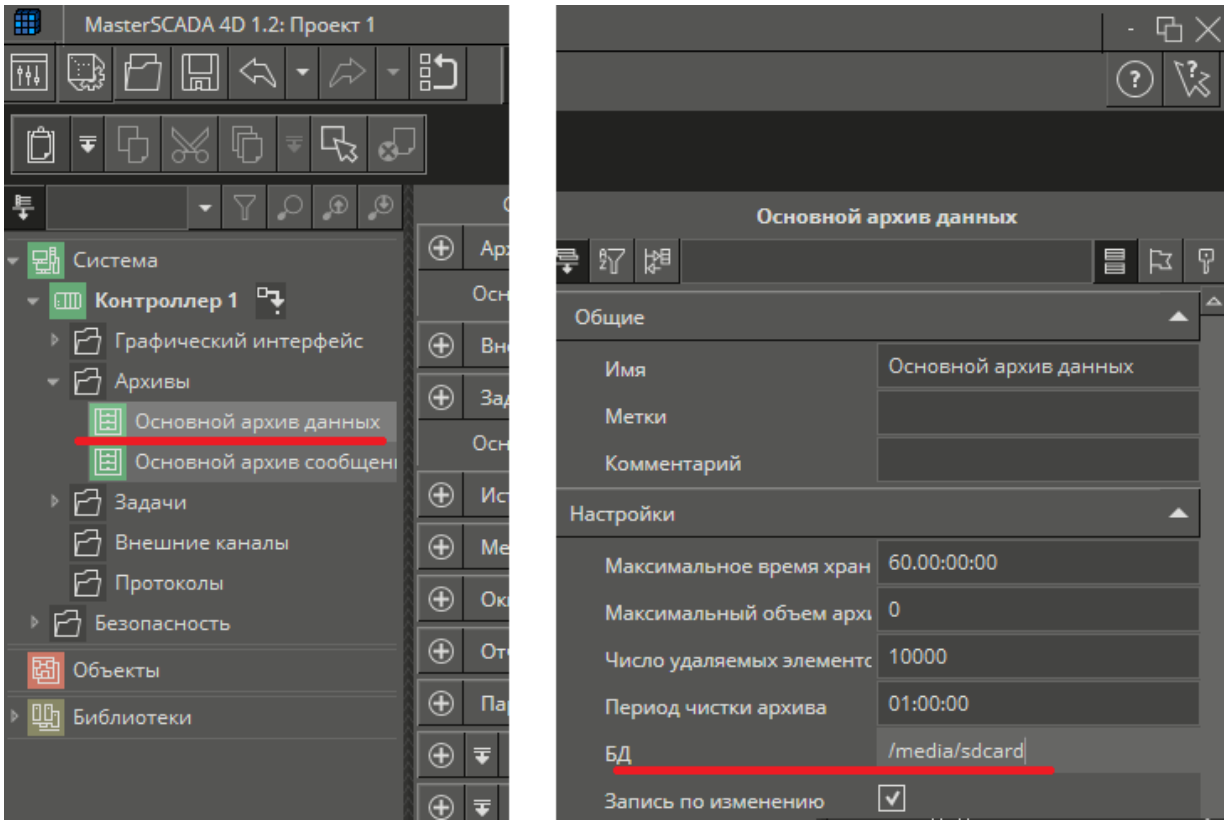


Рисунок 29.2. Фрагменты окна среды разработки MasterSCADA 4D с элементами настройки архива (дерево объектов слева и настройки архивирования справа).
Архивирование производится по изменению на внешнюю SD-карту.

Внимание!

Внешняя память (SD-карта или USB-накопитель), на которую предполагается производить архивирование, должна быть отформатирована в формате FAT32, (**ОБЯЗАТЕЛЬНО** извлечена из компьютера **БЕЗОПАСНО**) и вставлена в **ВЫКЛЮЧЕННЫЙ** контроллер.

Установленные в контроллер внешние накопители отражаются в настройках (*см. Рис. 28*). Если габариты USB-накопителя препятствуют закрытию контроллера, то следует использовать кабель-удлинитель.

Для сохранения резервной копии следует перейти на страницу «**MPLC**» и нажать кнопку «**Скачать резервную копию**» (*см. Рис. 4*), после чего откроется диалоговое окно (*см. Рис. 30*).

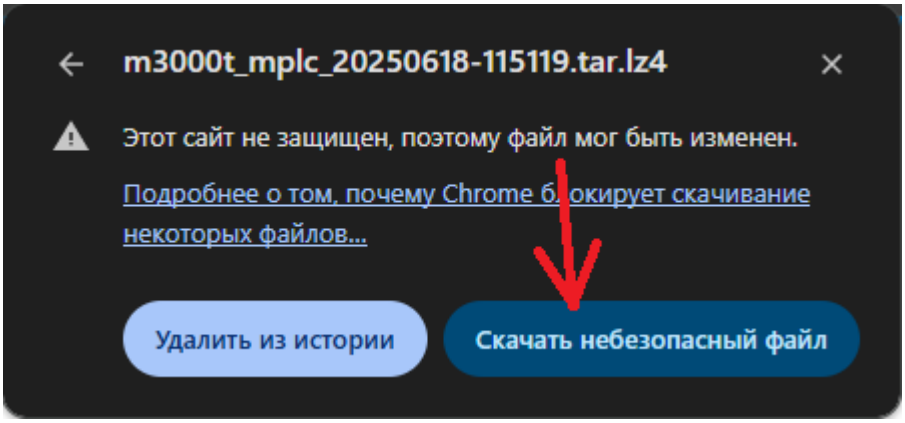


Рисунок 30. Диалоговое окно сохранения резервной копии.

При нажатии клавиши «Скачать небезопасный файл» или же «ОК» (в зависимости от браузера) производится сохранение файла. Процесс и результат загрузки можно просмотреть в окне «Загрузки» (*см. Рис. 31*).

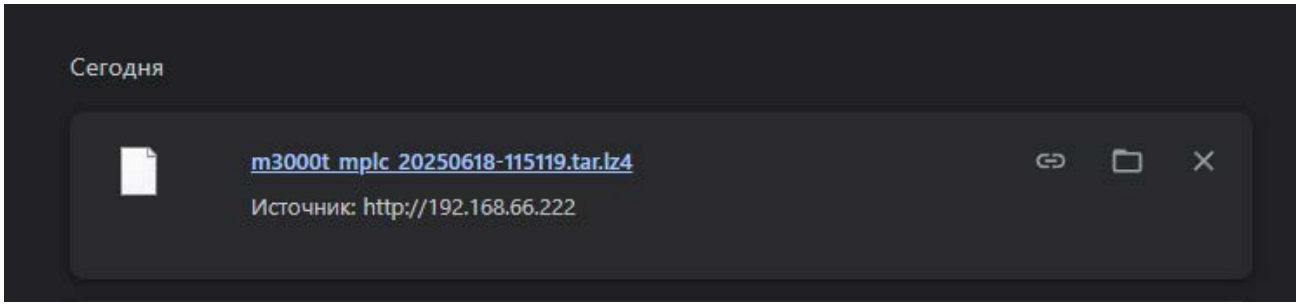


Рисунок 31. Окно загрузки резервной копии.

Для восстановления резервной копии нажимаем кнопку «**Восстановить резервную копию**», после чего открывается диалоговое окно в файловой системе ОС для поиска искомого файла. При двойном клике ЛКМ по необходимому файлу происходит его загрузка и восстановление резервной копии.

Внимание!

Важно! Установка архивов резервных копий на ПЛК, созданных НЕ контроллером СТРОГО ЗАПРЕЩЕНА.

Внимание!

Активирование и изменение лицензии на встроенное ПО производится при непосредственном участии компании-производителя ПО ИНСАТ.

Среда разработки, а также демо-версия среды исполнения с ограничением времени работы в режиме опроса периферийного оборудования и межузлового обмена в течение часа предоставляются бесплатно.

Активация применяется для исполнительной системы, работающей на любой операционной системе, кроме Windows. Без активации исполнительная система работает в демо-режиме. При подключении к среде исполнения из редактора (среды разработки) будет выдано системное сообщение об окончании работы в демо-режиме.

При нажатии клавиши «Получить код» будет выведено сообщение, содержащее код активации (*см. Рис. 32*), который вместе с номером лицензии (восьмизначное число на марке на процессорном модуле контроллера) и названием организации необходимо отправить по электронному адресу **scada@insat.ru**. В ответ вы получите файл для активации лицензии.

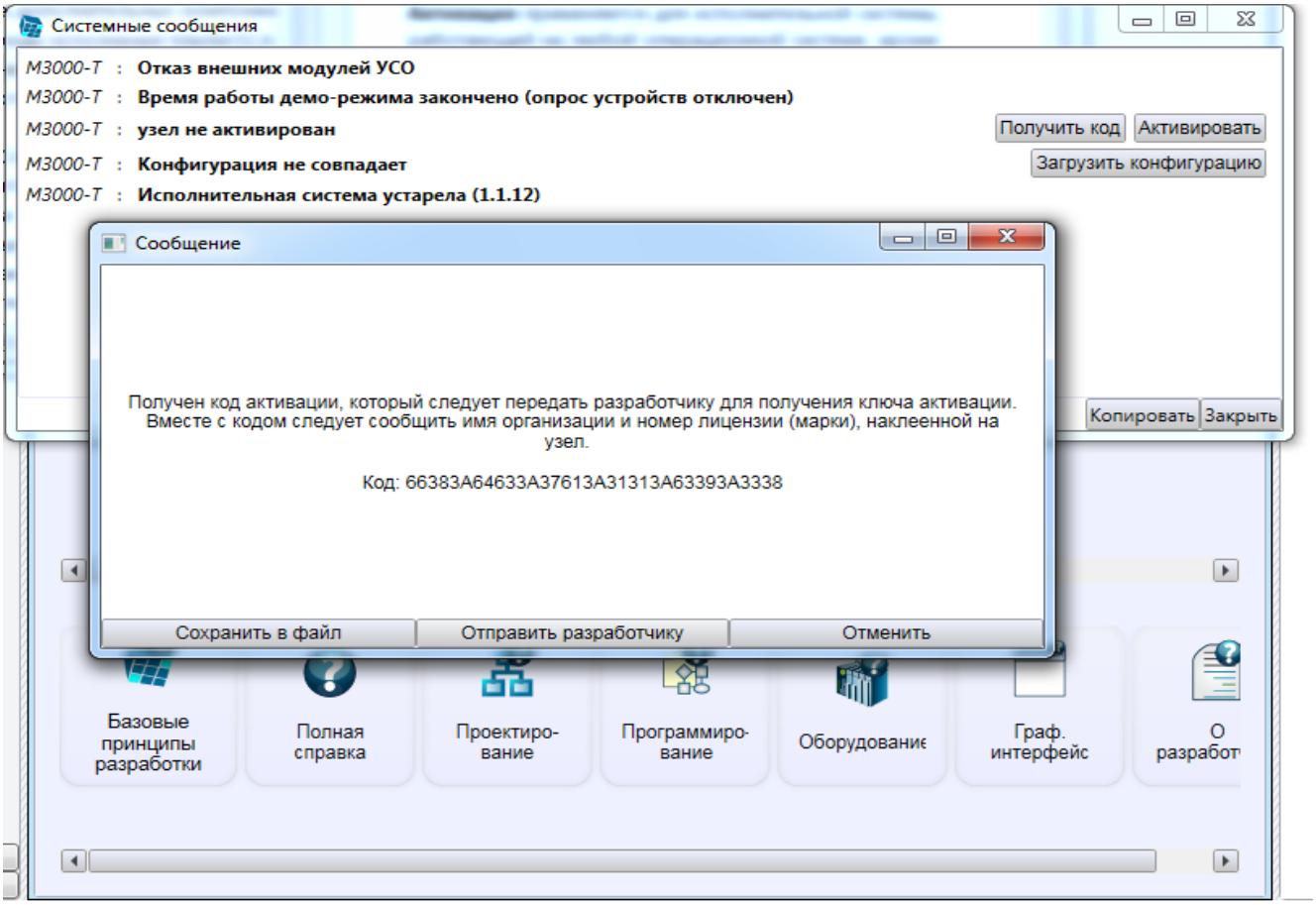


Рисунок 32. Окно с полученным кодом активации.

