ИСО 9001

КОНТРОЛЛЕР ПРОГРАММИРУЕМЫЙ ЛОГИЧЕСКИЙ

"М3000-Т ИНСАТ"

Руководство по эксплуатации

АЦДР.421455.003 РЭп

2019

СОДЕРЖАНИЕ

Настоящее руководство по эксплуатации предназначено для ознакомления обслуживающего персонала с устройством, конструкцией, работой и техническим обслуживанием Контроллера программируемого логического «М3000-Т Инсат» версии 1.21 (далее по тексту контроллер или ПЛК). Контроллер выпускается согласно ТУ АЦДР.421455.008 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 1.2.4.7252.

Список принятых определений и сокращений:

ЛКМ – левая клавиша 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) – «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 с эталлоном;

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

UTC (англ. **U**niversal **T**ime **C**oordinated) — всеми́рное координи́рованное вре́мя — стандарт определения времени и даты;

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**iper **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**)** — 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

HTTPS/WSS — протокол соединения HTTP поверх TLS/SSL;

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 **Sh**ell**)** — (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.

1.2 Логика работы ПЛК определяется потребителем в процессе программирования контроллера. Программирование осуществляется с помощью программного обеспечения Инсат. При этом поддерживаются все языки программирования, указанные в МЭК 61131-3.

1.3 Область применения ПЛК: системы автоматизированного управления технологическим оборудованием в энергетике, на транспорте, в т.ч. железнодорожном, в различных областях промышленности, жилищно-коммунального и сельского хозяйства.

1.4 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 2.1.

Таблица 2.1 – Основные технические характеристики контроллера

Наименование характеристики	**Значение**
Операционная система	Linux
Среда разработки	MasterSCADA 4D
Встроенная среда исполнения	MasterSCADA 4D
Языки программирования	FBD/SFC/LD/ST/IL (Стандарт МЭК 61131-3)
Центральный процессор	Cortex™-A9 Core 1.0 Ghz
Объем оперативной памяти (тип памяти)	512MB (DDR3 RAM)
Объем энергонезависимой памяти общий (тип памяти)	4(8) GB (eMMC)*
Объем энергонезависимой памяти доступно пользователю (тип памяти)	3,2(7.2) GB (eMMC)*
Время выполнения пустого цикла, милисекунд	1 (настраивается в основной задаче) ПО MasterScada4D.
Дополнительное оборудование	– держатель СД-карты – часы реального времени – элемент питания.
Количество интерфейсов RS-485	4
Количество интерфейсов Ethernet	1
Количество интерфейсов USB	1
Количество отладочных интерфейсов RS- 232	1
Диапазон напряжения питания, В	от 10,2 до 28,4 постоянного тока
Потребляемый ток, мА: – при напряжении питания 12 В – при напряжении питания 24 В	 не более 260 не более 140
Количество входов питания	2
Диапазон температур, °С	от минус 40 до +55
Степень защиты оболочки по ГОСТ 14254-96	IP30
Масса контроллера, кг	не более 0,3

Таблица 2.1 (окончание)

Наименование характеристики	Значение
Габаритные размеры контроллера, мм	156x107x39
Время непрерывной работы контроллера	круглосуточно
Средняя наработка контроллера на отказ в дежурном режиме работы, ч	не менее 80000
Вероятность безотказной работы	0,98758
Средний срок службы контроллера, лет	10
Время технической готовности контроллера к работе, с	не более 30
Индустриальные радиопомехи, создаваемые контроллером по ГОСТ Р 51318.22 (СИСПР22—2006) пп. 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 3

* 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;

– 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 других конструкциях охраняемого помещения в местах, защищённых от воздействия атмосферных осадков и механических повреждений;

– закрепляется контроллер на стене в удобном месте. Если контроллер устанавливается в неохраняемом помещении, рекомендуется устанавливать его на высоте не менее 2,2 м от пола;

– монтаж контроллера производится в соответствии с РД.78.145-92 "Правила производства и приёмки работ. Установки охранной, пожарной и охранно-пожарной сигнализации";

4.4 Подключение контроллера

4.4.1 Схема внешних подключений приведена в приложении Б.

4.4.2 Подключение линий интерфейса RS-485.

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

а) контакты "A" и "B" подключить соответственно к линиям A и B интерфейса RS-485;

б) подключить цепь "0B" 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".

4.4.3 Включение контроллера.

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

− при напряжении ниже 10 В работа контроллера не гарантируется (контроллер прекращает функционировать, однако, из строя не выходит);

− при превышении напряжения питания уровня 26 В 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 5.1 и 5.2 соответственно.

Таблица 5.1 – Светодиод «Работа»

Состояние контроллера	Содержание извещения
Рабочий режим	Индикатор включен

Таблица 5.2 – 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

Подключение контроллера к компьютеру производится с использованием:

– интерфейса RS-232-D по COM-порту со следующими настройками: 115200, 8, N, 1;

– или по сети Ethernet программами «HyperTerminal», «PuTTY» или их аналогами.

ВНИМАНИЕ!!! Логины в Linux-консоли и вебконфигураторе разные.

Логин пользователя по умолчанию: «**root**».

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

По данному интерфейсу предоставляется доступ к Linux-консоли.

5.3 Настройка контроллера через браузер

Настройка контроллера через браузер производится записью в адресной строке браузера командой вида: http://ip_device/bolid_web_cfg/, где «ip_device» – текущий сетевой адрес контроллера (по умолчанию 192.168.0.50).

После выполнения этой команды (при прямом подключении с настройками IP-адреса к контроллеру ПК IP-адрес: 192.168.0.1, маска подсети: 255.255.255.0) появляется окно ввода пароля, представленное на Рис.1.

Страница доступа к сетевым настройкам изменилась!!!

Логин при входе через браузер: **«admin»** (в предыдущей версии был **«root»**), пароль пользователя по умолчанию: «**p@ssw0rd1234**».

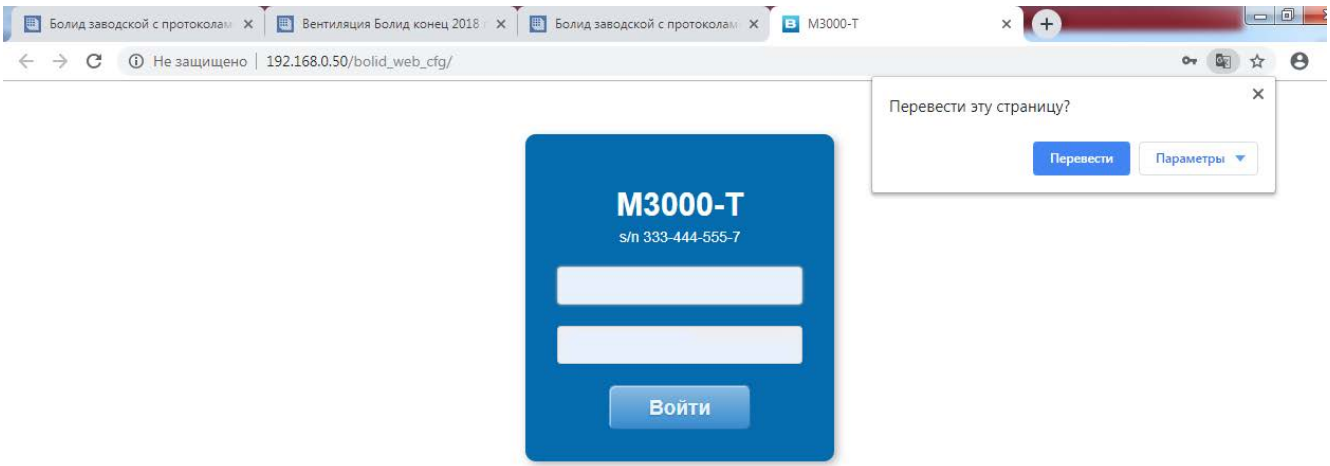


Рисунок 1. Окно ввода пароля

5.3.1 Страница «Пользователи»

Общий вид страницы представлен на рисунке 2. Страница предназначена для добавления и удаления пользователей.

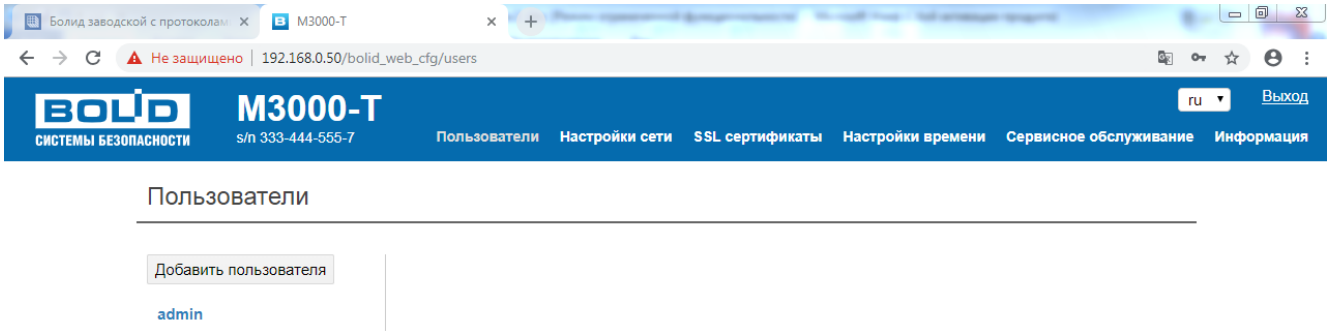


Рисунок 2. Страница «Пользователи»

5.3.2 Страница «Настройки сети»

Общий вид страницы представлен на рисунке 3. Страница разделена на 4 вкладки: «Общие», «Ethernet», «USB-modem» и «WiFi». Параметры вкладки «Общие» описаны в таблице 6, параметры вкладки «Ethernet» - в таблице 7, параметры вкладки WI-FI - в таблице 8.

Общий вид страниц представлен на рисунках 3, 4, 5 и 6 соответственно.

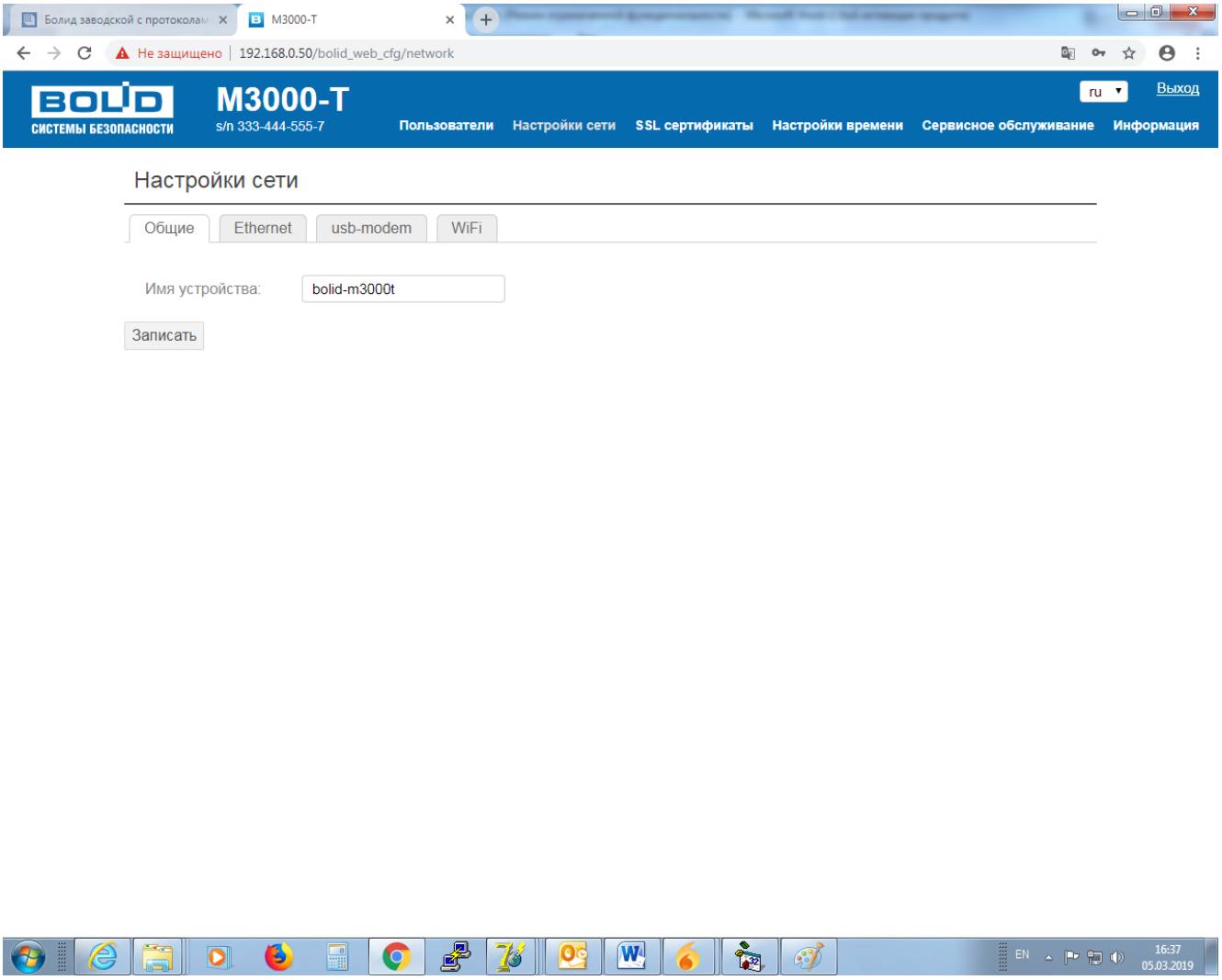


Рисунок 3. Настройка сети

Таблица 5.1. Описание параметров настройки сети, вкладка «Общие»

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

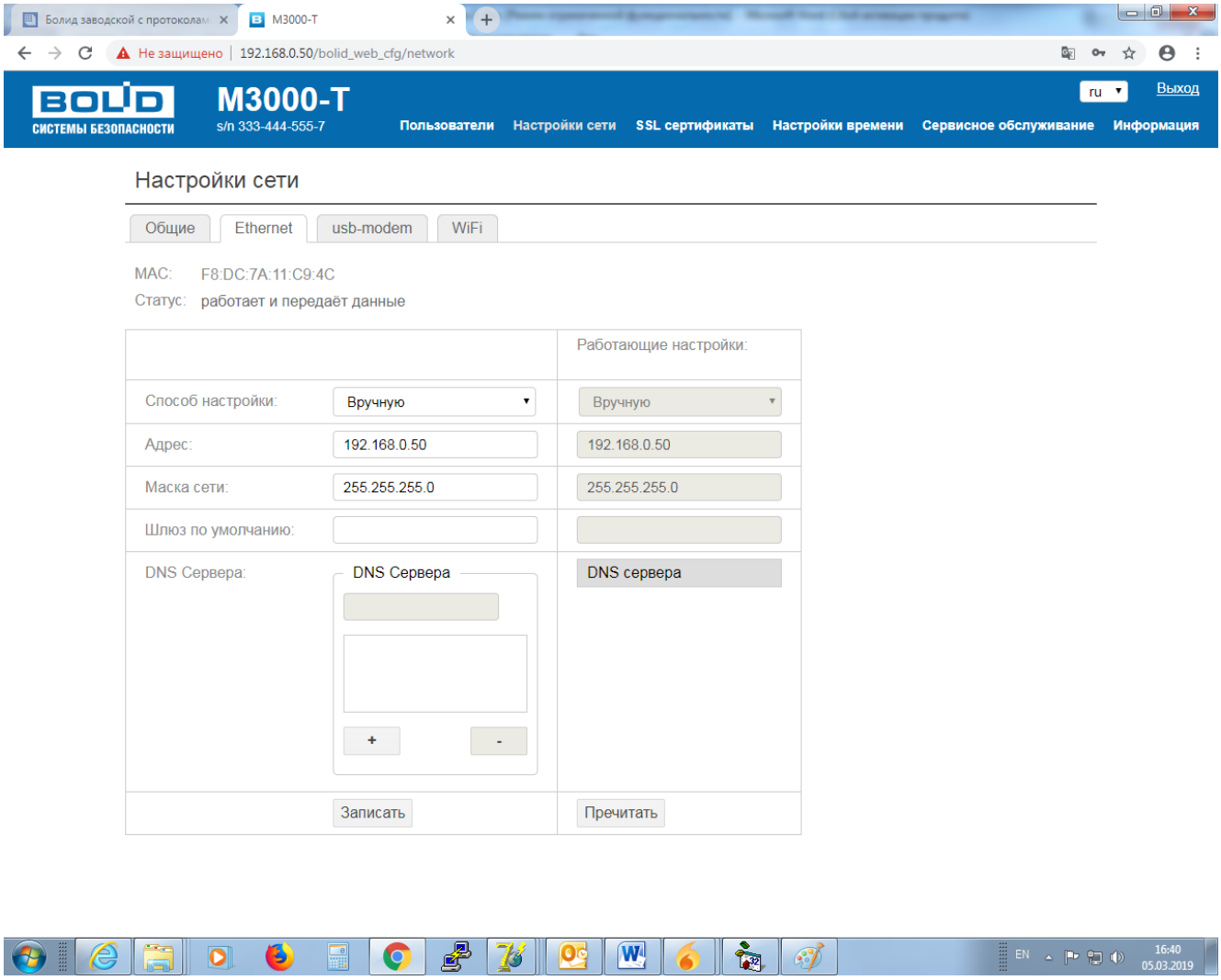


Рисунок 4. Настройка сети, вкладка «Ethernet»

Таблица 5.2. 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	Значение не редактируется.
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 «Ethetnet» 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».