Активировать полученный ключ возможно на странице «**MPLC**» нажатием кнопки «Загрузить» соответственно пункту «Лицензия MasterPLC» и далее выбором присланного файла для активации лицензии и его применением (*см. Рис. 33*).

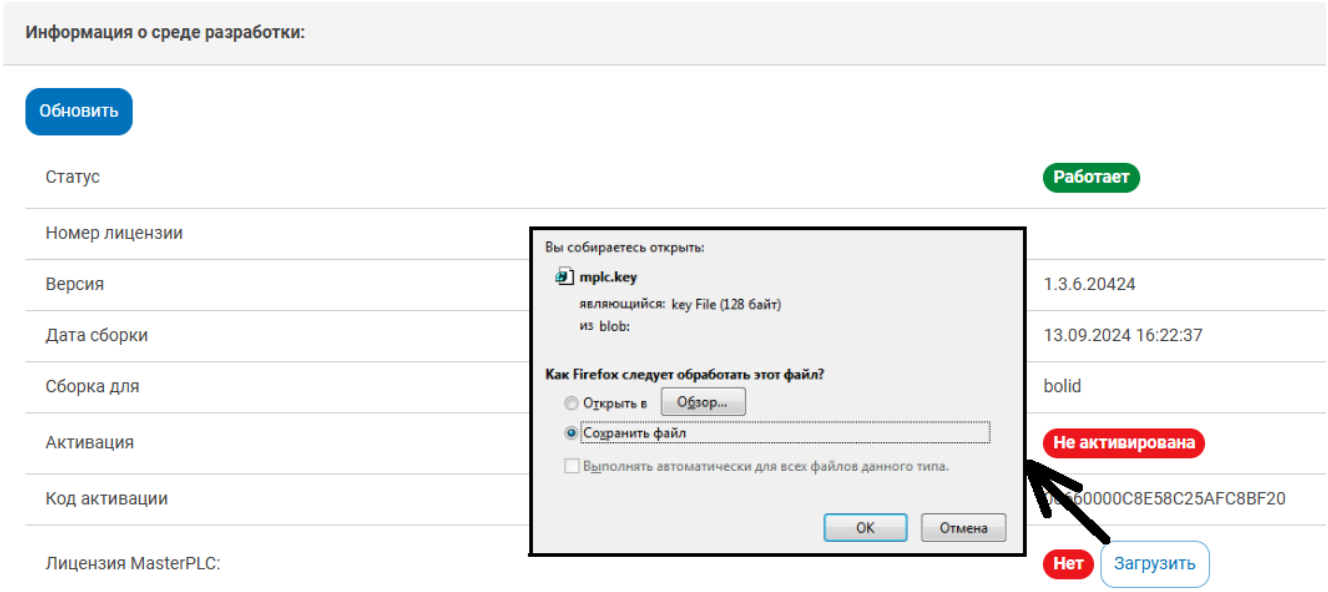


Рисунок 33. Диалоговое окно открытия файла лицензии

5.3.8 – 3 – Вкладка «Обновление».

Данная вкладка предназначена для обновления прошивки контроллера через веб-конфигуратор. Внешний вид вкладки представлен на Рисунке 34.1.

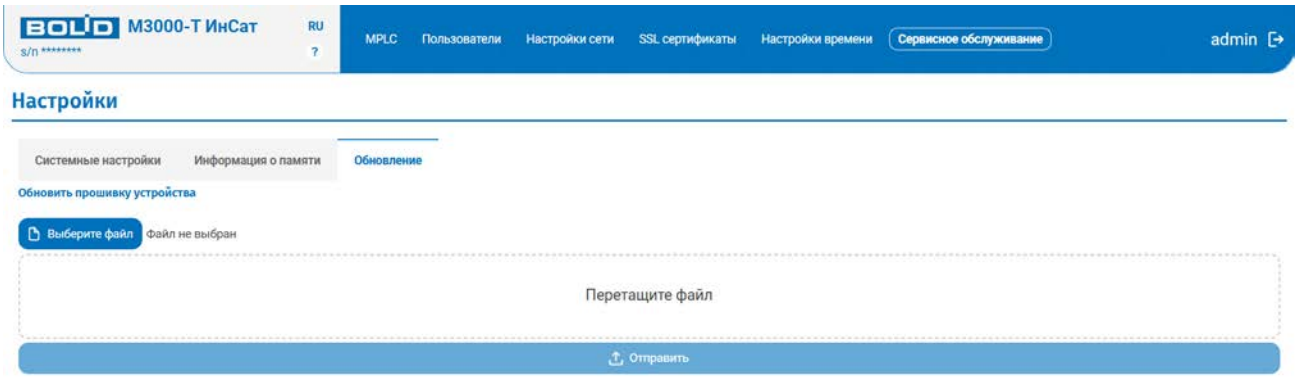


Рисунок 34.1. Вкладка «Обновление»

Контроллер имеет возможность обновления версии своего встроенного программного обеспечения («прошивки»). Новая версия ПО позволяет расширить функционал прибора и/или устранить недостатки имеющейся версии.

Внимание!

Перед обновлением прошивки устройства рекомендовано сохранить Ваш текущий проект.

Для этого необходимо перейти на страницу MPLC и нажать кнопку «**скачать резервную копию проекта**» и при необходимости «**Восстановить из резервной копии**»!

При обновлении прибор загружает в контроллер заводскую версию проекта системы SCADA!

Список доступных прошивок «М3000-Т Инсат», их ключевые особенности и рекомендуемые обновления доступны на сайте bolid.ru (ссылка кликабельна) в соответствующем разделе «Прошивки».

Обновление прошивки осуществляется через веб-конфигуратор контроллера. Подробнее *читать пункт 9.2 «Обновление прошивки через веб-конфигуратор»* настоящего Руководства.

6. УСТАНОВКА СВЯЗИ

Перед тем, как проводить любые действия в сети, целесообразно убедиться, что контроллер и компьютер находятся в одной «подсети» и проверить наличие связи между компьютером и контроллером.

Учитывая, что заводские настройки IP-адреса контроллера - 192.168.0.50, то и компьютер должен иметь IP-адрес в диапазоне 192.168.0.0 … 192.168.0.250, исключая 192.168.0.50 (это адрес контроллера, а двух одинаковых адресов быть не должно) и маску подсети 255.255.255.0. Примерные настройки представлены на Рисунке 35.

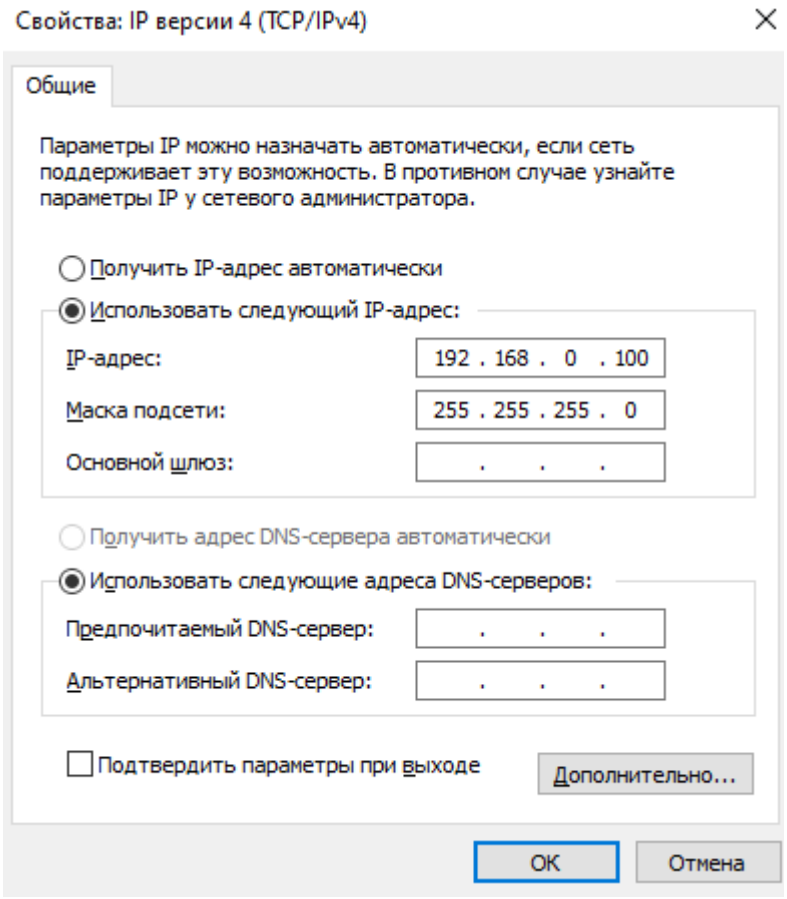


Рисунок 35. Сетевой адрес компьютера и маска подсети

Наиболее простой способ проверки целостности и качества соединения – воспользоваться специальной одноимённой утилитой «**Ping**». Для этого необходимо выполнить следующую последовательность действий:

- нажать «**Windows+R**» и в появившемся окне «**Выполнить**» в поле «**Открыть**», ввести «**cmd**» (*см. Рис. 36*):

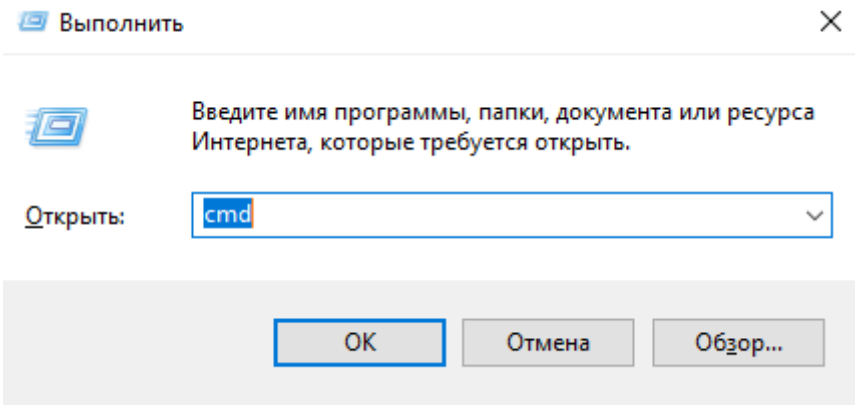


Рисунок 36. Окно «Выполнить»

- нажать «ОК». В появившейся командной строке» (*см. Рис. 37*), вводим команду «**ping**», пробел и адрес контроллера «192.168.0.50»:

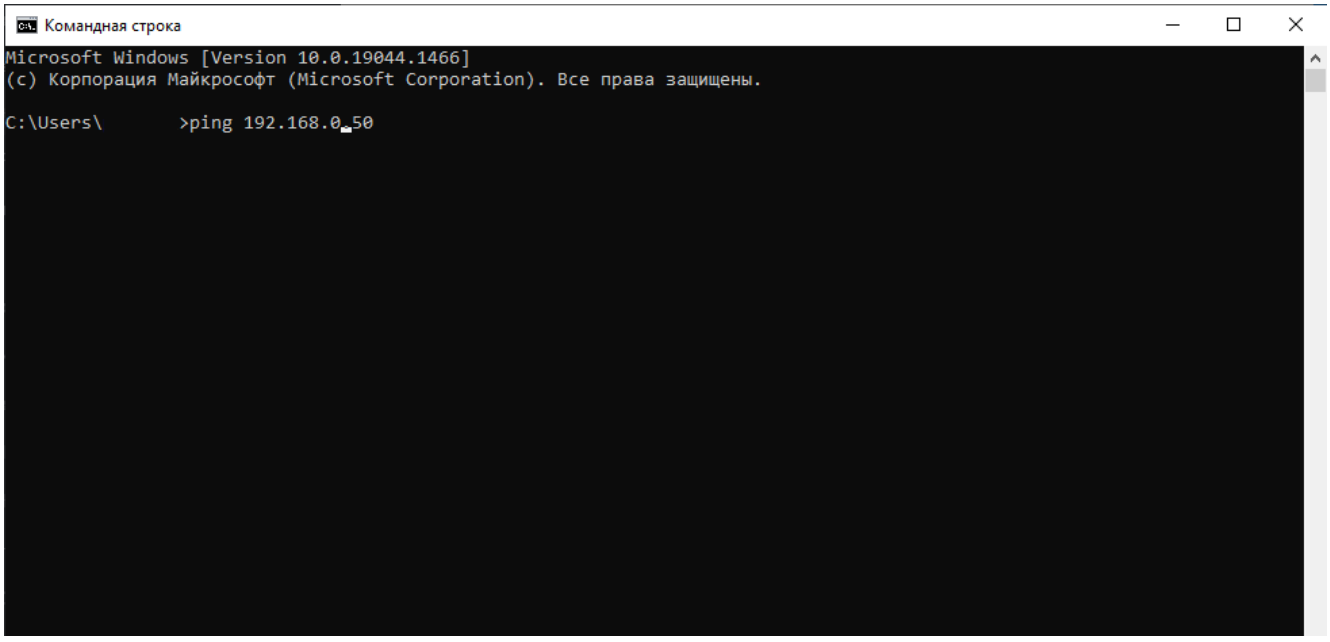


Рисунок 37. Окно командной строки. Результат вписанной команды.