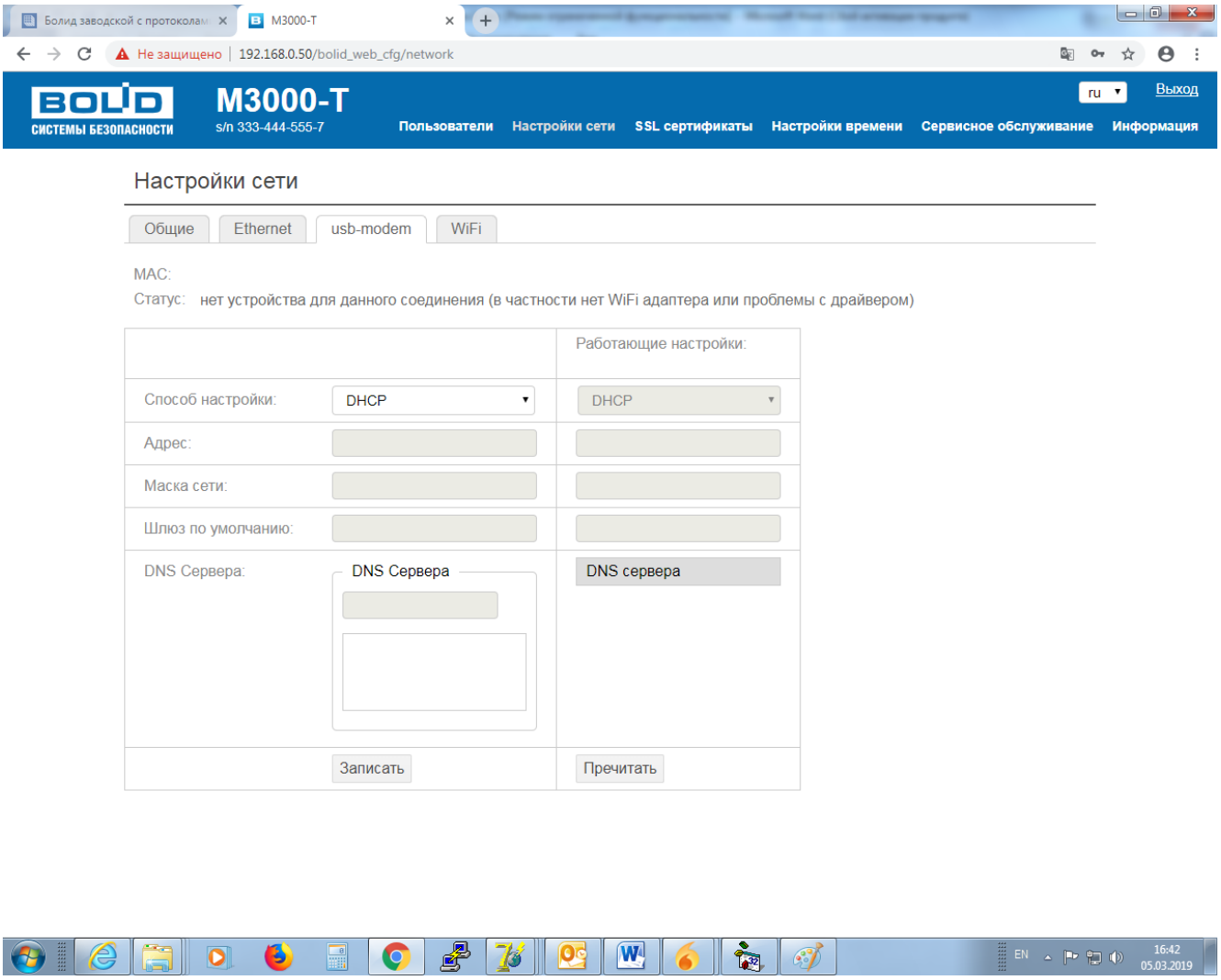


Рисунок 5. Настройка сети, вкладка «usb-modem»

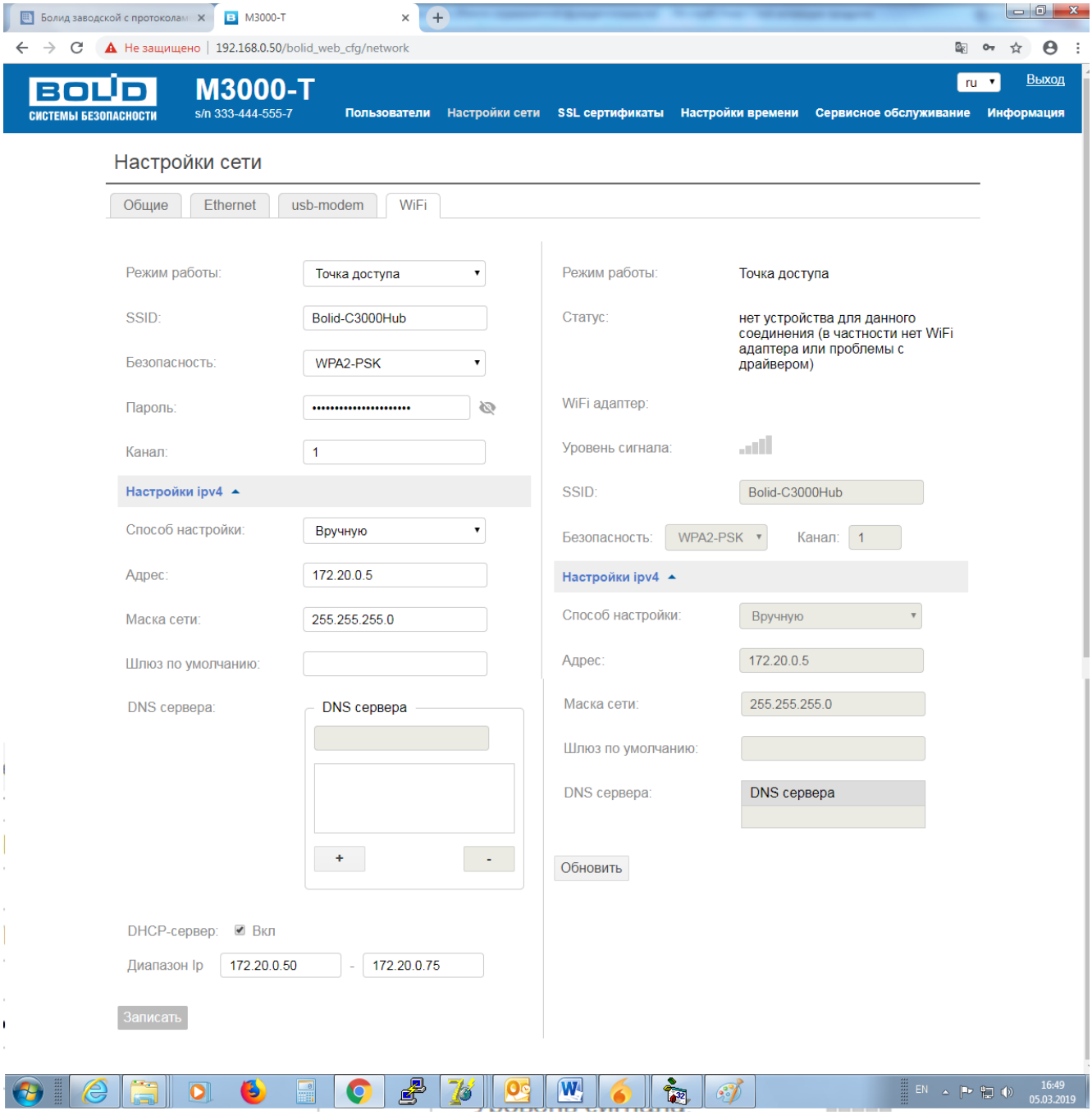


Рисунок 6. Настройка сети, вкладка "WI-FI"

Таблица 5.3. Описание параметров настройки сети, вкладка «WI-FI»

Вкладка WiFi		
Название параметра	**Значение по умолчанию**	**Описание**
Режим работы	Точка доступа	Режим работы Wi-Fi Возможные значения: • Выключено • Клиент • Точка доступа
SSID	Bolid-C3000Hub	Идентификатор сети (на рисунке пароль скрыт)
Безопасность	WPA2-PSK	Тип безопасности беспроводной сети

Пароль	С3000hub-серийный номер прибора (буквы латинские)	Пароль для подключения к беспроводной сети
Канал	1	Номер канала WiFi
Настройки ipv4		
Способ настройки	Вручную	Тип задания IP-адреса, маски сети, шлюза Возможные значения: • DHCP • Вручную
Адрес	172.20.0.50	Сетевые настройки Wi-Fi (доступны для редактирования в случае если режим работы указан «Вручную».
Маска	255.255.255.0	
Шлюз	-	
DHCP-сервер	Вкл Диапазон С 172.20.0.50 Диапазон ПО 172.20.0.75	
На вкладке «WiFi» 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».		

5.3.3 Страница «SSL-сертификаты»

Общий вид страницы представлен на рисунке 7.

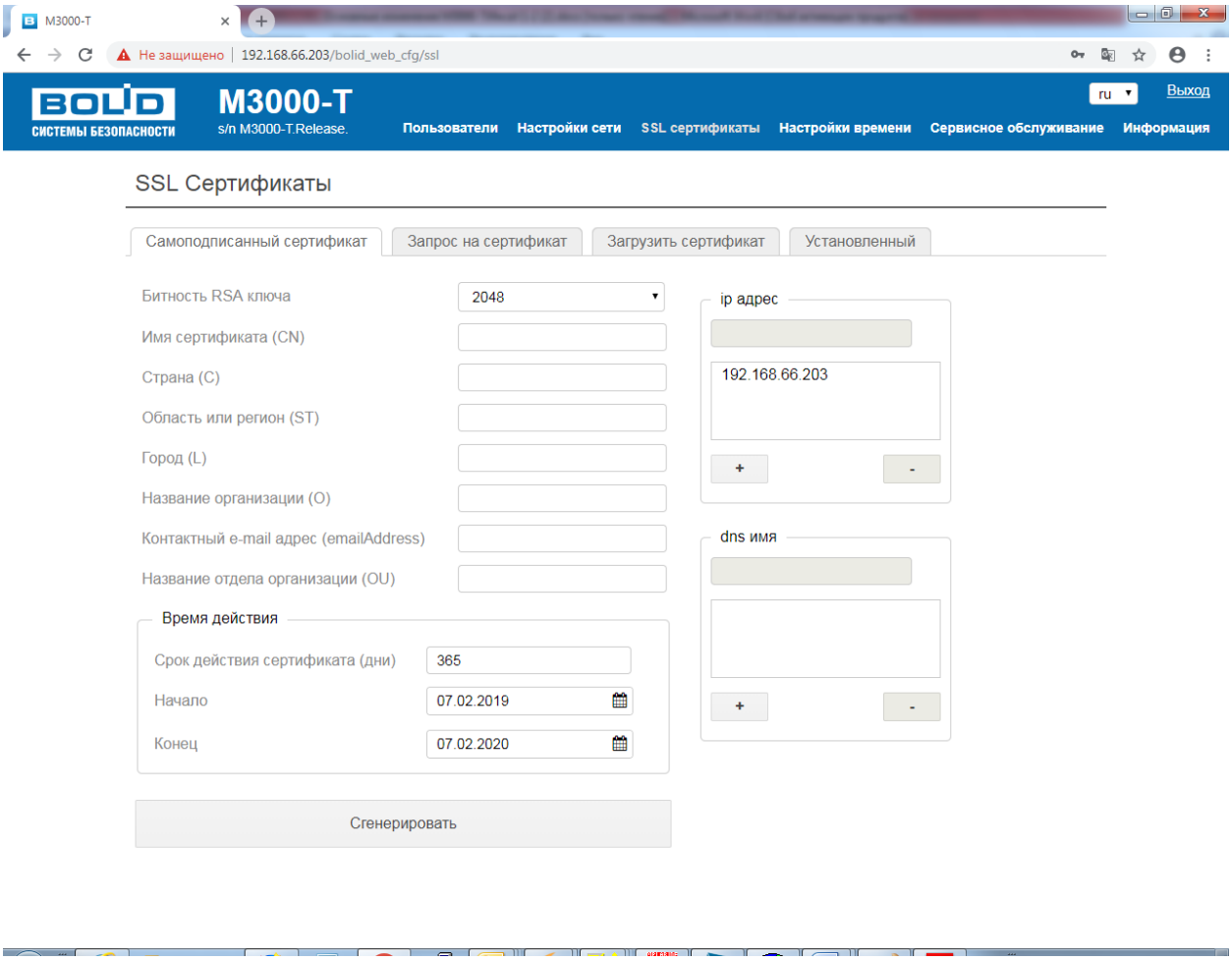


Рисунок 7. Страница SSL сертификаты

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 поверх TLS/SSL). Для работы требуется настройка PKI (установка сертификатов), а также включение безопасного соединения на вкладке «Сервисное обслуживание/Прочие настройки».
Для установки сертификата SSL реализовано 2 схемы:
1. Генерация цепочки самоподписанных SSL сертификатов. Подходит для одиночных устройств или когда нет инфраструктуры PKI на предприятии.
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.
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 FTP. 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.
5.3.2.1 Генерация самоподписного сертификата.
Генерация сертификата осуществляется на вкладке «Самоподписанный сертификат»
Чтобы сгенерировать самоподписанный сертификат, необходимо заполнить параметры сертификата в соответствие с таблицей 4.
Обязательные параметры для заполнения:

- Битность ключа шифрования (доступные значения: 1024, 2048, 4096);
- IP-адрес или DNS-имя (может быть несколько);
- Срок действия сертификата в днях.