- нажимаем «Enter» и получаем информацию по наличию и качеству связи, (*см. Рис. 38*):

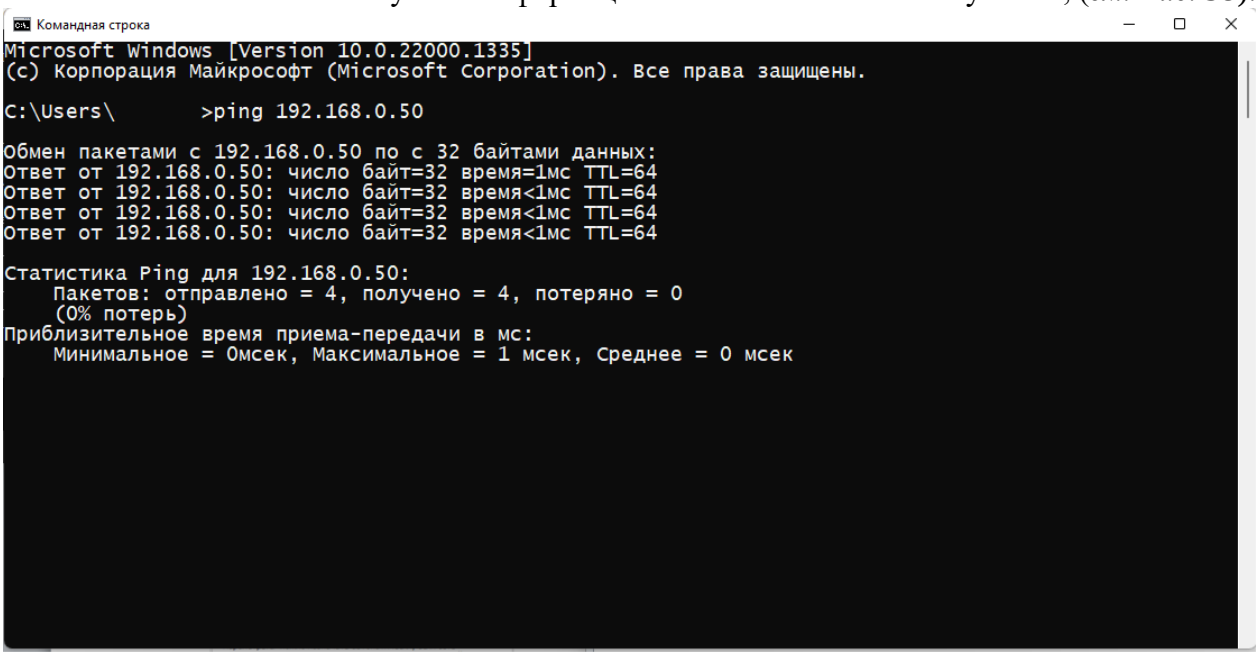


Рисунок 38. Окно «Командная строка». Статистика обмена пакетами.

Как видим, из четырёх отправленных 32-х байтных пакетов ни один не потерялся, а время ожидания - 1 миллисекунда - вполне приемлемое.

6.1 Установка связи по интерфейсу Ethernet

При установке связи по интерфейсу Ethernet в программе «PuTTY», необходимо подключить контроллер к компьютеру через витую пару (штекер 8P8C, разъём на контроллере - XS2), после чего указать IP-адрес контроллера (*см. Рис. 39*) и нажать кнопку «Open».

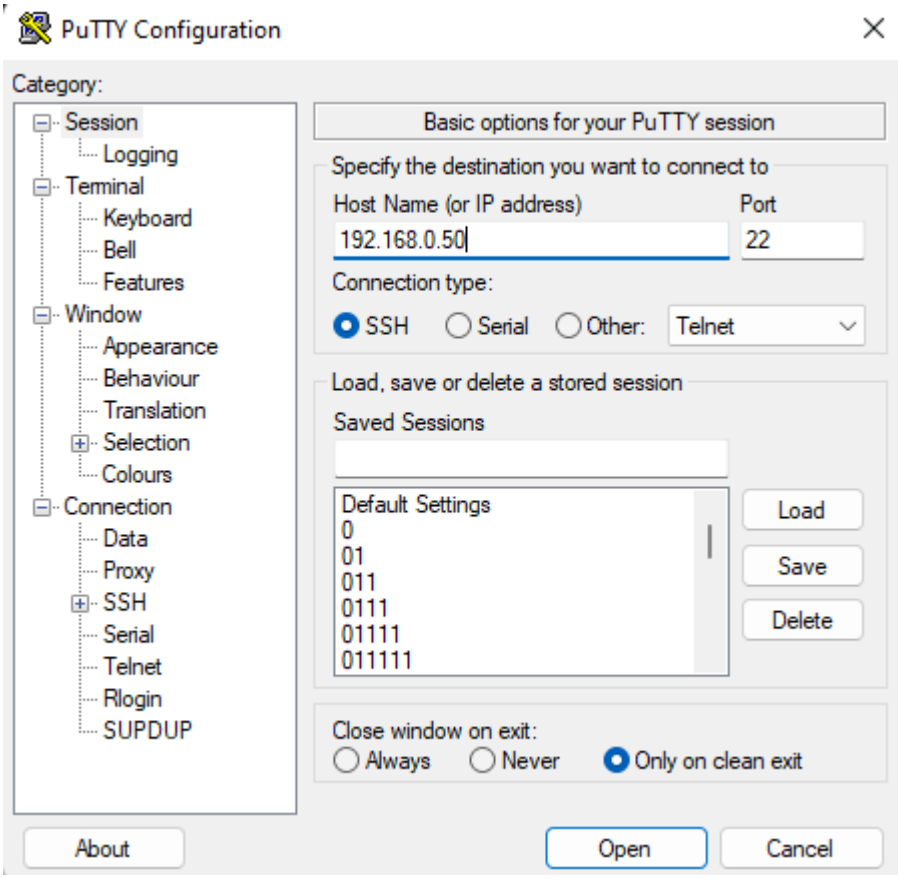


Рисунок 39. Ввод IP-адреса контроллера

В открывающемся окне при первом подключении выводится сообщение о возможной угрозе безопасности (*см. Рис. 40*). Для продолжения процесса установки следует нажать «Accept».

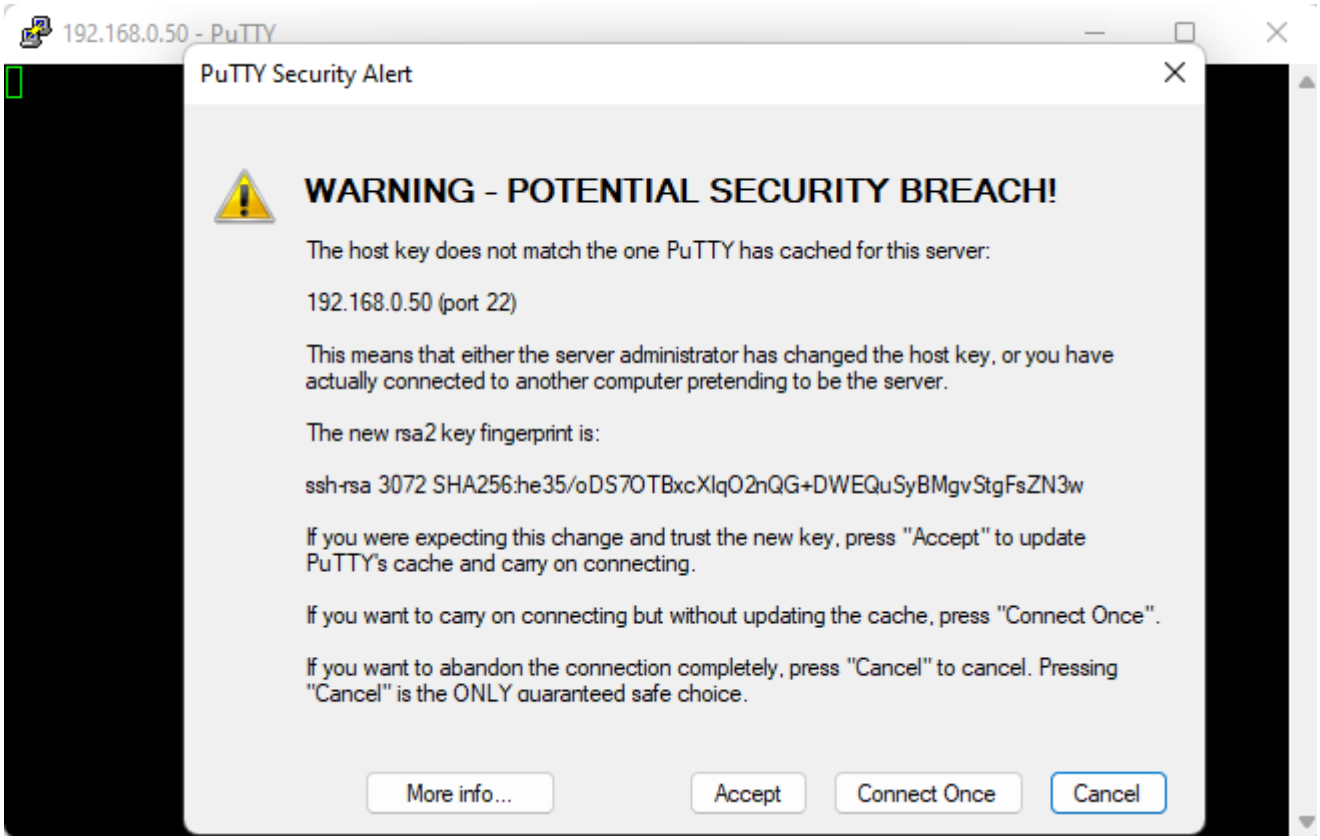


Рисунок 40. Сообщение о возможной угрозе безопасности.

На экране монитора появится текстовое окно для ввода логина (*см. Рис. 41*). После ввода логина появится текстовое окно для ввода пароля (*см. Рис. 42*) и система запросит ввод пароля (без отображения вводимых символов пароля).

Рисунок 41. Окно ввода логина.