После заполнения этих параметров (См. Рисунок 8.1) достаточно нажать кнопку **«Сгенерировать»**

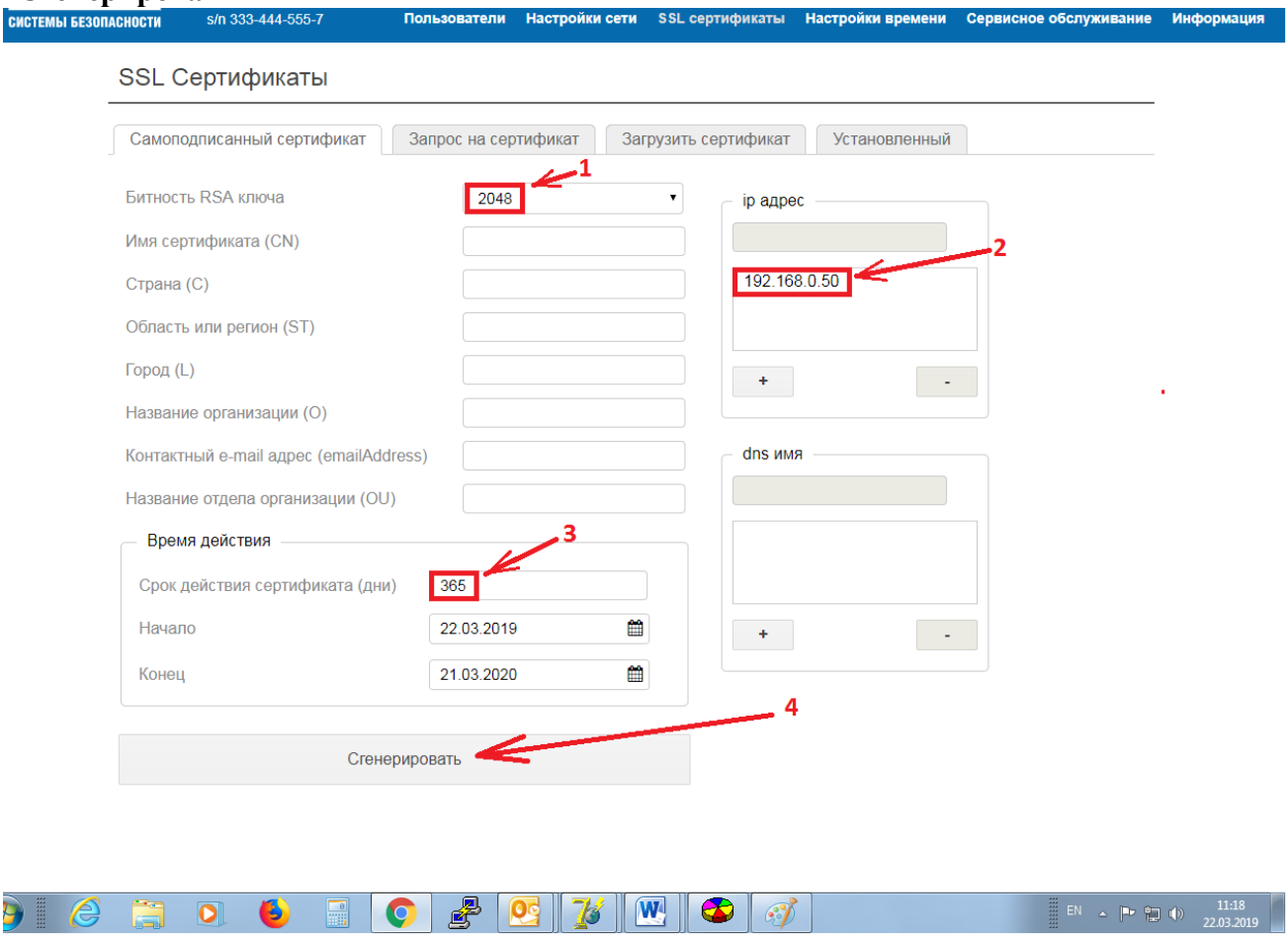


Рисунок 8.1. Окно генерации самоподписанного сертификата с минимальным набором заполненных полей.

и на экран будет выведено сообщение о генерации сертификата (см. Рисунок 8.2)

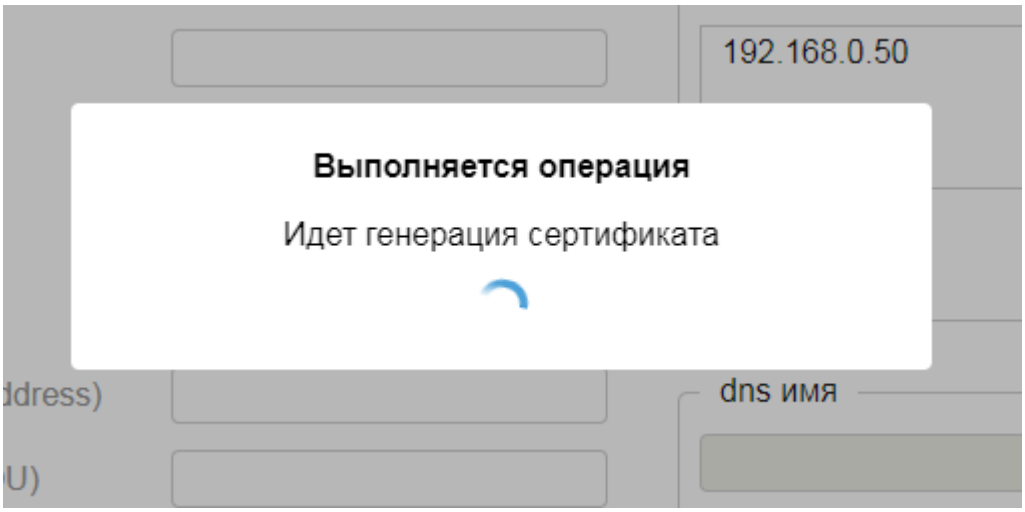


Рисунок 8.2. Сообщение о генерации сертификата.

после генерации сертификат применяется автоматически. То есть, происходит установка сертификата в веб-сервер и на протокол JSON RPC. Дождитесь появления сообщения о том, что сертификат применён (см. Рисунок 8.3).

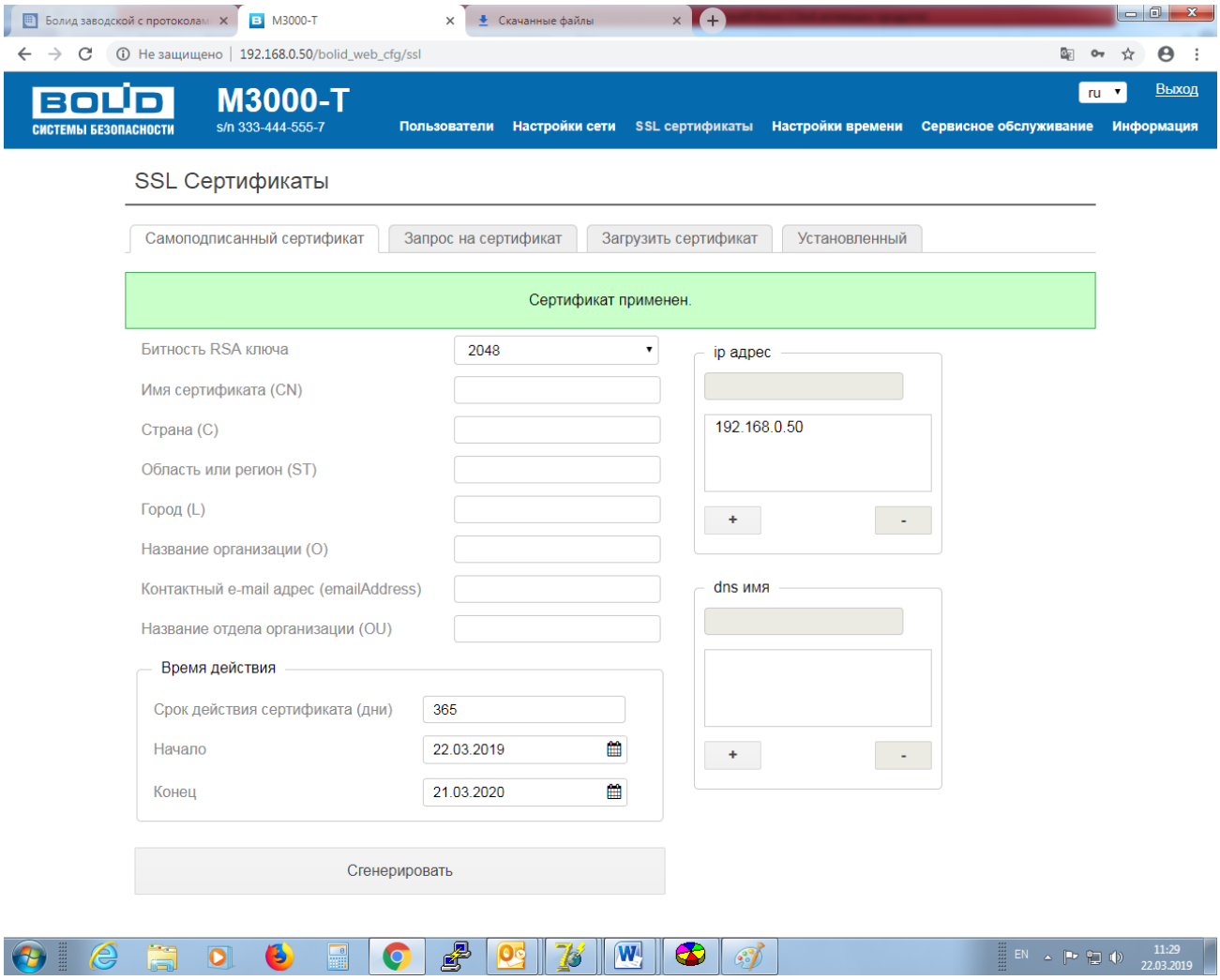


Рисунок 8.3. Сообщение о применении сертификата.

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.

Импорт сертификатов в ОС Windows.

В операционной системе семейства Windows предусмотрено глобальное хранилище сертификатов. Это хранилище используют браузеры Chrome, Opera, MS Edge, MS InternetExplorer. *Добавление сертификата для браузера Mozilla Firefox, описано отдельно.*

Для импорта сертификатов необходимо:

1. Перейти в веб-интерфейсе на страницу «Установленный» Рис. 9 и нажать кнопку «Скачать»:

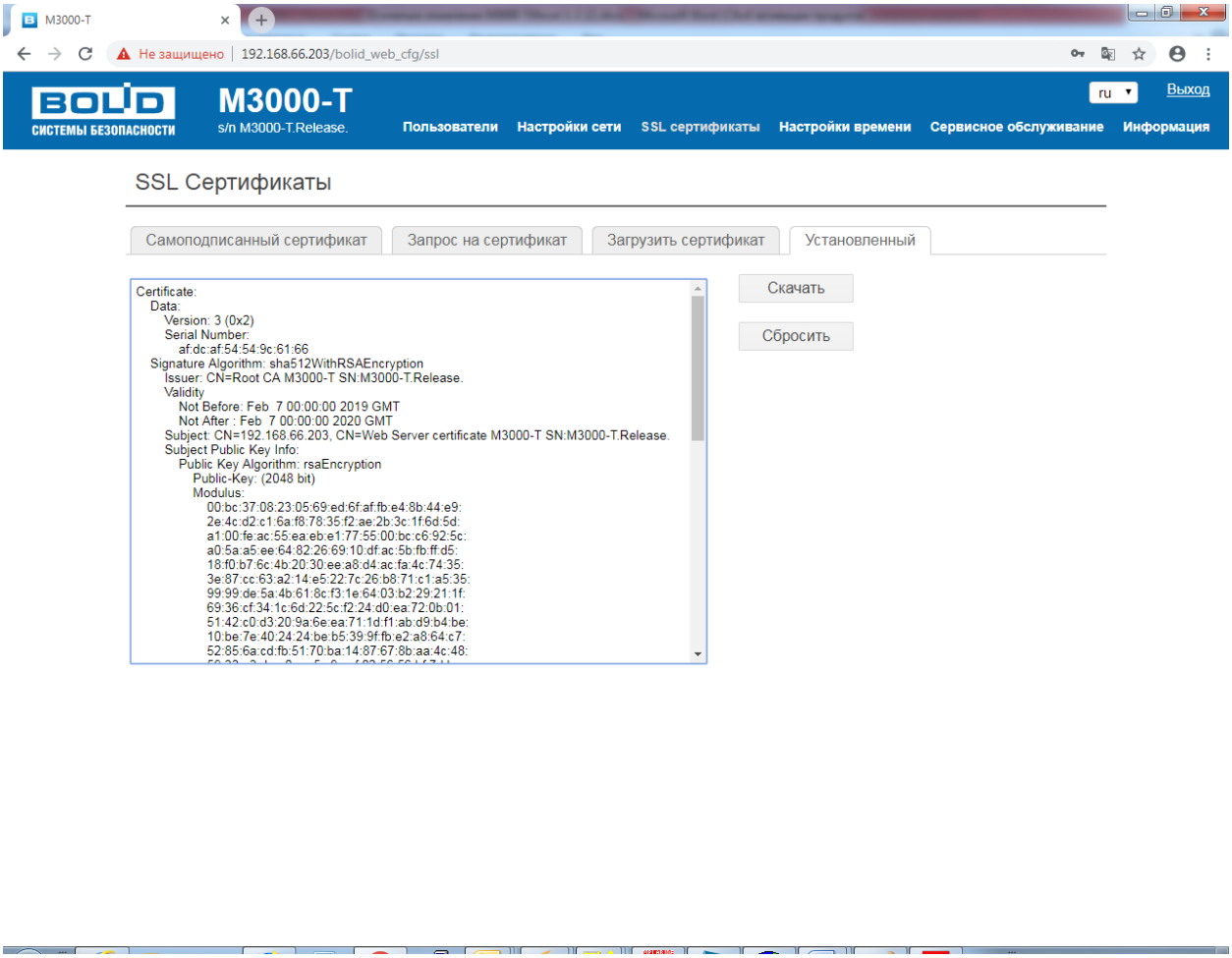


Рисунок 9. Скачивание файла цепочки сертификатов

2. Перейти в папку загрузок Рисунок 10 и кликнуть два раз левой кнопкой мыши по скачанному файлу.