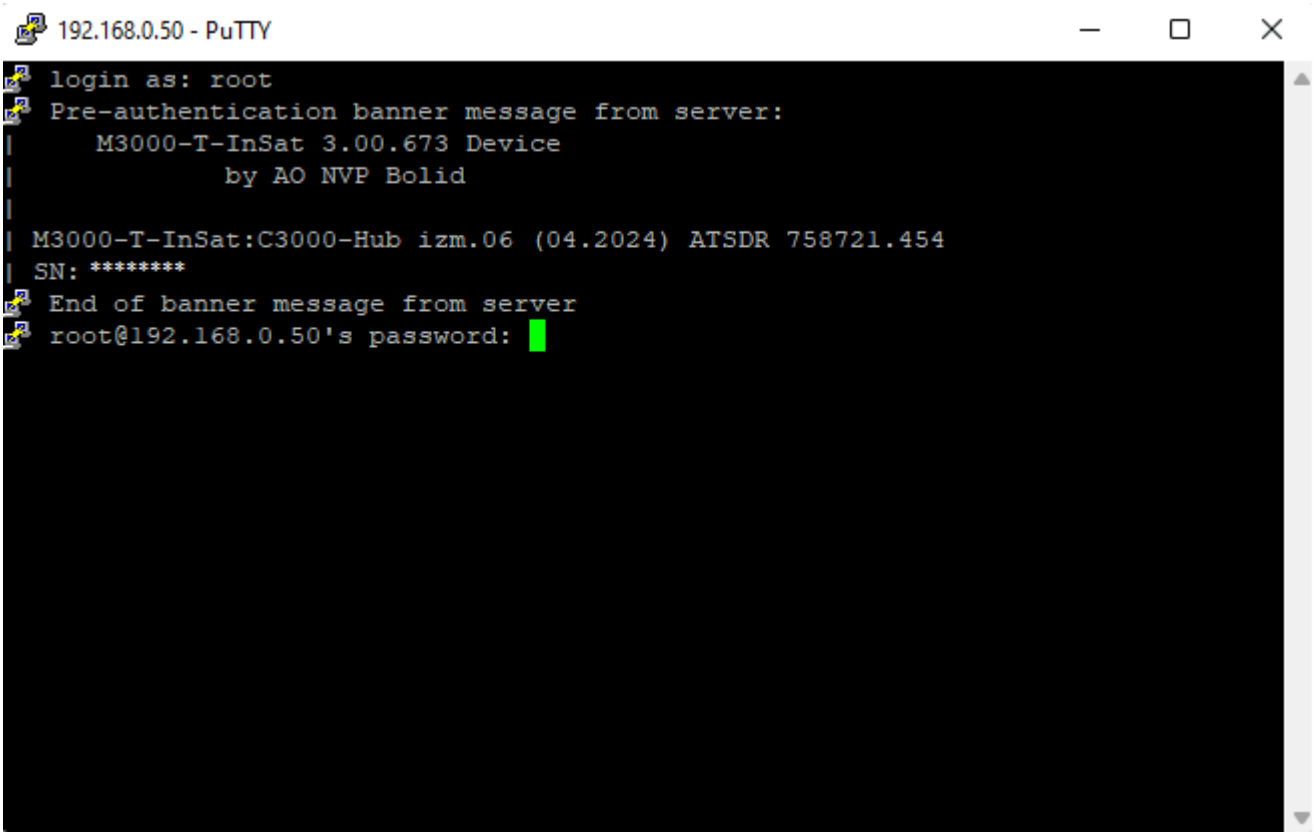


Рисунок 42. Окно ввода пароля.

6.2 Установка связи по интерфейсу MicroUSB

При установке связи по интерфейсу MicroUSB требуется:

1) Подключить USB шнур к разъёму X1 (MicroUSB с поддержкой USB OTG), после чего найти номер появляющегося при этом COM-порта;
2) В программе «**PuTTY**» выбрать тип соединения «Serial»;
3) В разделе «**Serial**» выбрать следующие параметры: 115200; 8; 1 (*на Рис. 43 параметры отмечены цифрами 1, 2, 3 соответственно*);
4) В разделе «**Session**» ввести номер USB-порта, к которому подключен контроллер (*см. Рис. 44*) и нажать кнопку «Open».

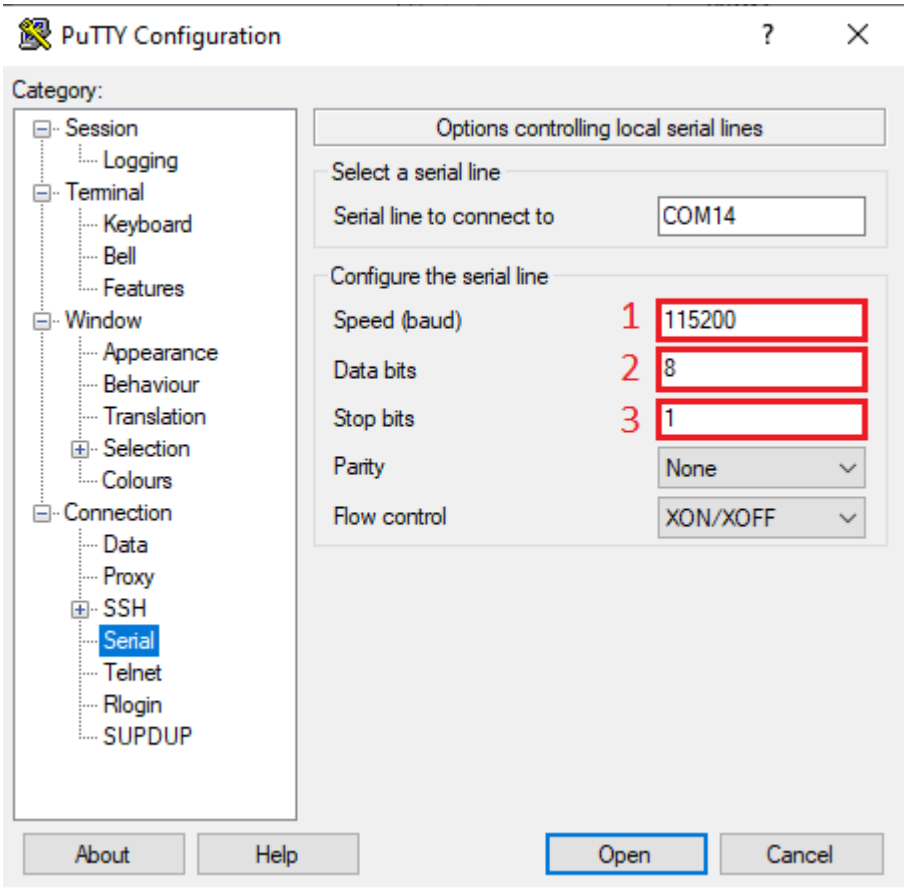


Рисунок 43. Установка параметров MicroUSB подключения

В открывающемся окне установить параметры USB-порта согласно Рисунку 45, после чего установить параметры соединения (*см. Рис. 44*). После чего следует нажать «Open».

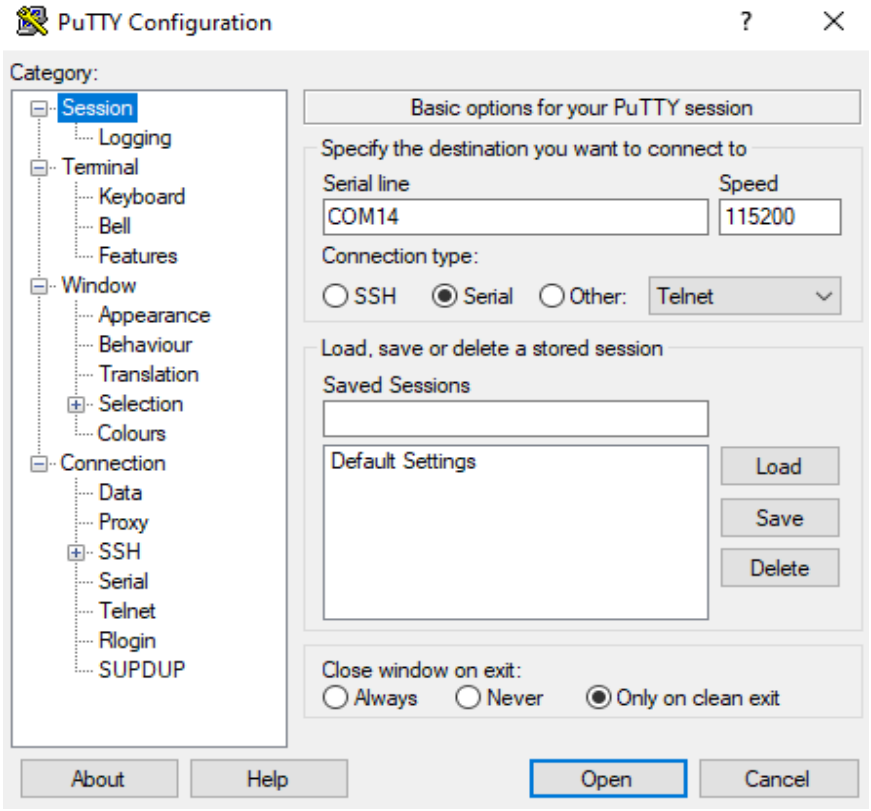


Рисунок 44. Установка параметров соединения

При запуске контроллера в открывающемся окне появляются служебная информация и диалоговое окно для ввода логина (*см. Рис. 41*), пароля (*см. Рис. 42*). После загрузки контроллера автоматическая выдача информации в порт прекращается.

6.3 Установка связи по интерфейсу MicroUSB со спецификацией USB OTG

Подключение к контроллеру посредством интерфейса MicroUSB с поддержкой USB OTG, позволяет сделать контроллер сетевым устройством. Подключение по данному интерфейсу требует:

1) Подключения USB шнура к разъёму X1 (MicroUSB с поддержкой USB OTG);
2) В программе «Диспетчер устройств» найти во вкладке «Другие устройства» устройство с названием «CDC NCM», после чего нажать по нему ПКМ и перейти во вкладку «Обновить драйвер» (*см. Рис. 45)*;

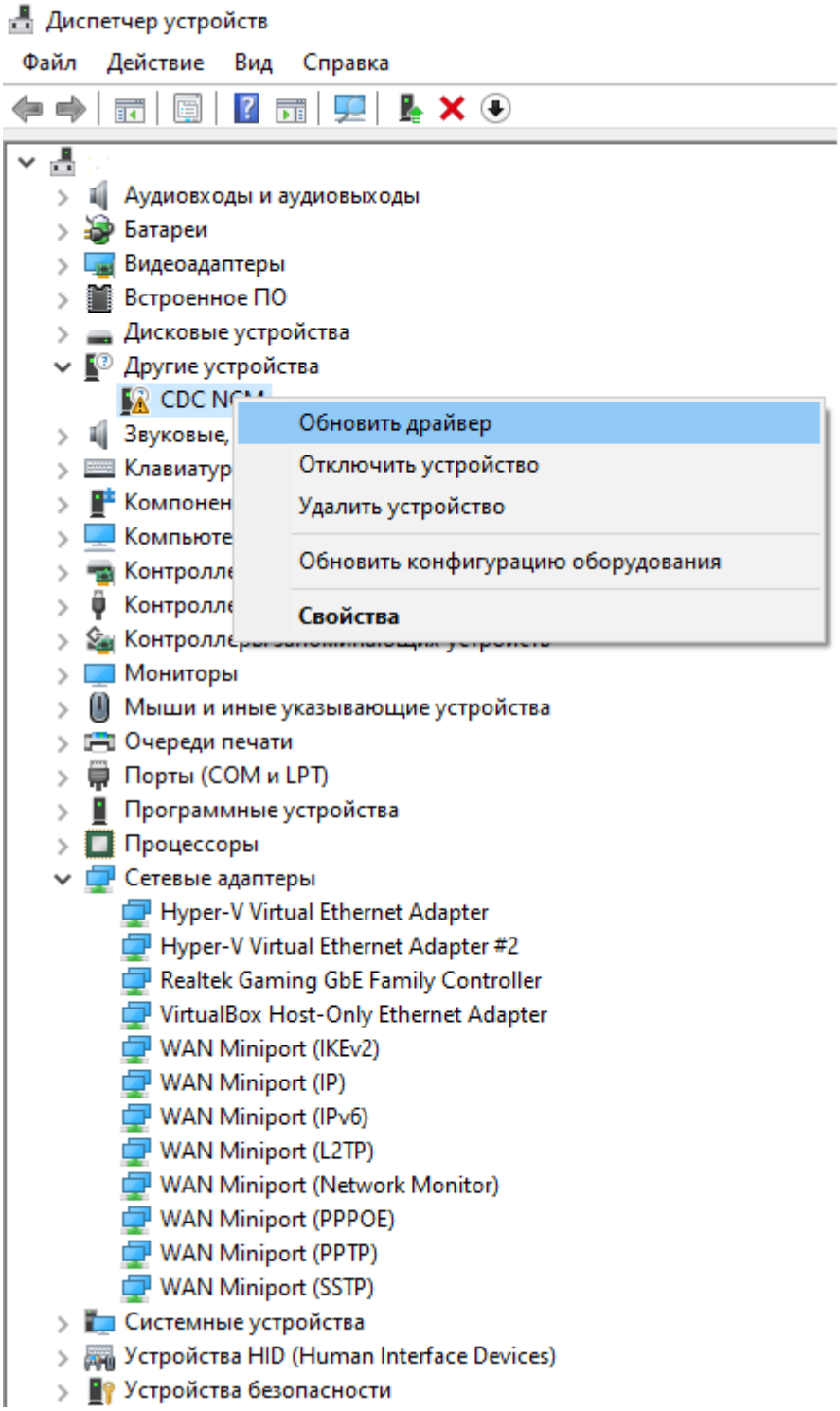


Рисунок 45. Программа «Диспетчер устройств», выбор вкладки «Обновить» для контроллера