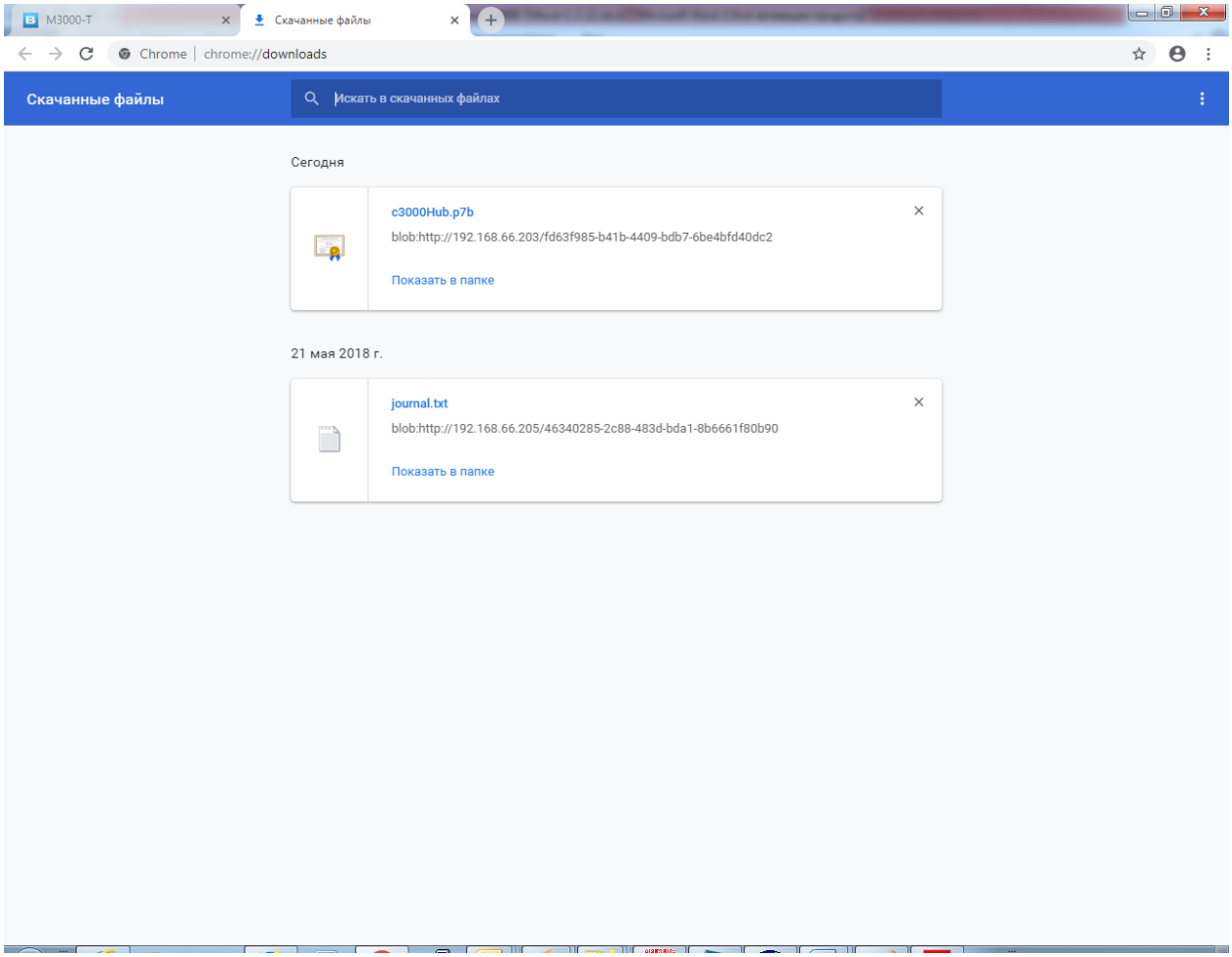


Рисунок 10. Папка загрузок

Откроется окно со списком содержащихся в нём сертификатов Рис. 11.:

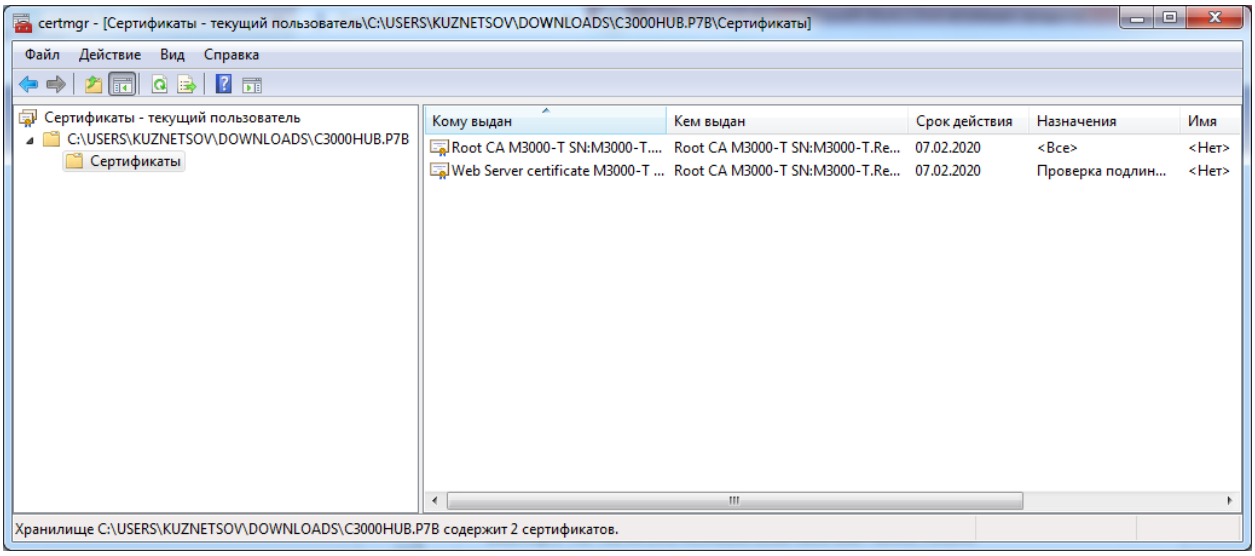


Рисунок 11. Список сертификатов, хранящихся в файле цепочки сертификатов

3. В списке сертификатов выбрать сертификат, начинающийся с символов «Root CA…» и щелкнуть по нему два раза. Откроется окно (Рис. 12), в котором нужно нажать кнопку «Установить сертификат»:

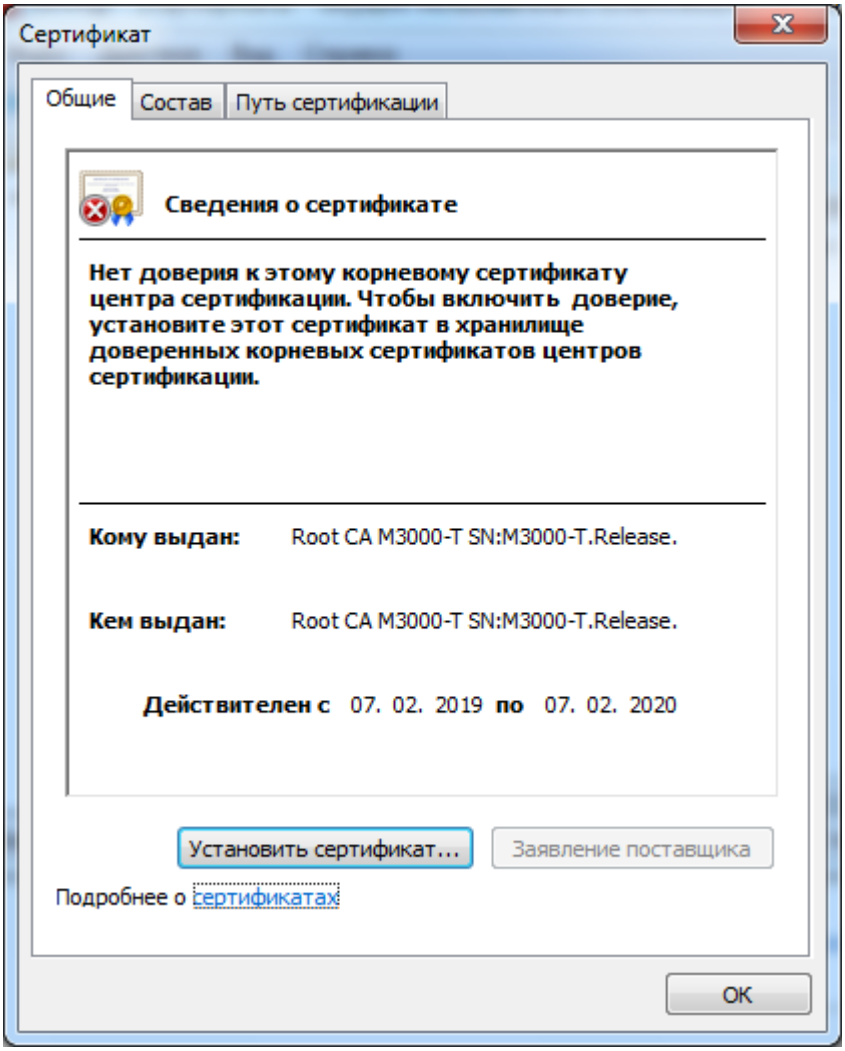
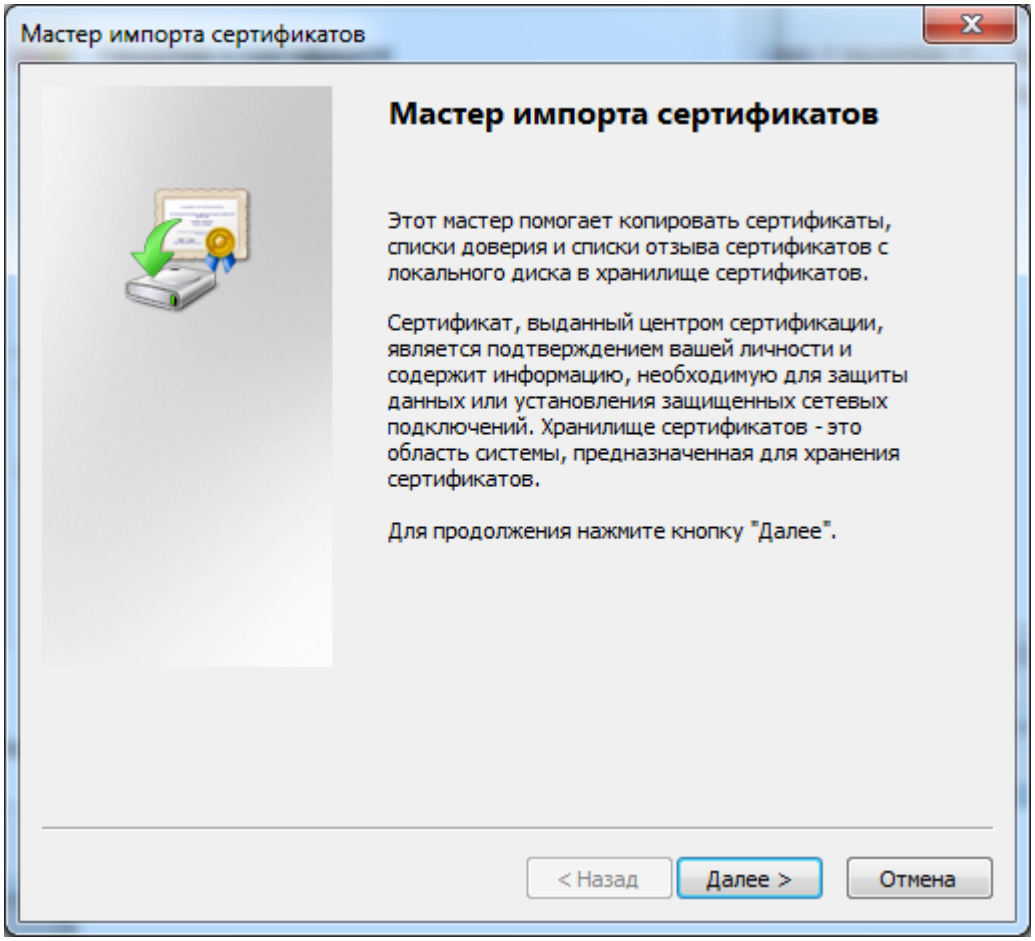


Рисунок 12. Окно установки сертификата

В появившемся «Мастере импорта сертификатов» перейти на вторую страницу, нажав кнопку «Далее». Выбрать пункт «Поместить все сертификаты в выбранное хранилище» и нажать кнопку «Обзор» (Рис. 13).



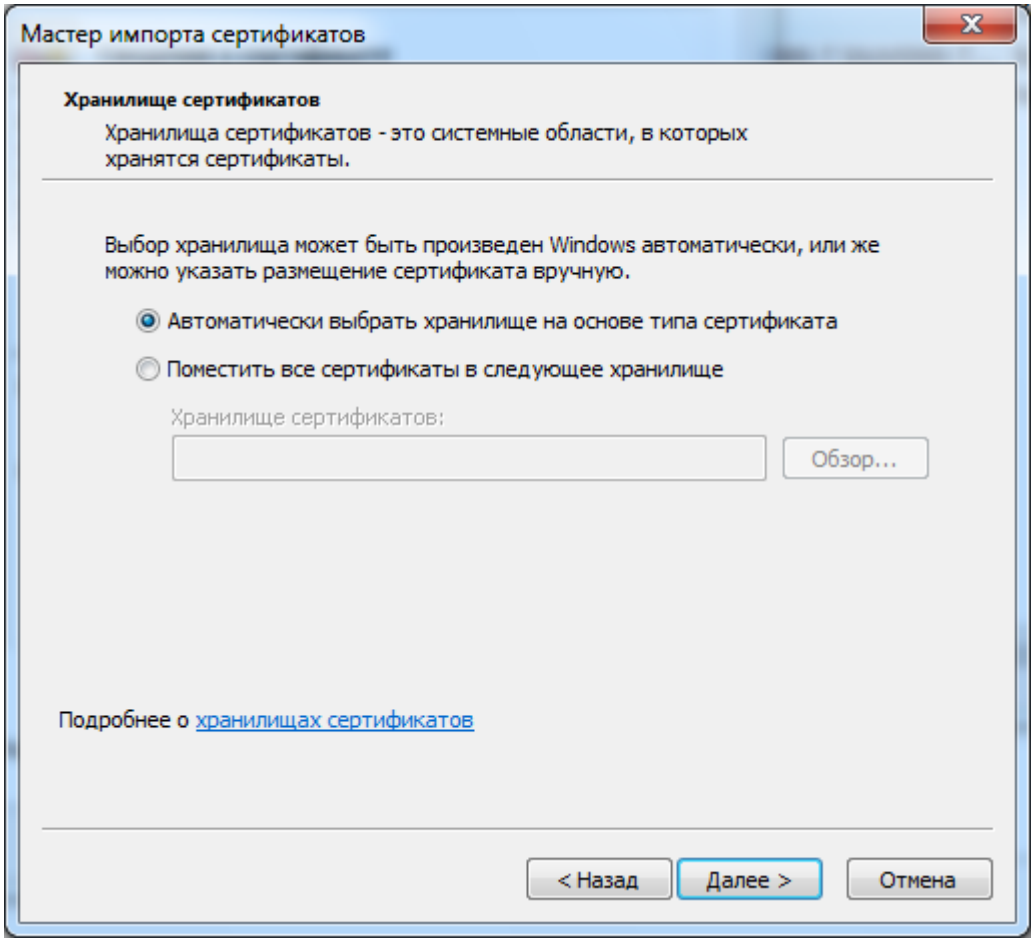


Рисунок 13. Выбор хранилища сертификатов

В диалоговом окне (Рис. 14) выбрать папку «Доверенные корневые центры сертификации» и нажать «Далее».