3) В появившемся окне по поиску драйверов следует выбрать вариант «Автоматический поиск драйверов», после чего найти в списке возможных устройств «Сетевые адаптеры» и нажать кнопку «Далее» (*см. Рис. 46, Рис. 47*).

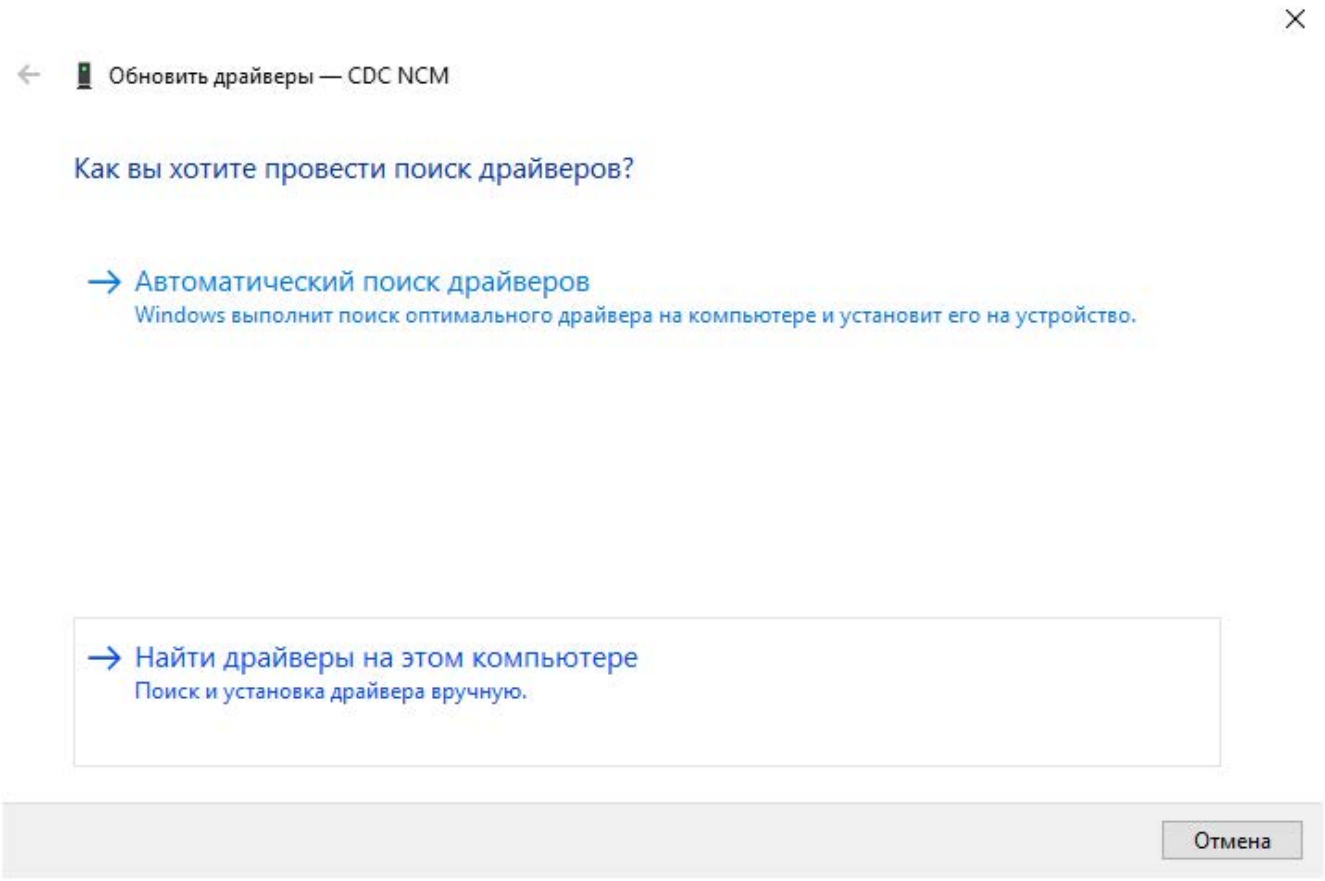


Рисунок 46. Окно с поиском драйверов

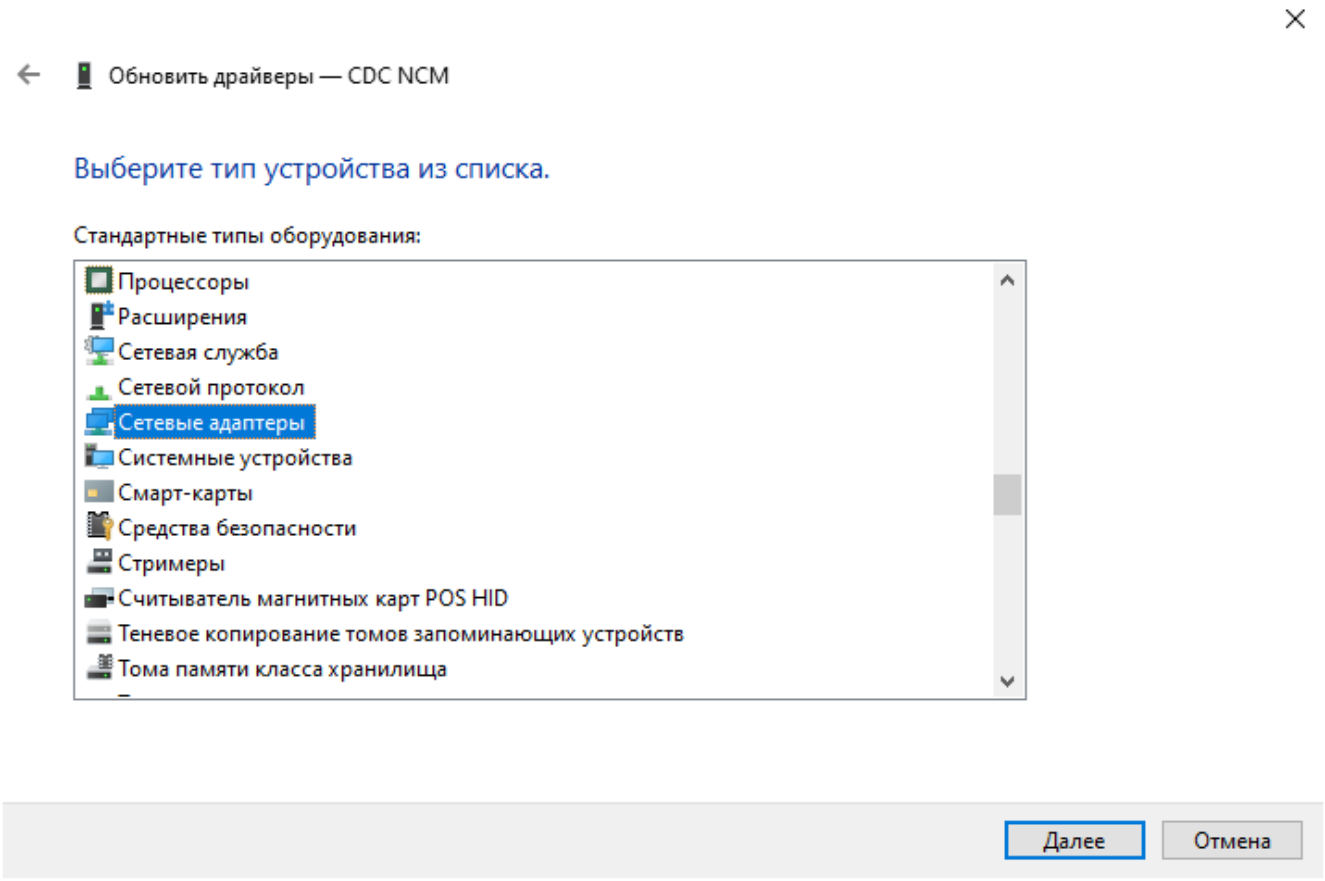


Рисунок 47. Список с типами устройств; выбранный тип – «Сетевые адаптеры»

4) В дальнейшем необходимо найти изготовителя драйвера «Microsoft» в левой стороне окна, после чего найти модель «UsbNcm Host Driver» и установить её.