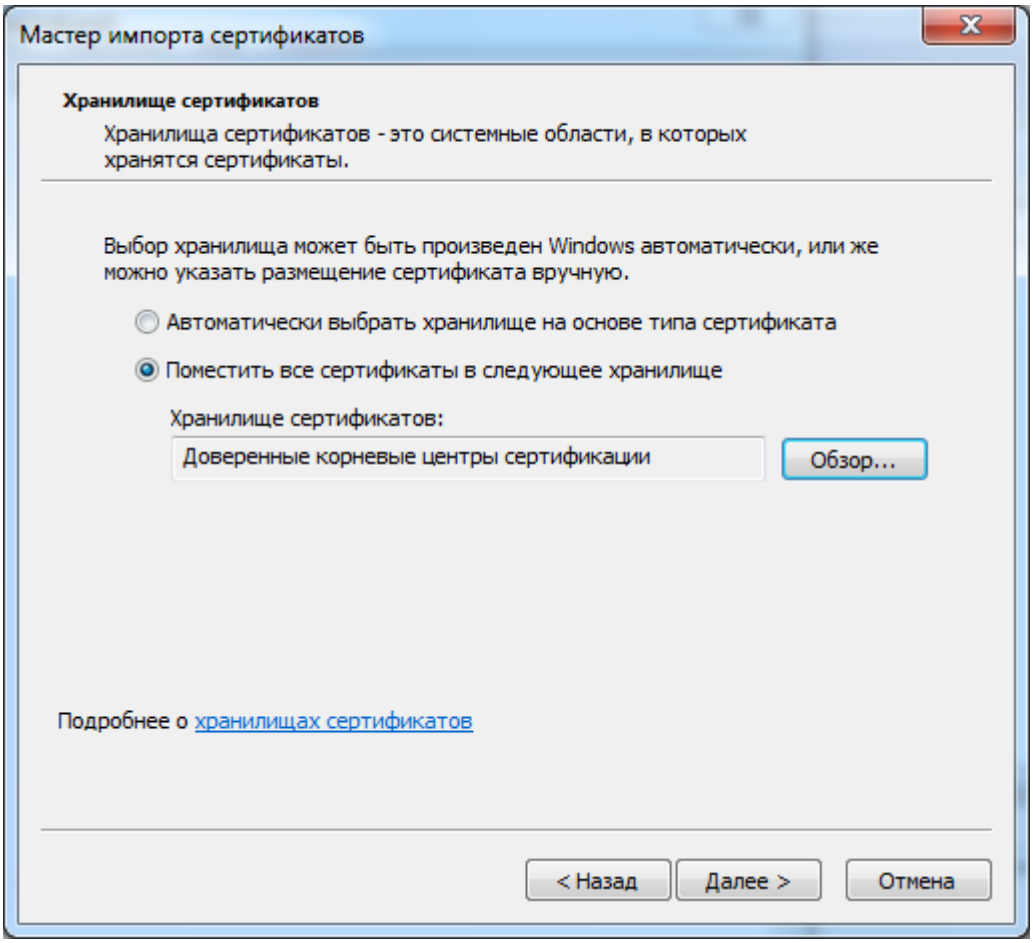


Рисунок 14. Выбор хранилища сертификатов

После выбора хранилища завершить импорт, нажав кнопку «Далее», «Готово» В появившемся предупреждении безопасности, нажать «Да», после чего должно появиться завершающее окно Рис. 15 с подтверждением выполнения импорта.

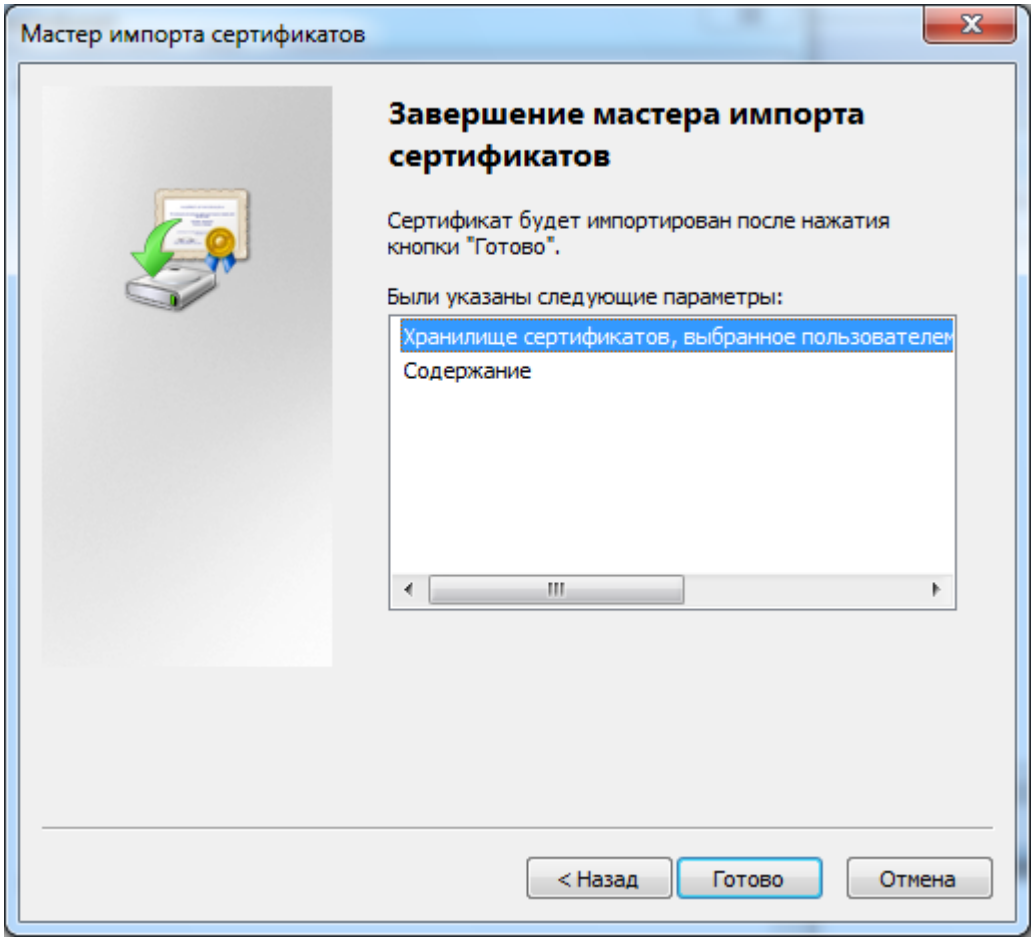


Рисунок 15. Завершение импорта

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-интерфейс.

Для добавления сертификата нужно запустить браузер и в основном меню (Рис. 16) выбрать пункт «Настройки»:

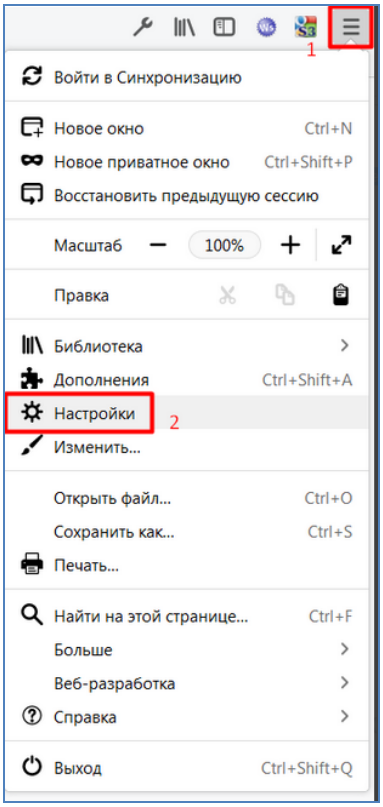


Рисунок 16. Меню настроек Mozilla Firefox

В настройках (Рисунок 17) выбрать раздел «**Приватность и защита**», подраздел «**Защита - Сертификаты**», нажать кнопку «**Просмотр сертификатов**»:

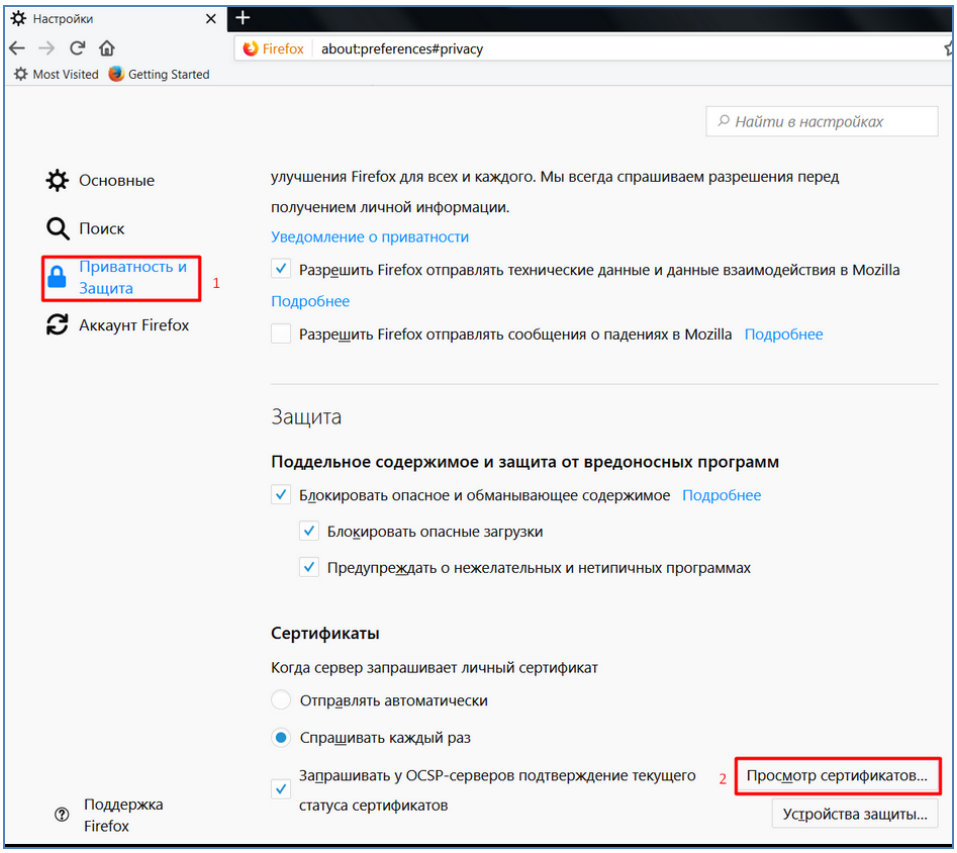


Рисунок 17. Окно настроек "**Приватность и защита**" Mozilla Firefox

Откроется окно «Управление сертификатами» (Рис. 18):

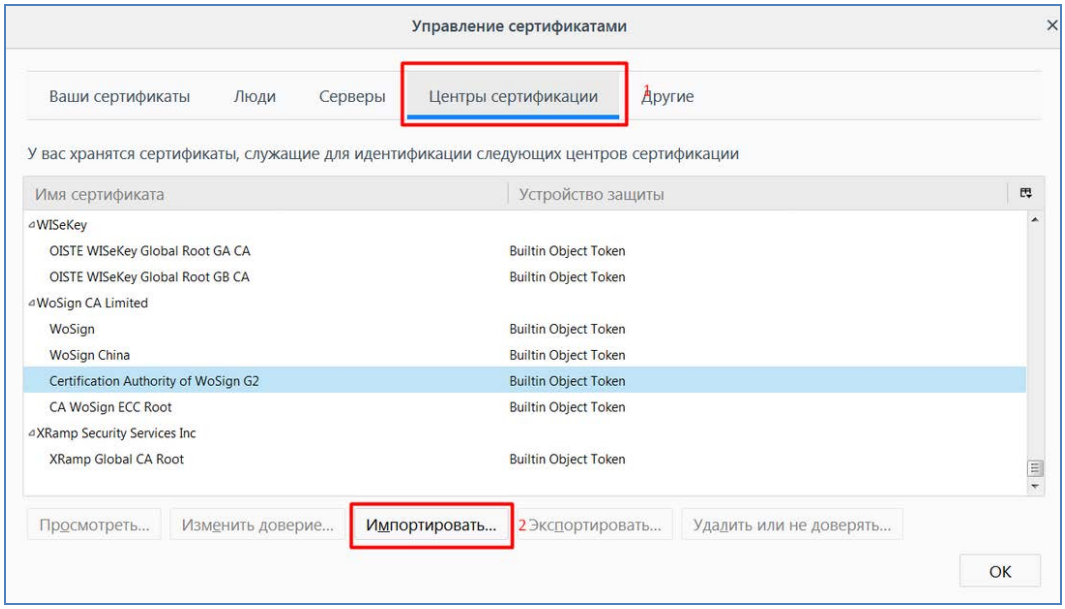


Рисунок 18. Импорт сертификата в Mozilla Firefox

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

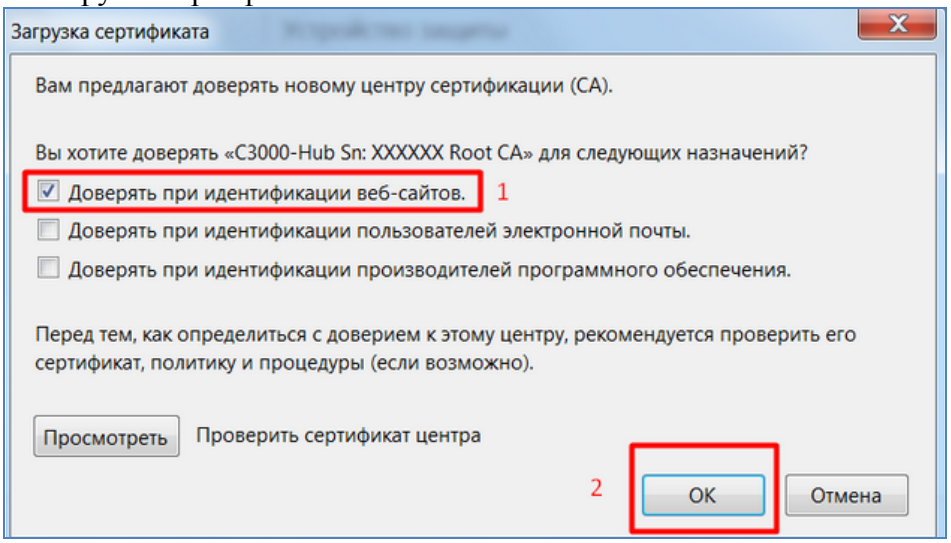


Рисунок 19. Завершение импорта сертификата в Mozilla Firefox

Отметить пункт «Доверять при идентификации веб-сайтов». Нажать кнопку «ОК». Убедиться, что сертификат появился в списке:

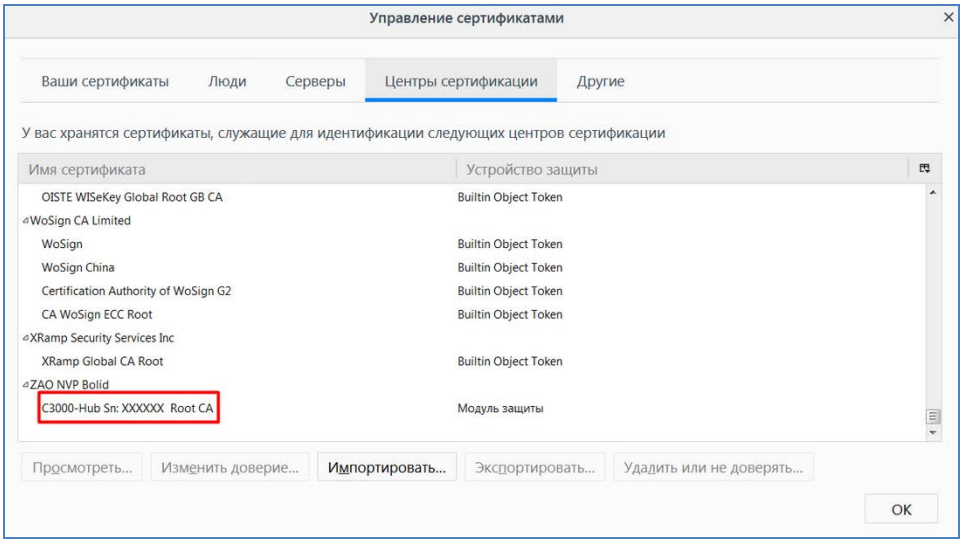


Рисунок 20. Окно отображения сертификатов в Mozilla Firefox

Импорт сертификатов ОС Linux

Данная инструкция подходит для веб-браузеров Chromium и Opera.

Необходимо установить пакет libnss3-tools. Выполнить 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

5.3.3.1 Создание сертификата по запросу на подпись (CSR)

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.

Для создания запроса на сертификат перейдите на вкладку «Запрос на сертификат», заполните параметры в соответствие с таблицей 4, а затем нажать кнопку «Сгенерировать» Рис. 21.