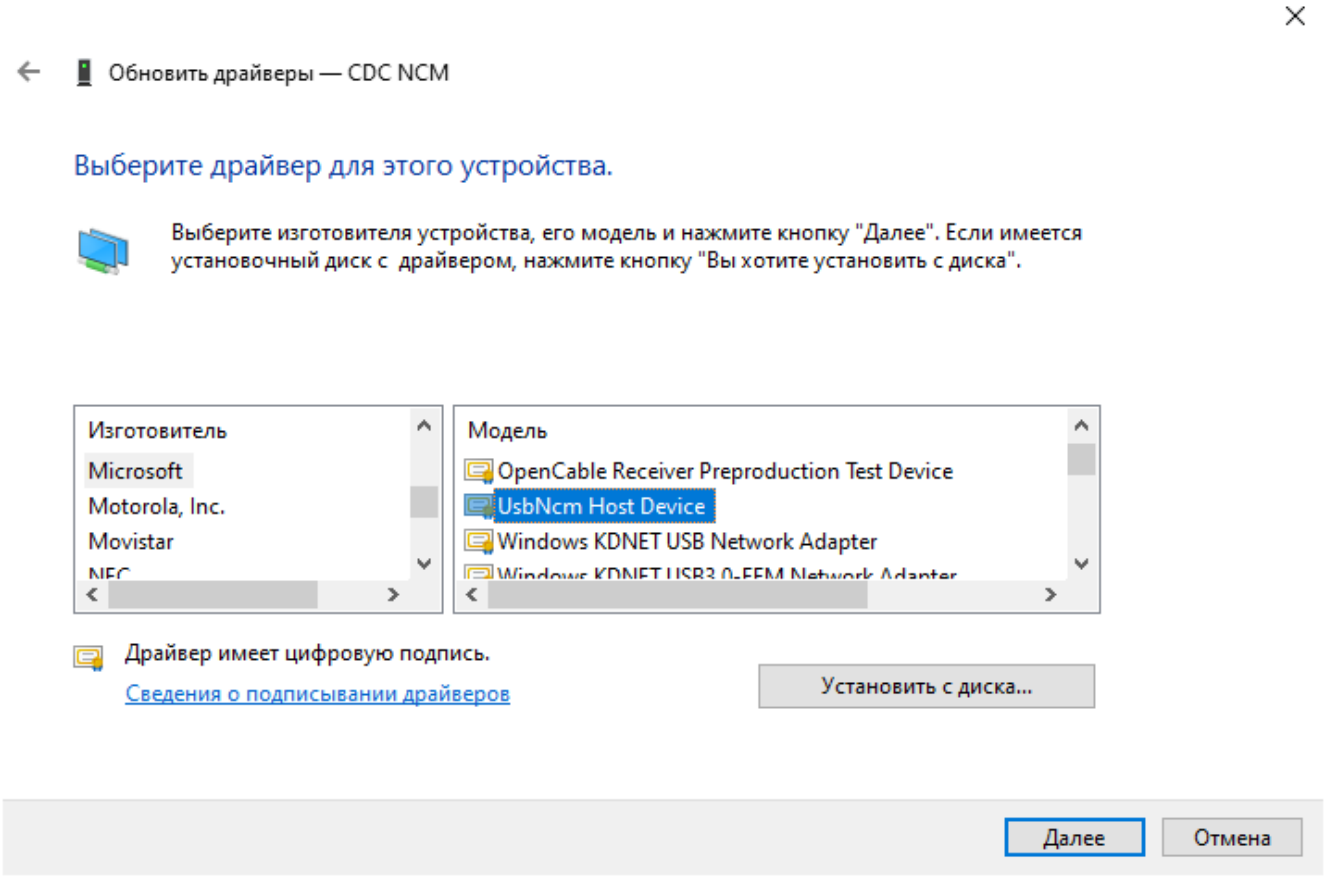


Рисунок 48. Выбор драйвера для установки

6.4 Тамперные коды контроллера

В контроллере предусмотрена возможность изменения некоторых конфигурационных параметров при помощи набора комбинации коротких и длинных нажатий датчика вскрытия корпуса (тампера, на схеме – S1), расположенного на плате.

Состояния тампера:

- **Длинное нажатие (тире или «1»)** – это удержание тампера в состоянии «Нажато» в течение более 0,5 сек, но менее 6 сек.
- **Кратковременное нажатие (точка или «0»)** – это удержание тампера в состоянии «Нажато» в течение 0,02…0,5 сек. Пауза между кратковременными нажатиями должна быть не менее 0,02 сек.

Примечания:

- Отсутствие нажатия на тампер в течение более 2 секунд является признаком конца набора комбинации.
- Нажатие на тампер длиною более 6 секунд аннулирует комбинацию нажатий для введения кода.

Для сброса настроек необходимо при запуске контроллера дождаться начала «перемигивания» светодиодов «Работа» и «232D» зелёным цветом, и произвести комбинацию нажатий «тире» и «точка» тампером.

Предусмотрены следующие варианты включения и сброса прибора тампером:

1) Полный сброс к заводским настройкам:

«точка» - «точка» - «точка» - «тире» - «тире» - «тире» - «точка» - «точка» - «точка»;

0 - 0 - 0 - 1 - 1 - 1 - 0 - 0 - 0.

2) Сброс сетевых адресов на значения, указанные в инструкции:

«тире» - «тире» - «тире» - «точка»

1 - 1 - 1 - 0

3) Сброс пароля владельца на заводское значение:

«тире» - «тире» - «точка» - «точка» - «тире» - «тире» - «точка» - «точка»

1 - 1 - 0 - 0 - 1 - 1 - 0 - 0

Прочие тамперные коды можно получить от технической поддержки, в случае возникновения проблем с работой прибора/затруднении в эксплуатации (*читать п. «Необходимость техподдержки»*).

Таблица 11. Специальные режимы включения, сброса и загрузки

Комбинация нажатий тампера	Режим
0 0 0 1 1 1 0 0 0	полный сброс устройства к заводским настройкам
1 1 1 0	сброс сетевых адресов на значения, указанные в инструкции
1 1 0 0 1 1 0 0	сброс пароля владельца на заводское значение

7. КОНФИГУРИРОВАНИЕ

Использование по назначению

Перед использованием ПЛК необходимо запрограммировать, т.е. создать пользовательскую программу. Созданная пользовательская программа может быть сохранена в энергонезависимой Flash-памяти контроллера, а также может запускаться после включения питания или перезагрузки. Программирование осуществляется с помощью ПО «MasterSCADA 4D», которое можно скачать на сайте www.insat.ru. Для связи со средой программирования используется интерфейс контроллера: Ethernet. Активация лицензии ПО «MasterSCADA 4D» проводится сотрудниками технической поддержки компании «Инсат» (www.insat.ru) по лицензионному ключу, расположенному на процессорном модуле контроллера.

Изменение начальной конфигурации контроллера

Изменение конфигурации и программирование ПЛК производится в среде разработки «MasterSCADA 4D».

1. Работа с операционной системой Linux в консольном режиме.

Для консольного доступа к системе Linux используется порт MicroUSB. Для ввода команд подойдет любая терминальная программа, например, «PuTTY». Для подключения необходимо задать следующие сетевые настройки последовательного порта:

- Скорость (бит/с): 115200;
- Биты данных: 8;
- Четность: Нет;
- Стоповые биты: 1;
- Управление потоком: Нет

Данный порт позволяет отслеживать диагностическую информацию контроллера в процессе загрузки: сетевые настройки, версию прошивки, объем памяти и т.д. Также существует возможность доступа к консоли Linux по интерфейсу Ethernet с использованием протокола SSH. Доступ осуществляется по IP-адресу контроллера и порту «22».

Консольный доступ позволяет работать со встроенной операционной системой напрямую, используя команды операционной системы Linux. Для входа в консольный режим требуется дождаться полной загрузки ПЛК, после чего в терминальной программе нажать «Enter».

Появится окно, в котором следует ввести:

в поле ввода логина «Логин»: «**root**» (по умолчанию; в протоколе http(s) - «**admin**»),

в поле ввода пароля «Пароль»: **p@ssw0rd1234** (по умолчанию).

Полный перечень команд и более подробную информацию об их использовании можно найти на сайте разработчика: https://busybox.net/downloads/BusyBox.html.

2. Изменение версии программного обеспечения.

Изменение версии программного обеспечения контроллера производится в веб-конфигураторе (*читать пункт 9.2 «Обновление прошивки устройства через веб-конфигуратор»* настоящего Руководства).

8. ПРОВЕРКА РАБОТОСПОСОБНОСТИ

Самодиагностика основных узлов контроллера производится автоматически при включении контроллера или после выполнения команды «Сброс».

- произвести визуальный контроль работоспособности контроллера;
- убедиться в постоянном свечении светодиода «Работа», что свидетельствует о наличии напряжения питания и его соответствии норме;
- убедиться в мигающем режиме светодиодов активных портов RS-485 при обмене;
- при подключении порта Ethernet должна быть светодиодная индикация на разъёме XS2 интерфейса Ethernet (при установке соответствующих сетевых настроек 192.168.0.1/24).

9. ОБНОВЛЕНИЕ ПРОШИВКИ КОНТРОЛЛЕРА

Внимание!

Перед началом работы с прошивкой стоит учитывать два немаловажных фактора, которые могут повлиять на будущую работу контроллера!

НАСТОЯТЕЛЬНО рекомендовано ознакомиться с абзацами ниже, перед тем как приступать к пунктам 9.1 и 9.2, непосредственно связанным с обновлением ПО устройства!

При работе с прошивкой контроллера есть два ключевых фактора, способные повлиять на его работу при окончании обновления:

- При необходимости обновления прошивки контроллера на более совершенную версию (современнее той, что установлена на контроллере ДО обновления), необходимо будет прочитать **журнал обновлений**, указанный на странице с доступными для скачивания материалами контроллера этой ссылке.

  В журналах обновлений указывается информация о том, какие настройки контроллера будут сохранены и какие будут обнулены при обновлении прошивки.

  IP-адрес, а также логин и пароль от веб-конфигуратора при обновлении на новую версию всегда остаются неизменными!

- При необходимости обновления прошивки на более старую версию (выпущенную в релиз раньше той, что установлена на контроллере ДО обновления), необходимо учитывать, **что содержимое памяти** (настройки контроллера, данные для авторизации в веб-конфигураторе) **будет полностью стёрто, а сам контроллер обращён до заводских настроек!**

  IP-адрес, логины и пароли будут обращены в те, что описаны в данном Руководстве!

Для обновления прошивки контроллера предусмотрены два метода:

Первый вариант (читать пункт 9.1) – использование интерфейса MicroUSB со спецификацией USB OTG. Для этого необходимо установить связь между контроллером и компьютером (*читать пункт 6.3*) и загрузить новую прошивку в соответствии с пунктом 9.1 настоящего Руководства.

Второй вариант (читать пункт 9.2) – обновление через веб-конфигуратор. Для этого необходимо загрузить файл прошивки с сайта bolid.ru, после чего загрузить его в конвертер веб-конфигуратора устройства, и провести инсталляцию необходимой версии прошивки (*читать пункт 9.2*).

Обновление прошивки устройства через веб-конфигуратор

В конвертер веб-конфигуратора - расположенный на вкладке «Обновление», страницы «Сервисное обслуживание» - загружается файл обновления прошивки (скачанный с сайта bolid.ru). Необходимо перейти на необходимую вкладку, нажать кнопку «Выбрать», после чего выбрать нужный файл прошивки в проводнике ПК и нажать кнопку «Загрузить» (*см. Рис. 49, поз. 1, поз.2, поз. 3*):

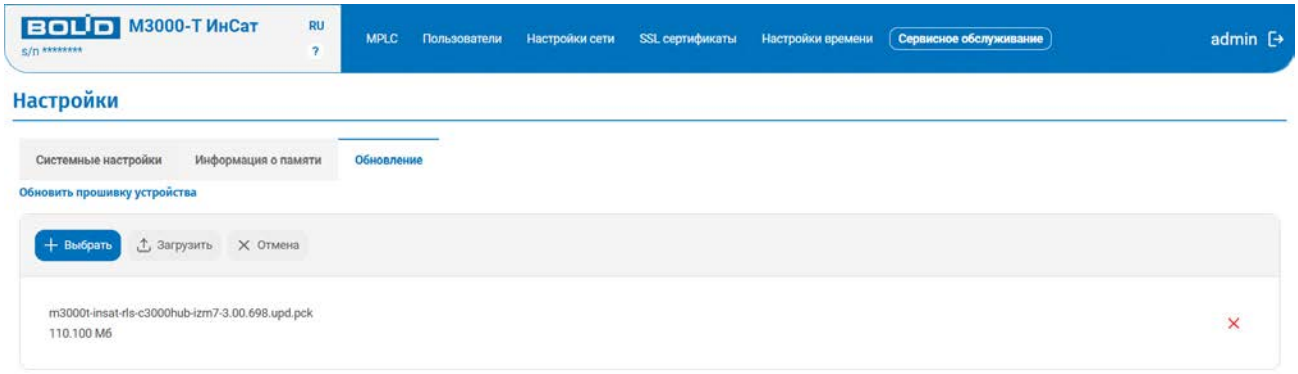


Рисунок 49, позиция 1. Страница «Сервисное обслуживание», вкладка «Обновление». Файл прошивки загружен в конвертер веб-конфигуратора ПЛК.

После нажатия на кнопку «Загрузить», веб-конфигуратор покажет окно по центру экрана, в котором можно будет наблюдать три этапа загрузки файлов на контроллер; процесс можно остановить в любой момент, нажав на соответствующую кнопку «Остановить»:

1. Проверка файла обновления. Заключается в удостоверении целостности файла прошивки и возможности обновления контроллера. Внешний вид окна представлен на рисунке 49, поз. 2.