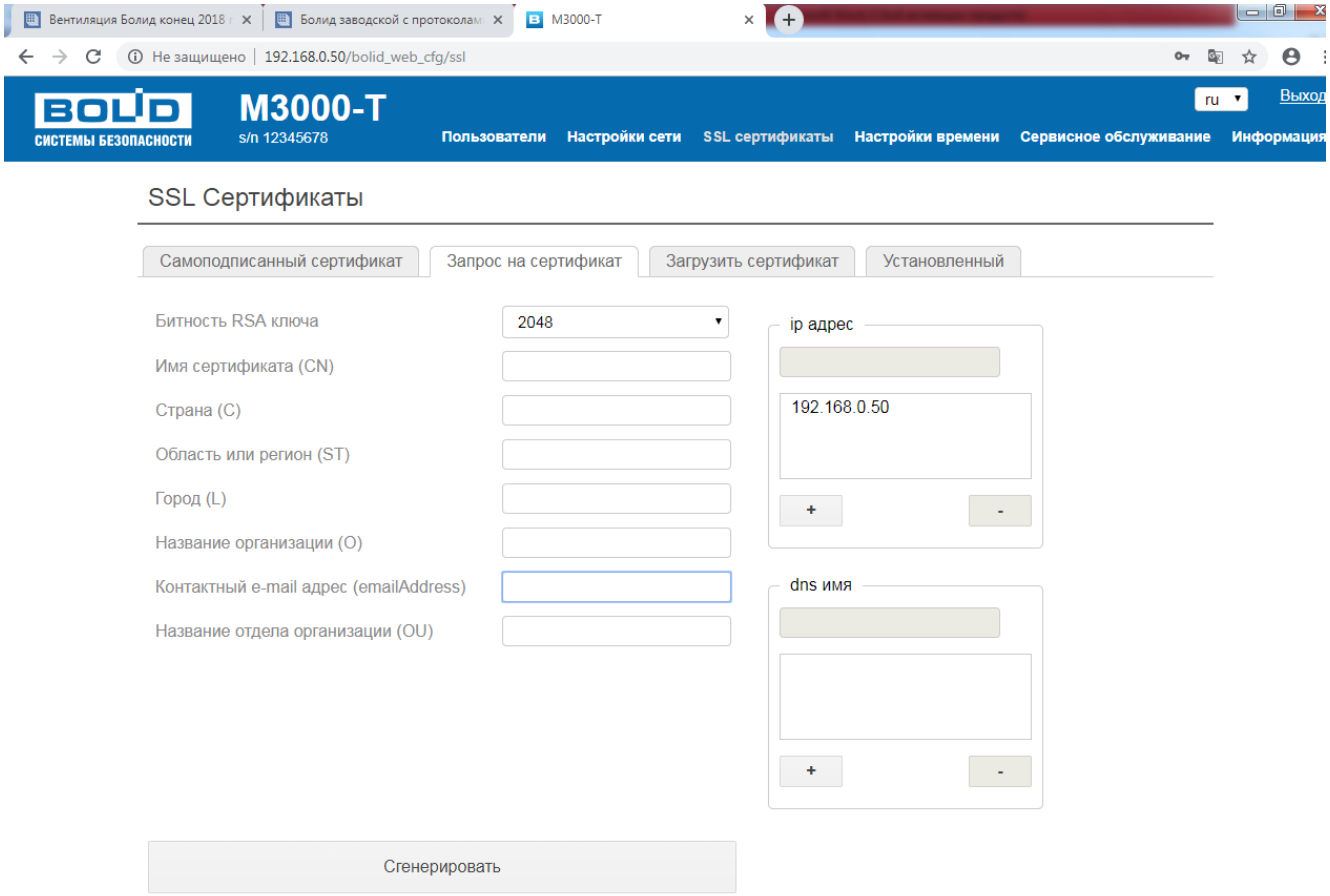


Рисунок 21. Страница создания запроса на сертификат

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 «Выбрать файл», выберите файл на своем компьютере и нажмите кнопку «Загрузить»:

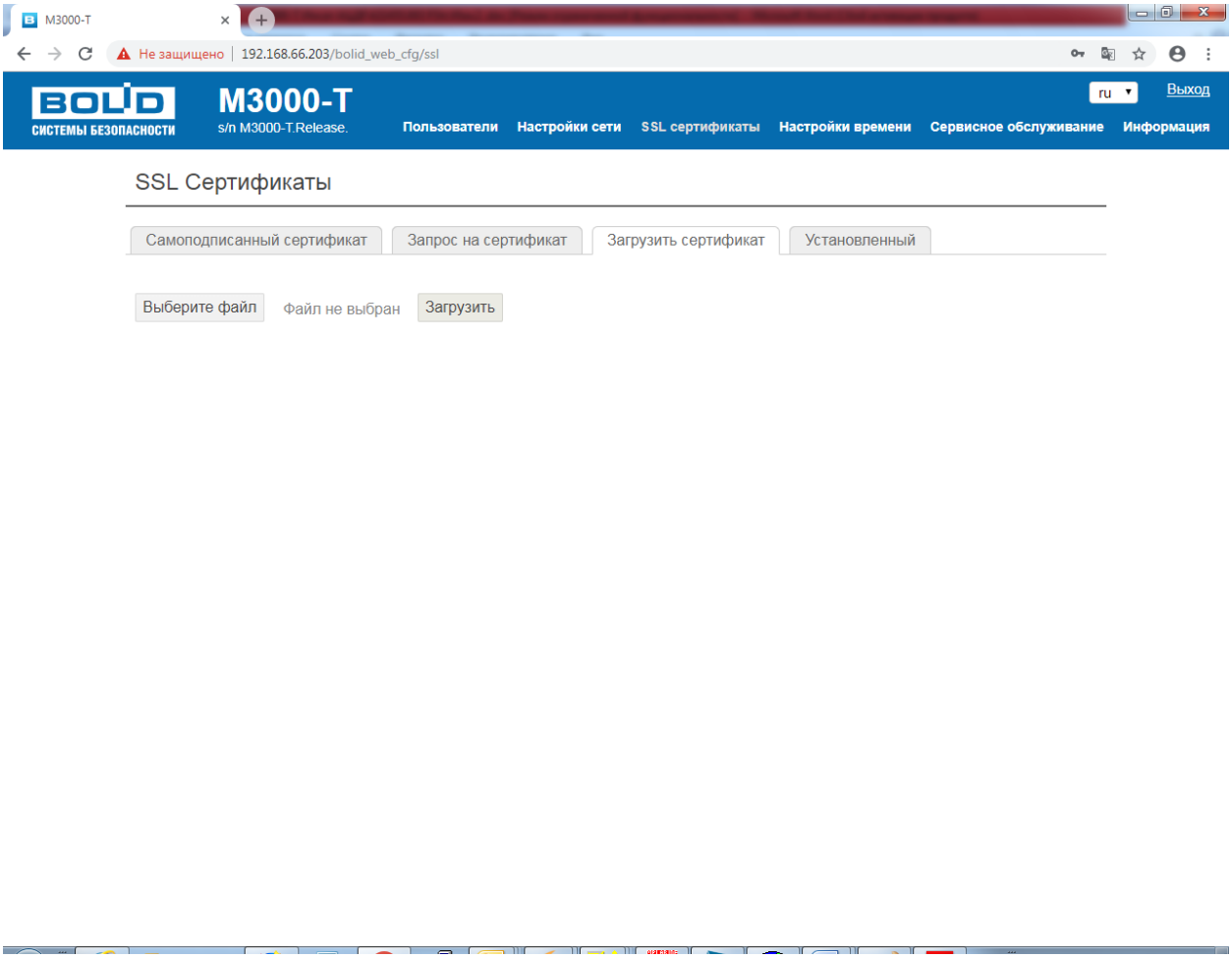


Рисунок 22. Страница загрузки сертификата

Дождитесь сообщения о том, что файл загружен и примените сертификат, нажав кнопку «Применить…». После этого необходимо включить опцию «Доступ по https» в настройках устройства. Изменения вступят в силу после перезагрузки устройства.

5.3.3.2 Просмотр сертификатов

Для просмотра сертификата на приборе перейдите на вкладку «Установленный» и нажмите кнопку «Скачать»:

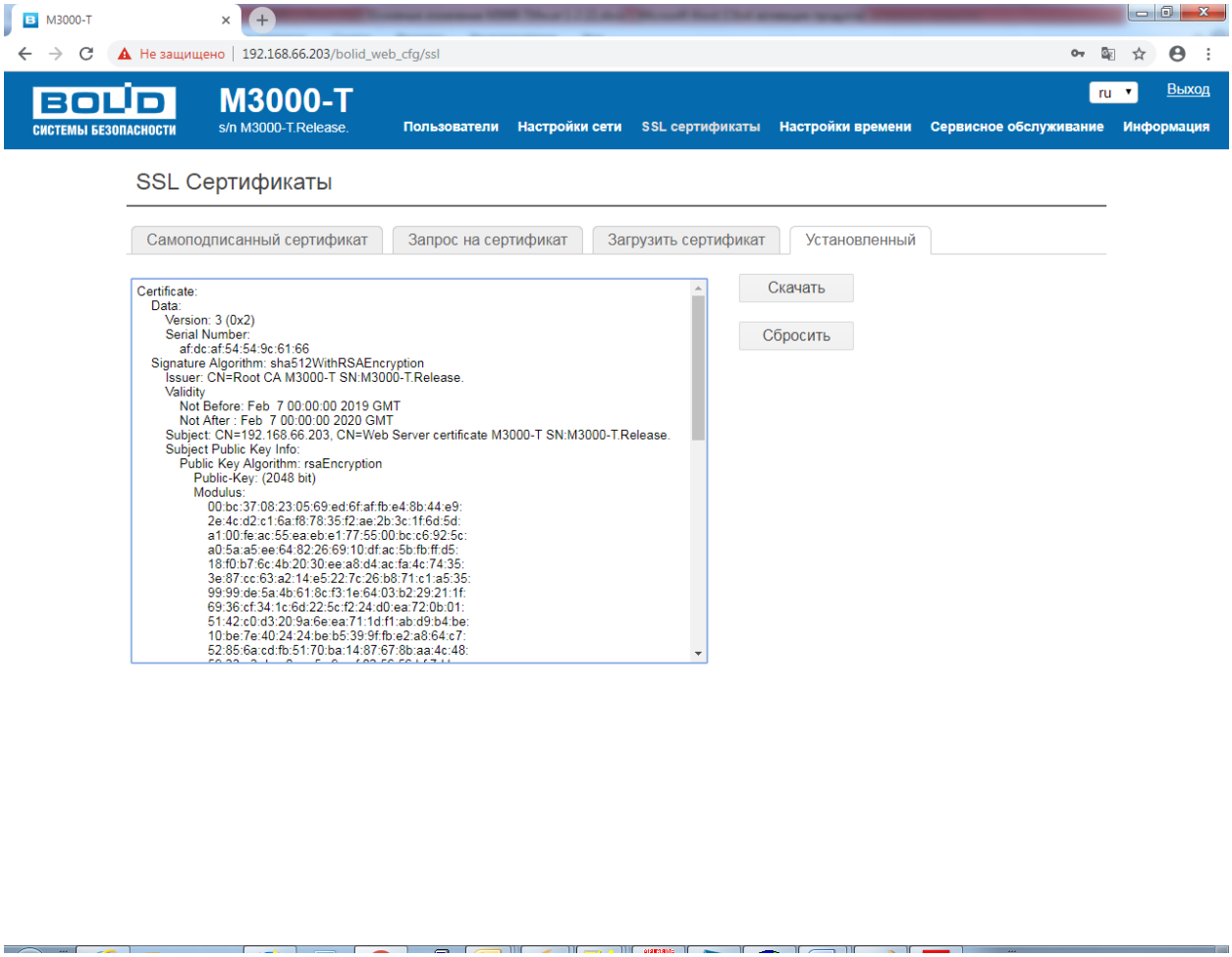


Рисунок 23. Страница просмотра и сброса сертификата

Примечание. Кнопка «Сбросить» удаляет сертификат из устройства.

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

5.3.3.3 Параметры сертификатов

Таблица 4. 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 «C3000-HUB 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 организации - 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	Никак
Дата конца	Дата конца времени действия сертификата	0	Дата конца времени действия сертификата	Дата конца времени действия сертификата	Никак
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)	никак
ip адрес	Любой допустимый ip адрес	Ip адрес из адресной строки браузера (если входили по ip адресу)	никак	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)	никак	Каждый dns добавляет компонент CN субъекта. Компонент поля Subject Alternative Names	Каждый dns добавляет компонент CN субъекта. Компонент поля Subject Alternative Names

5.4 Страница «Настройки времени»

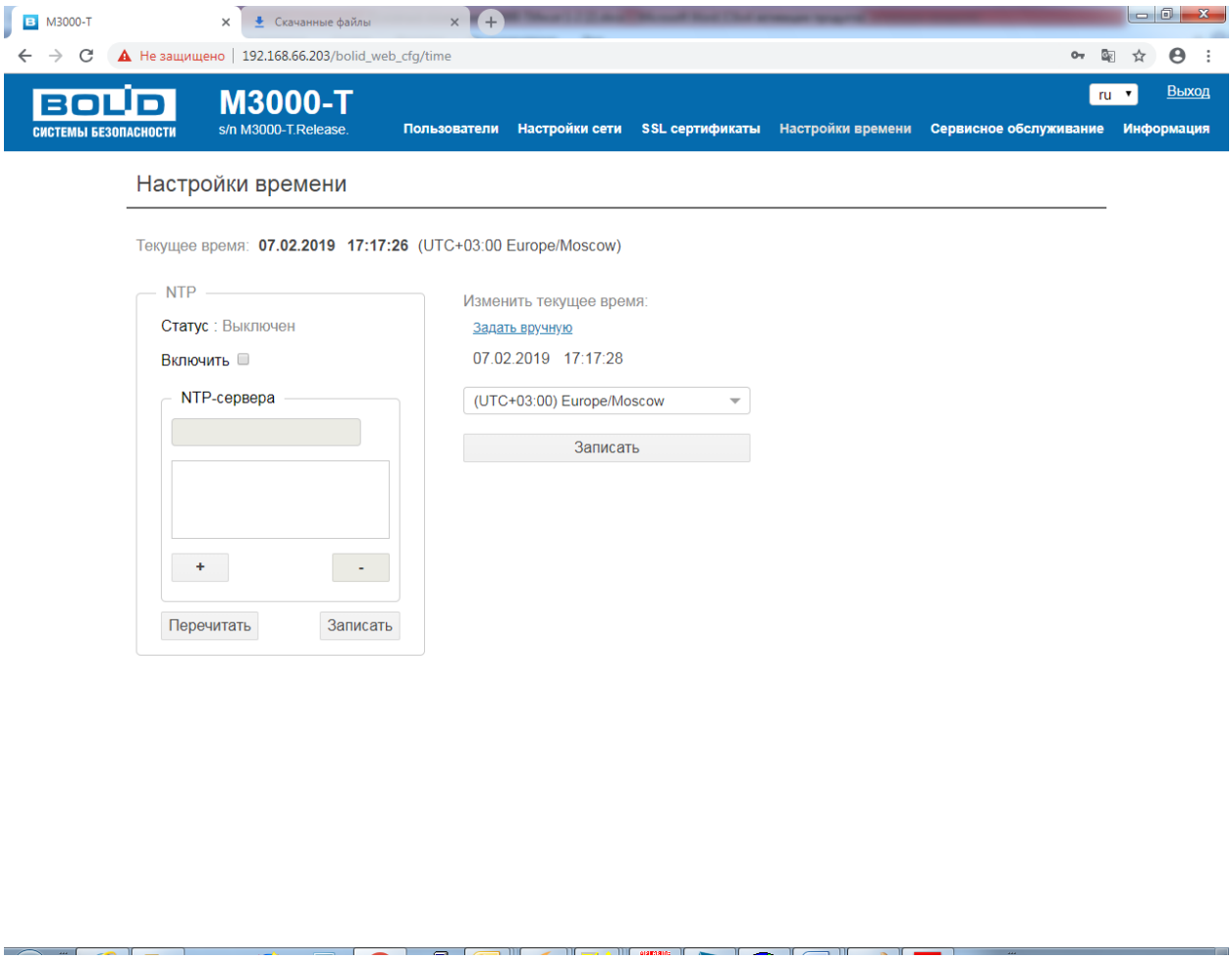


Рисунок 24.1. Страница настройки времени

Страница предназначена для настройки даты и времени устройства.

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

Каждый раз при кликании ЛКМ на надписи «**Текущее время**» она меняется на «Задать вручную» и наоборот (поз.1 Рис.24.2).

В том случае, если клик был произведён по надписи «**Задать вручную**» надпись меняется на «**Текущее время**» и появляется окно с текущей датой, временем и пиктограммой отрывного календаря (поз.2 Рис.24.2). При кликании по этой пиктограмме открывается набор вспомогательных окон для задания даты и времени См. Рис. 24.2, позволяющих установить требуемые параметры, производя «прокрутку» года, месяца, дня, часа и минуты (поз.4 Рис.24.4) или указав конкретную дату на календаре (поз. 3 и поз. 5 Рис.24.5), пользуясь только мышкой.

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

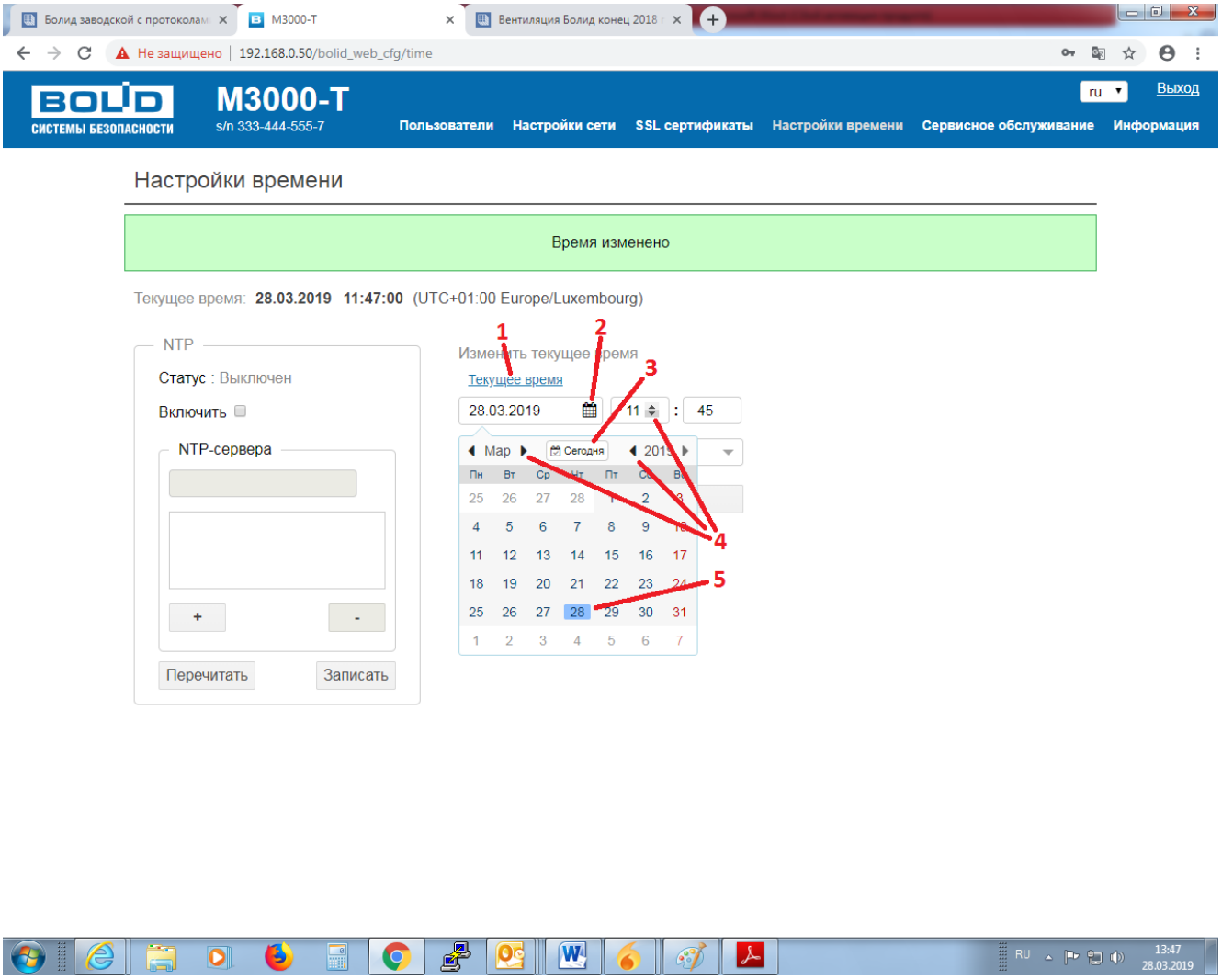


Рисунок 24.2. Страница настройки времени. Задание времени вручную.

В том случае, если клик был произведён по надписи «**Текущее время**» надпись меняется на «**Задать вручную**» и появляется окно с текущей датой и временем компьютера (см. Рис. 24.3). 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 кнопки «**Записать**» в правой нижней части экрана.

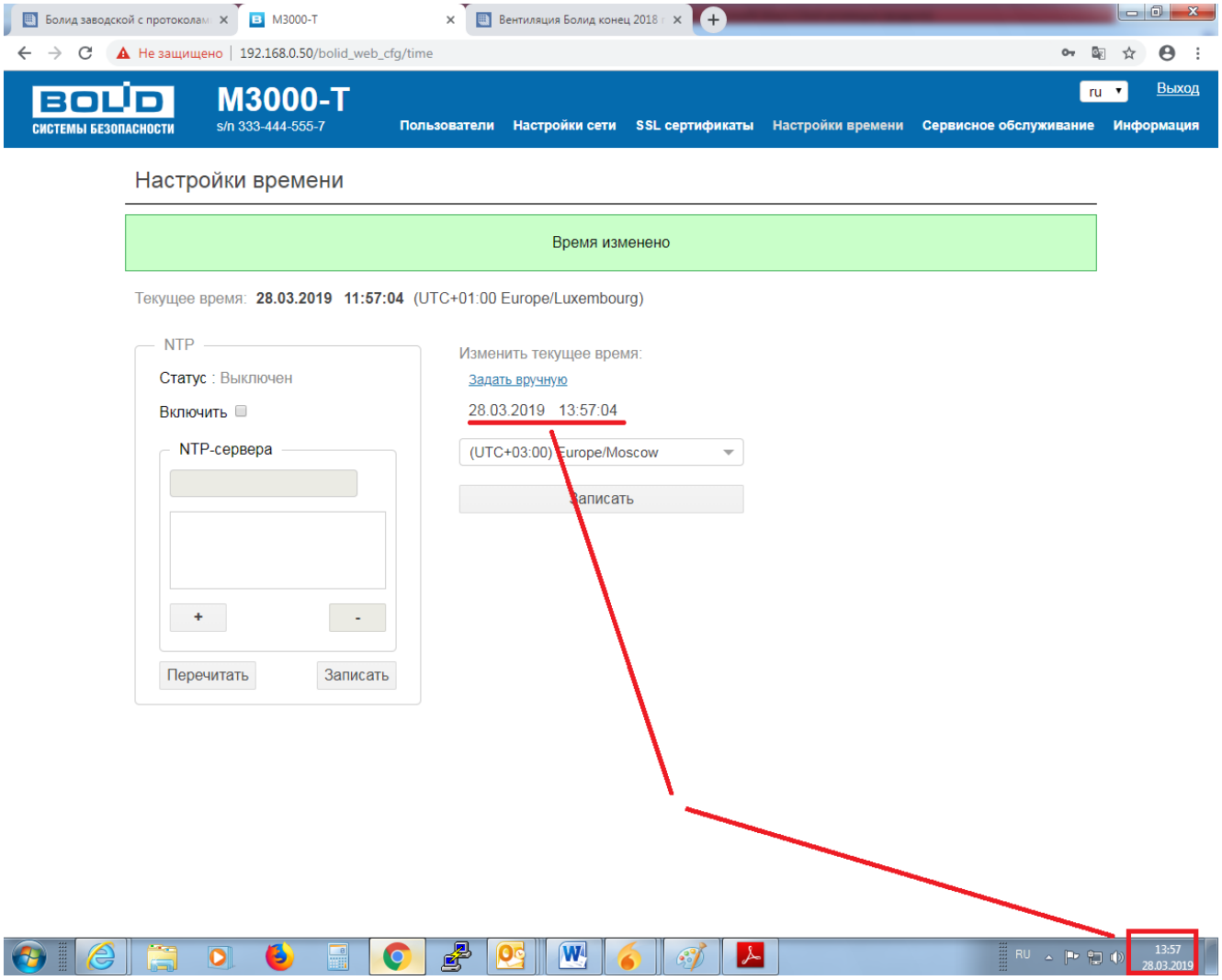


Рисунок 24.3. Страница настройки времени. Синхронизация даты и времени с компьютером.

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 24.4 показан контроллер с активированным NTP протоколом и NTP-сервером, имеющим адрес 192.168.0.1.

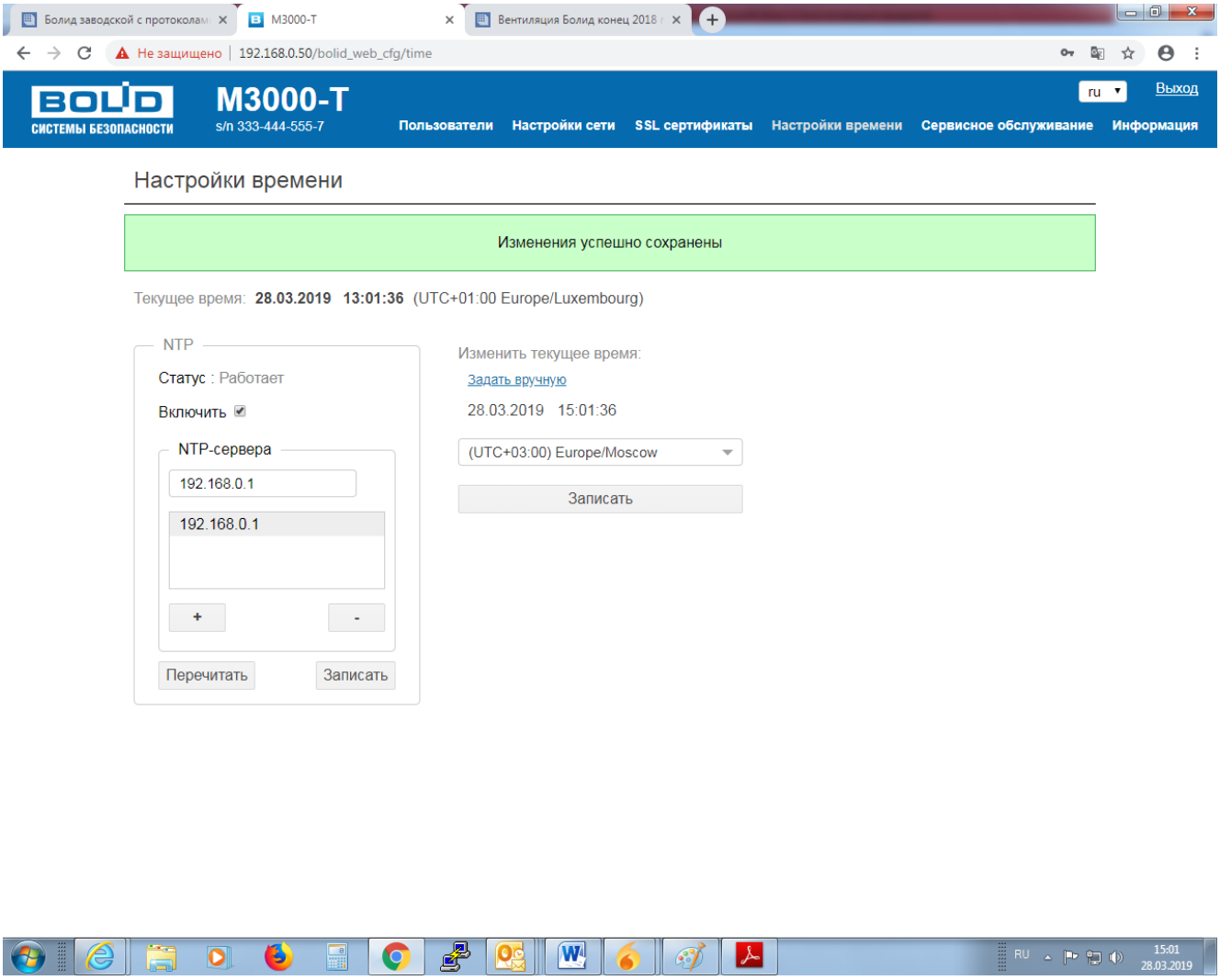


Рисунок 24.4. Страница настройки времени. Настройка NTP.

5.5 Страница «Сервисное обслуживание»

Страница разделена на три вкладки: «Прочие настройки», «MPLC», «Обновление»

5.5.1 Вкладка «Прочие настройки»

Дополнительные настройки контроллера. Внешний вид вкладки представлен на Рис. 25. Описание приведено в таблице 5.

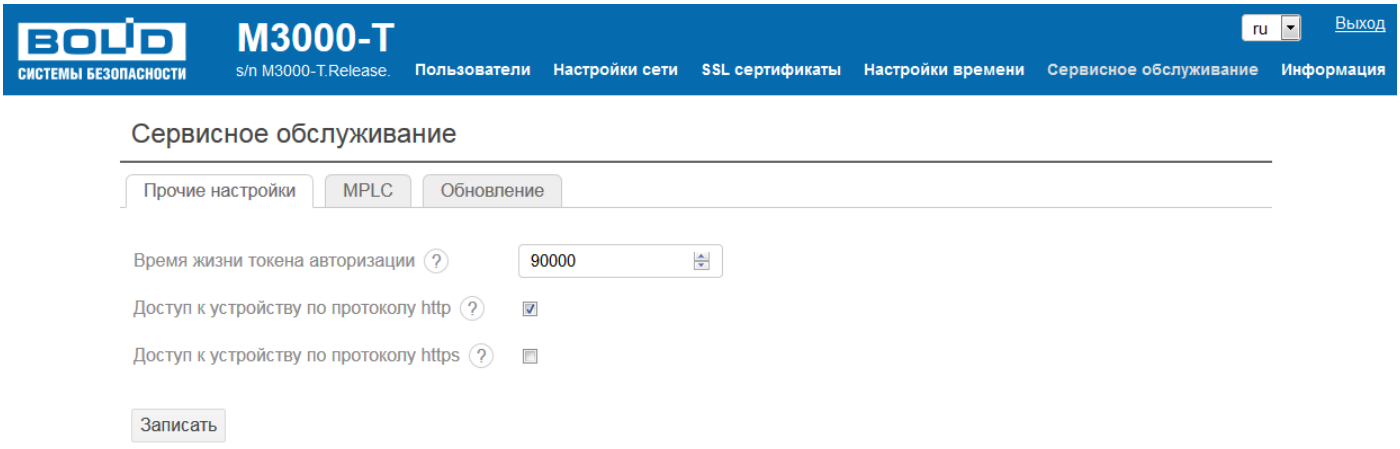


Рисунок 25. Сервисное обслуживание вкладка «Прочие настройки»

Таблица 5.1. Настройки раздела «Сервисное обслуживание»

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

5.5.1 Вкладка «MPLC»

Вкладка предназначена для получения информации о встроенной среде исполнения контроллера MasterPLC, определения статуса её работы, активирования лицензии и работы с резервной копией среды. Нижняя часть вкладки отражает распределение, объём и ресурс внутренней памяти контроллера, а также наличие и объём подключенных внешних накопителей. Внешний вид вкладки представлен на Рис. 26.1 (верхняя часть), Рис. 26.2 (нижняя часть) и Рис. 26.3 (нижняя часть).