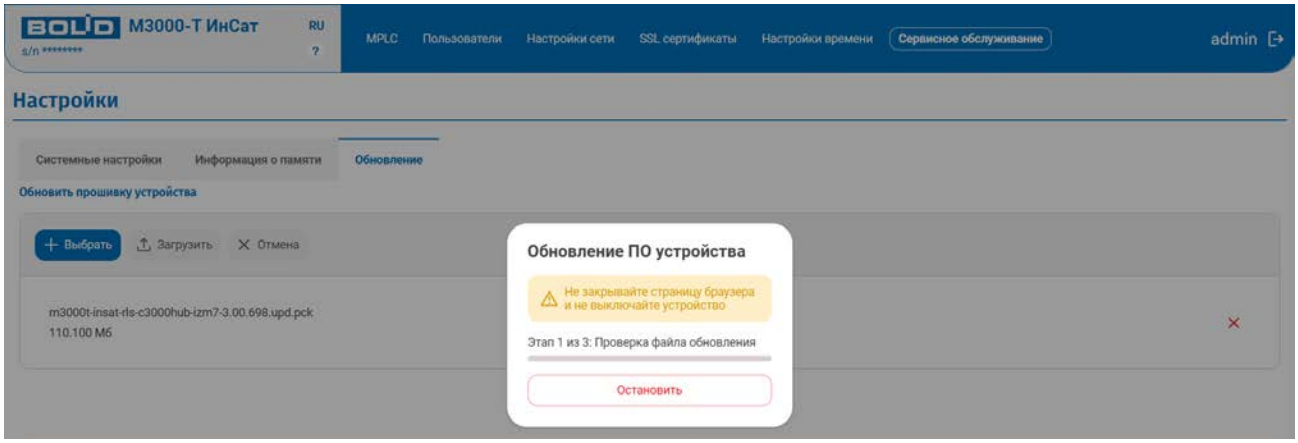


Рисунок 49, позиция 2. Обновление прошивки на устройстве через веб-конфигуратор. Окно проверки файла обновления.

2. Загрузка файла на устройство. Важный процесс, в течение которого происходит полная замена файлов прошивки. Прерывать процесс обновления ПЛК на данном этапе крайне нежелательно. Внешний вид окна представлен на рисунке 49, поз. 3.

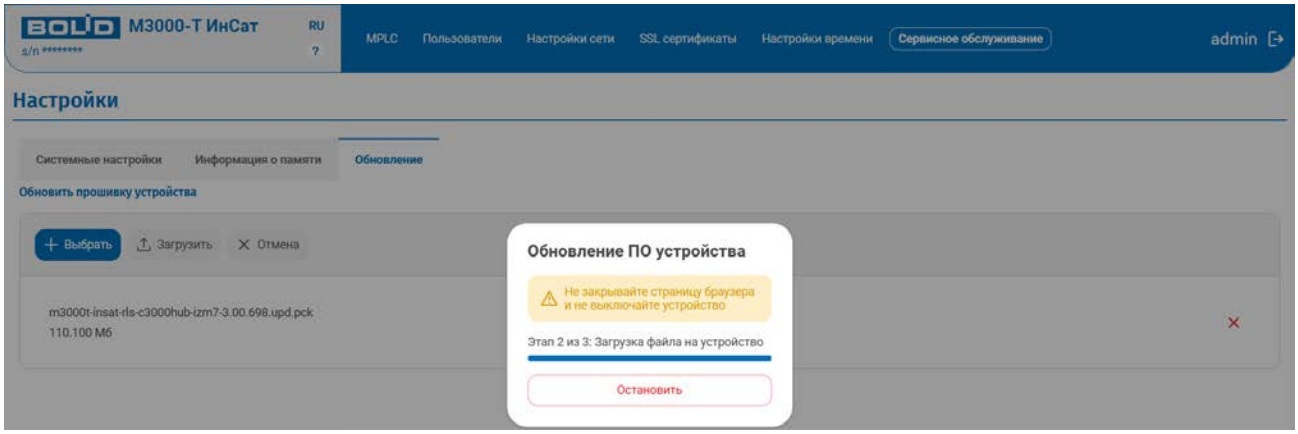


Рисунок 49, позиция 3. Обновление прошивки на устройстве через веб-конфигуратор. Окно загрузки файлов на устройство.

Удачный исход обновления

При удачном обновлении прошивки происходит автоматическая перезагрузка прибора, при этом связь с прибором теряется. После перезагрузки происходит автоматическое восстановление связи (*см. Рис. 50*).

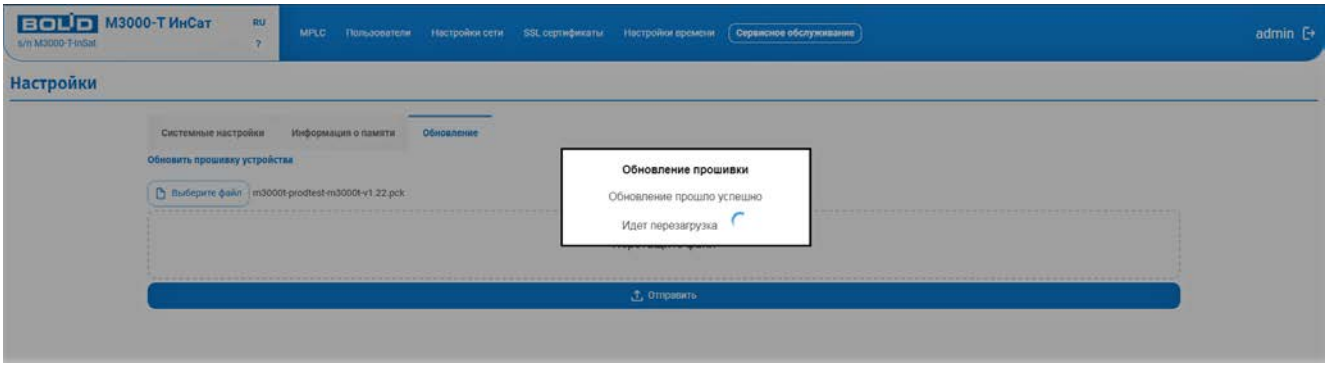


Рисунок 50. **Обновление прошивки на устройстве через веб-конфигуратор.**
Происходит перезагрузка ПЛК.

Неудачный исход обновления

При провале обновления, загрузка обновления на прибор будет прекращена, в центре экрана будет выведено предупредительное окно об ошибке при загрузке прошивки с описанием проблемы в обновлении. В таком случае, пользователю следует обратиться в техподдержку с детальным описанием проблемы (*читать п. «Необходимость техподдержки»*). Общий возможный вид проваленного обновления показан на рисунке 51.

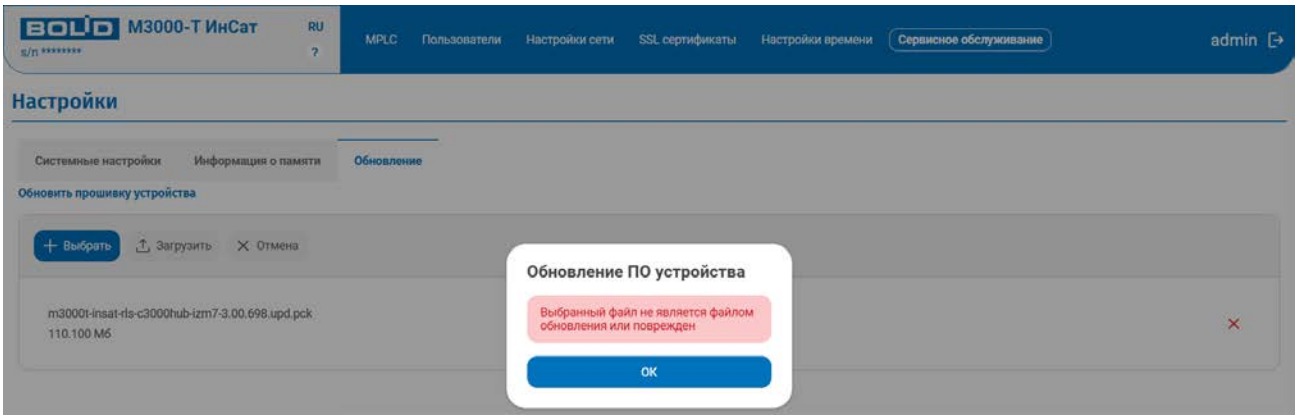


Рисунок 51. Возможный вариант неудачного исхода обновления прошивки контроллера.

Внимание!

Перед началом работы с установкой обновлений необходимо:

- выключить все виртуальные машины, развернутые на вашем ПК;
- закрыть все окна от приложения Oracle VirtualBox (если таковые открыты);
- подключить MicroUSB ПЛК к USB порту материнской платы вашего ПК **напрямую! Не к лицевой панели!**

10. ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И РЕМОНТ

Работы по техническому обслуживанию выполняются не реже 1 раза в год обслуживающим персоналом, имеющим группу электробезопасности не ниже второй.

Обслуживание контроллера (замену батарейки часов и т.д.) производится исключительно при соблюдении мер защиты от статического электричества.

Техническое обслуживание контроллера производится по планово-предупредительной системе, которая предусматривает годовое техническое обслуживание. Работы по плановому годовому техническому обслуживанию включают в себя:

- проверку внешнего состояния контроллера;
- проверку работоспособности согласно пункту 8 настоящего Руководства;
- проверку надёжности крепления контроллера, состояния внешних монтажных проводов, контактных соединений;
- проверку оставшегося ресурса памяти по записи согласно пункту 5.5.1 настоящего Руководства (в пределах от 10 до 90%);
- проверка наличия новых обновлений прошивки контроллера на сайте bolid.ru; в случае необходимости – обновить прошивку устройства в соответствии с должными пунктами настоящего Руководства.
- в случае критичности параметров и динамики уменьшения ресурса памяти необходимо или уменьшить скорость, и/или уменьшить объём и/или место архивирования в соответствии с рекомендациями пункта «*5.3.8 – 2 – Информация о памяти*» настоящего Руководства.

Смена батарейки часов

Батарейка часов контроллера CR2032, устанавливаемая в контроллер, имеет срок работы в один год; минимальное рабочее напряжение батареи для должной работы составляет 2,2В, ниже которого аппарат перестаёт считать время.

Замена энергонакопителя происходит при наступлении момента разряжения заряда батарейки. Узнать состояние батареи можно, открыв файл, что находится во внутреннем хранилище контроллера по следующему пути:

/sys/class/power_supply/rtc-backup-battery/health

В файле можно будет увидеть два возможных состояния батарейки: *good* и *dead* – хорошее и «мёртвое» состояние соответственно. В первом случае, батарею менять необязательно (разве что в случае, когда срок действия батареи начинает подходить к концу); во втором же случае, замена батареи необходима, и должна быть проведена как можно скорее.

Для замены батарейки необходимо избавиться от статического электричества на руках, надев антистатические перчатки или антистатический браслет, затем обесточить прибор. Далее необходимо снять заднюю крышку контроллера и с помощью рендера печатной платы (*см. Приложение В настоящего Руководства*) найти в левом нижнем углу «Место установки элемента питания», заменить отработанную батарейку CR2032 на новую батарейку.

Основания на составление акта о неисправности и необходимости гарантийного ремонта не распространяются на ремонт ПЛК в случаях:

- несоблюдения потребителем правил монтажа, эксплуатации, транспортировки или хранения;
- наличия механических повреждений, возникших по вине потребителя;
- в случае поражения ПЛК статическим электричеством при замене батареи часов, вследствие ненадлежащего соблюдения мер предосторожности в соответствии с ГОСТ 12.1.018-93 «Пожаровзрывобезопасность статического электричества»;

– в случае превышения «верхнего потолка» напряжения питания на ПЛК (выше 28В);
– в случае извлечения процессорного модуля контроллера при любых обстоятельствах;
– повышенного износа памяти ПЛК в результате большого числа быстрых операций по сохранению архивов.

Не пытайтесь снять печатную плату контроллера, это автоматически аннулирует гарантийные обязательства!

Внимание!
Претензии принимаются только при наличии приложенного акта о необходимости ремонта с описанием возникшей неисправности.

Акты о неисправности и о необходимости техподдержки направлять по адресу:
АО НВП «Болид», Россия, 141070, Московская область, г. Королёв, ул. Пионерская, 4.
Тел.: **+7 (495) 775-71-55**. E-mail: info@bolid.ru.
Адрес места осуществления деятельности по изготовлению продукции:
141006, Московская обл., г. Мытищи, Ярославское ш., 120Б, стр. 3.

При затруднениях, возникших при эксплуатации контроллера, рекомендуется обращаться в техническую поддержку по телефону **+7 (495) 775-71-55** или по электронной почте support@bolid.ru.

11. ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Перечень возможных неисправностей и способов устранения приведён в таблице 12.

Таблица 12. Возможные неисправности ПЛК и методы их устранения

Наименование неисправности	Вероятная причина	Способы устранения
1) При подключении к сети «12В» прибор не включается. Индикаторы на лицевой панели выключены	Нет напряжения питания	Проверить наличие напряжения
2) При подключении к сети Ethernet нет доступа к контроллеру в окне браузера	1) Неправильно выставлен IP-адрес. 2) Проект пользователя не загружен в контроллер.	- Подключиться к контроллеру по порту MicroUSB и выставить IP-адрес - Сбросить сетевые настройки - Загрузить в контроллер программу пользователя с визуализацией
3) При подключении к сети Ethernet нет доступа к контроллеру в окне браузера, доступ у страницы сетевых настроек работает.	Используется браузер Internet Explorer	Подключиться используя браузер Mozilla/Google Chrome
4) Отсутствует индикация обмена порта RS-485	Неправильно выставлены номера подключенных портов	Проверить номера портов в проекте
5) ПЛК не подаёт признаков работы после извлечения процессорного модуля	Извлечение процессорного модуля во время подачи напряжения на прибор	Отсутствуют, право на гарантийный ремонт не распространяется

12. ТРАНСПОРТИРОВАНИЕ, ХРАНЕНИЕ, УТИЛИЗАЦИЯ

- В транспортной таре контроллеры могут храниться в неотапливаемых складских помещениях при температуре окружающего воздуха от минус 50°С до плюс 50°С и относительной влажности до 95% при температуре плюс 35°С.
- Контроллеры должны храниться в потребительской таре в отапливаемых складских помещениях при температуре от минус 5°С до плюс 40°С и относительной влажности до 80% при температуре плюс 20°С.
- Хранение прибора происходит в обесточенном режиме с извлеченной батарейкой часов в соответствующей таре, указанной пунктами выше.
- Содержание драгоценных материалов: не требует учёта при хранении, списании и утилизации (п. 1.2 ГОСТ 2.608-78).
- Утилизация контроллера производится с учетом отсутствия в нем токсичных компонентов.
- Содержание цветных металлов: не требует учёта при списании и дальнейшей утилизации изделия.

13. ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Изготовитель гарантирует соответствие требованиям технических условий при соблюдении потребителем правил транспортирования, хранения монтажа и эксплуатации.

Гарантийный срок эксплуатации – 18 месяцев со дня ввода в эксплуатацию, но не более 24 месяцев со дня выпуска изготовителем.

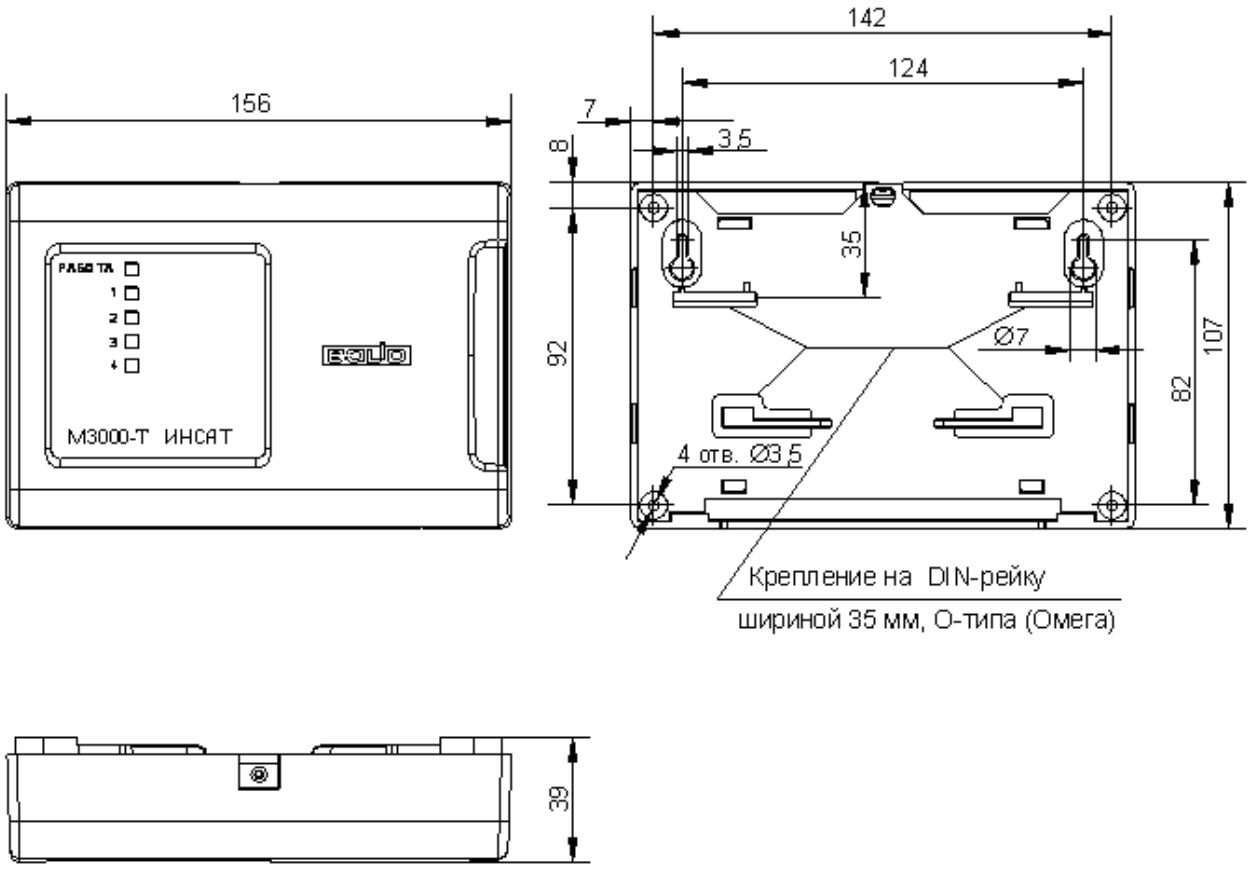
14. СВЕДЕНИЯ О СЕРТИФИКАЦИИ ИЗДЕЛИЯ

14.1 Контроллер программируемый логический «М3000-Т Инсат» АЦДР.421455.003 соответствует требованиям ТР ТС 020/2011 «Электромагнитная совместимость технических средств» и имеет декларацию о соответствии ЕАЭС N RU Д-RU.PA08.B.76525/25.

14.2 Производство контроллеров имеет сертификат соответствия ГОСТ Р ИСО 9001. Сертификат соответствия размещен на сайте http://bolid.ru в разделе «О компании».

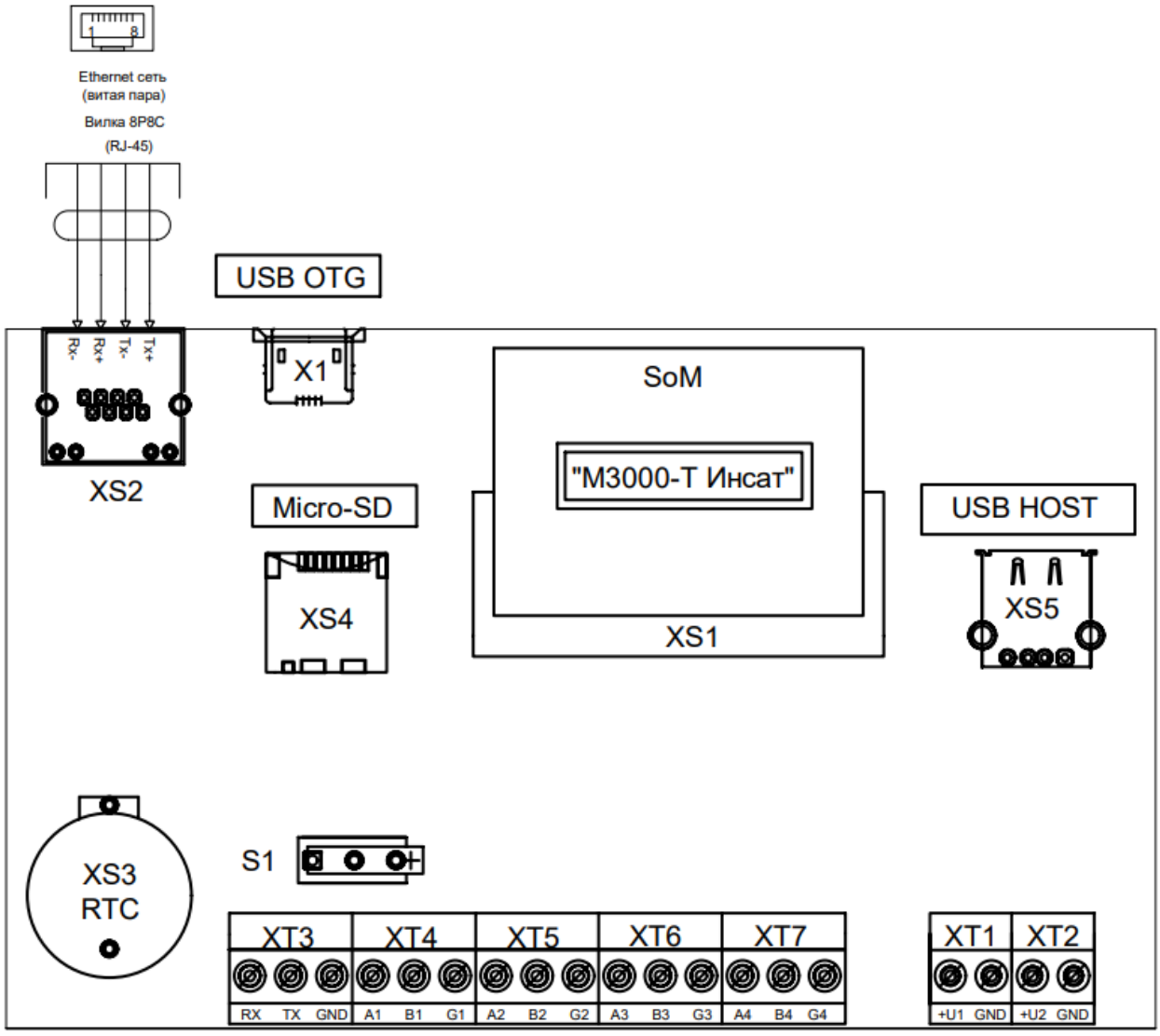
ПРИЛОЖЕНИЕ А

Габаритные и установочные размеры контроллера «М3000-Т Инсат»



ПРИЛОЖЕНИЕ Б

Схемы внешних подключений



X1 – разъём для подключения MicroUSB с поддержкой спецификации USB OTG;
XS1 – разъём для установки процессорного модуля ПЛК;
XS2 – разъём для подключения Ethernet-кабеля (витой пары);
XS3 – разъём для установки батарейки часов ПЛК (Real-Time Clock – RTC);
XS4 – слот для подключения MicroSD-карты;
XS5 – USB HOST (USB-A) разъём для подключения Wi-Fi модема (для работы контроллера в качестве точки доступа Wi-Fi) и USB модема сотовой связи;

XT1, **XT2** – клеммы для подключения контроллера к источнику питания;
XT3 – клеммы для подключения интерфейса RS-232;
XT4, **XT5**, **XT6**, **XT7** – клеммы для подключения устройств интерфейса RS-485;

S1 – тампер для ввода кодов.

ПРИЛОЖЕНИЕ В
Рендер платы ПЛК «М3000-Т Инсат»