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.

Для удобства пользователя информация по расходованию этого ресурса процесс износа выводится в отдельное поле, меняющее цвет в зависимости от процента износа накопителя.

Таблица 5.2. Вкладка «MPLC» Зависимость расцветки поля Ресурса памяти от износа.

Процент износа накопителя %	Цвет поля
0-50	зеленый
51-70	желтый
71-99	красный
100	Бордовый (выход из строя)

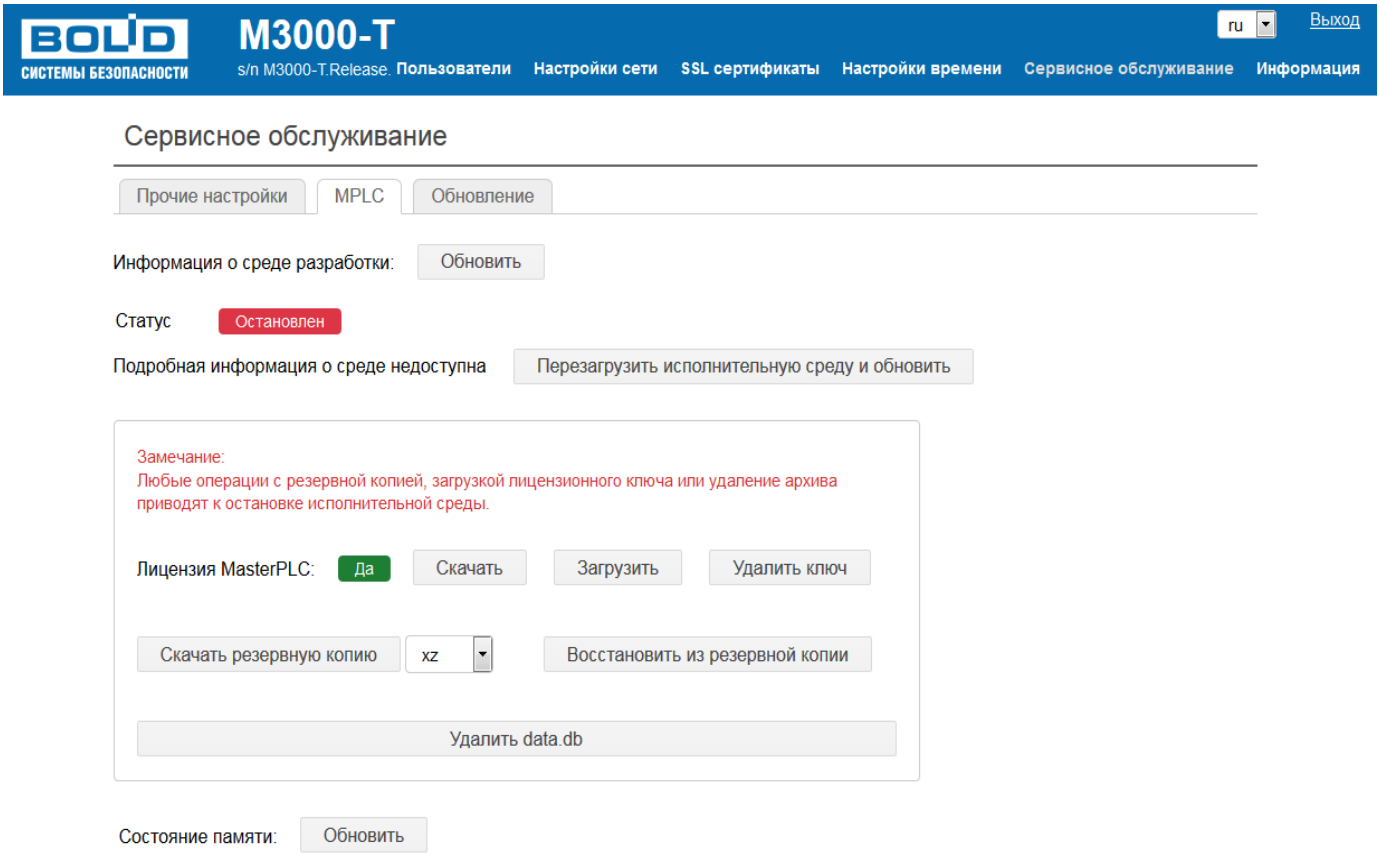


Рисунок 26.1. Сервисное обслуживание вкладка «MPLC» верхняя часть.

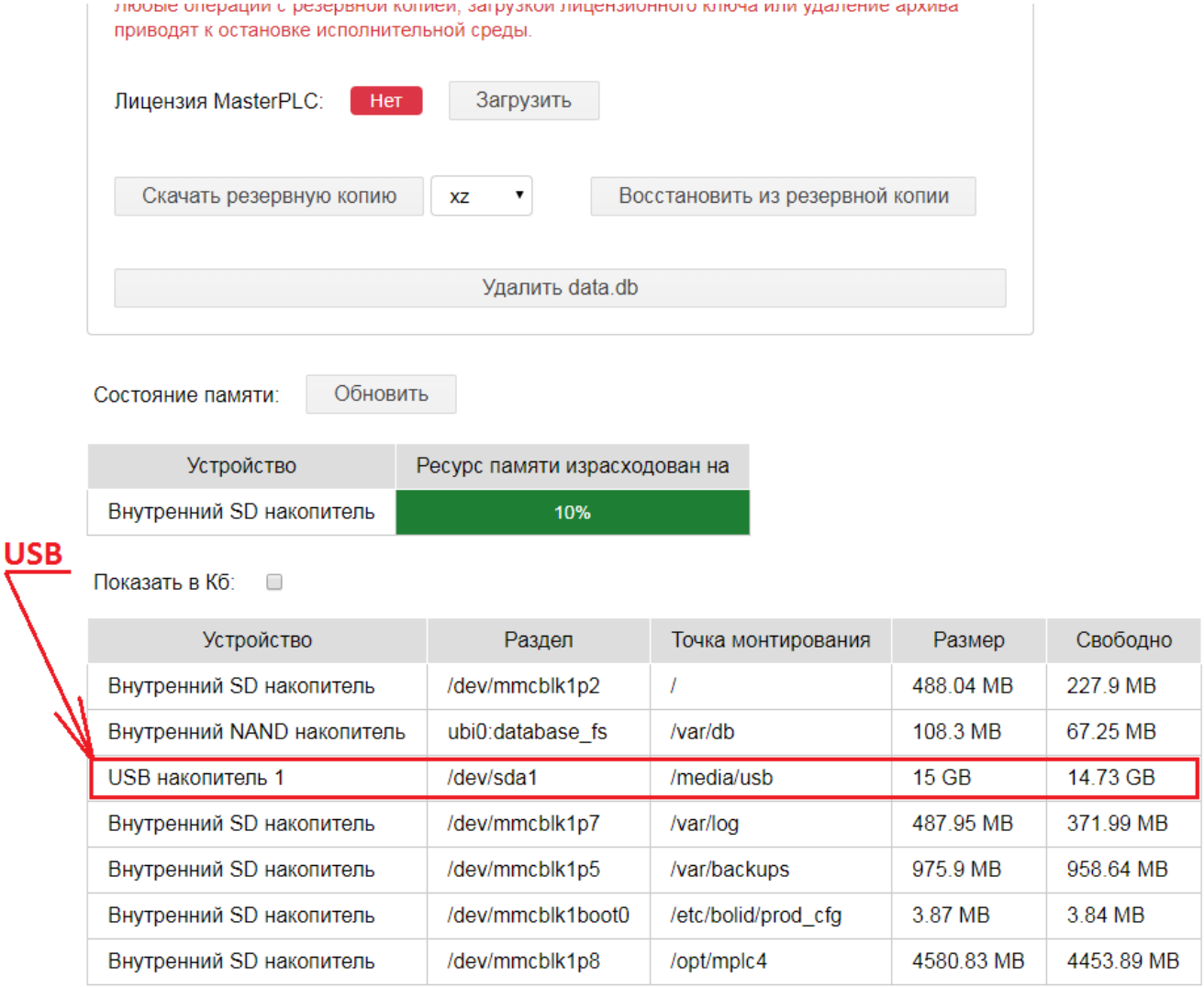


Рисунок 26.2. Сервисное обслуживание вкладка «MPLC» нижняя часть. В контроллер установлен внешний USB-накопитель.

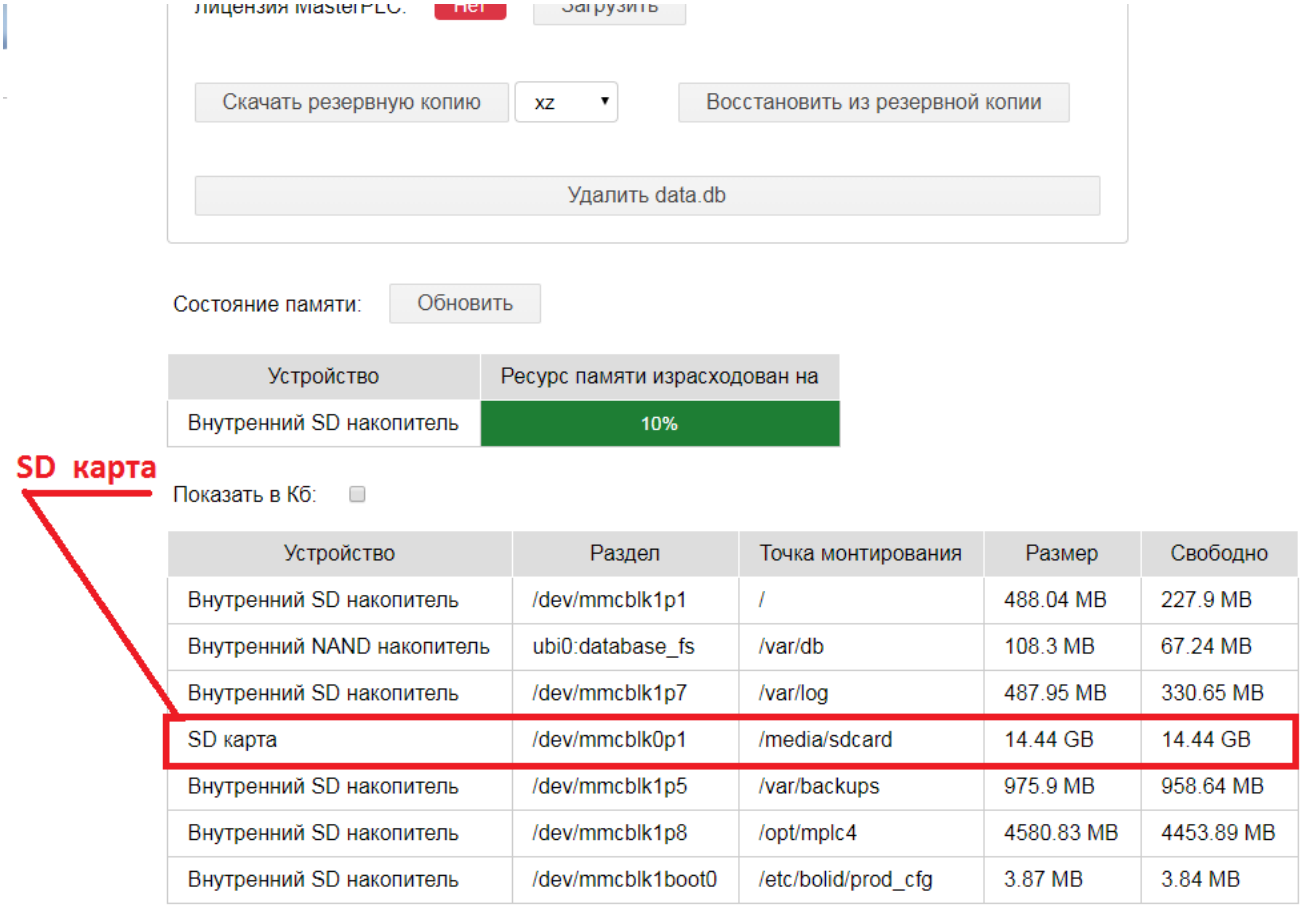


Рисунок 26.3. Сервисное обслуживание вкладка «MPLC» нижняя часть. В контроллер установлена внешняя SD-карта памяти.

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 рис. 27.1 и 27.2

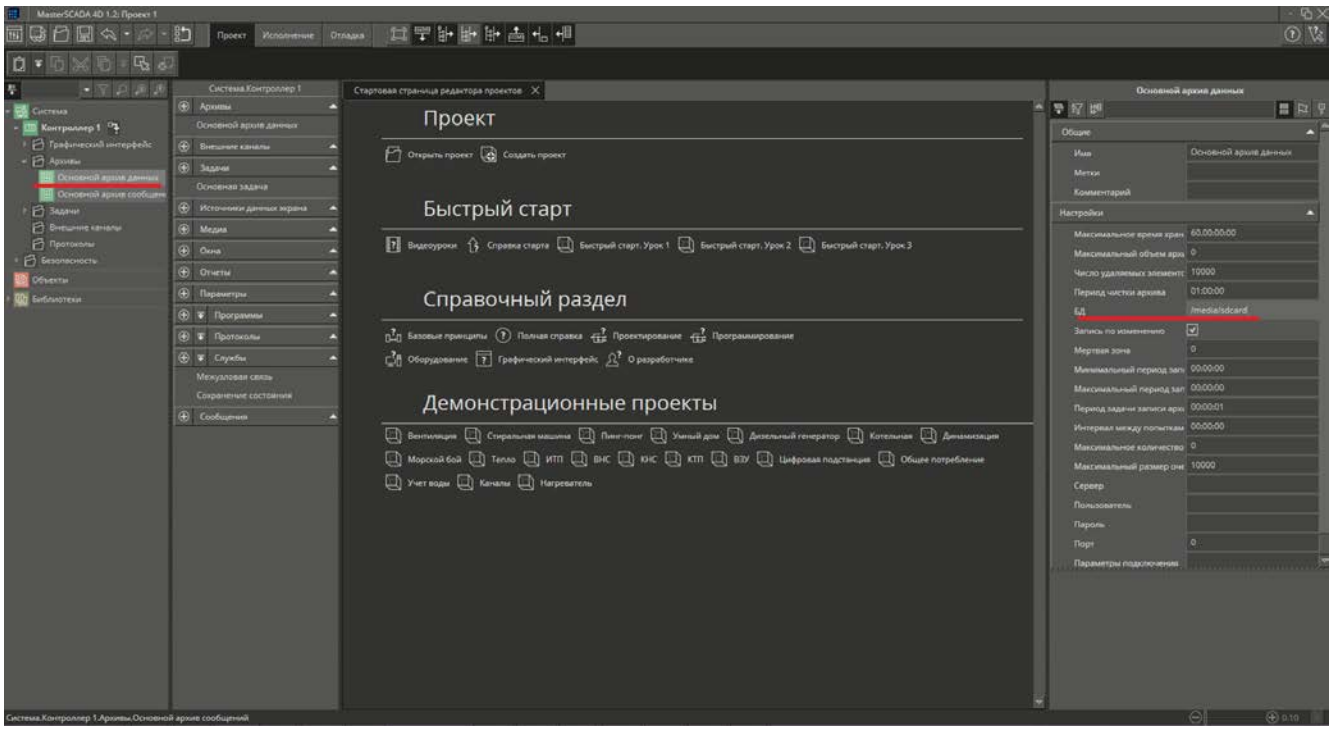


Рисунок 27.1. Окно среды разработки MasterSCADA 4D с элементами настройки архива (общий вид окна).

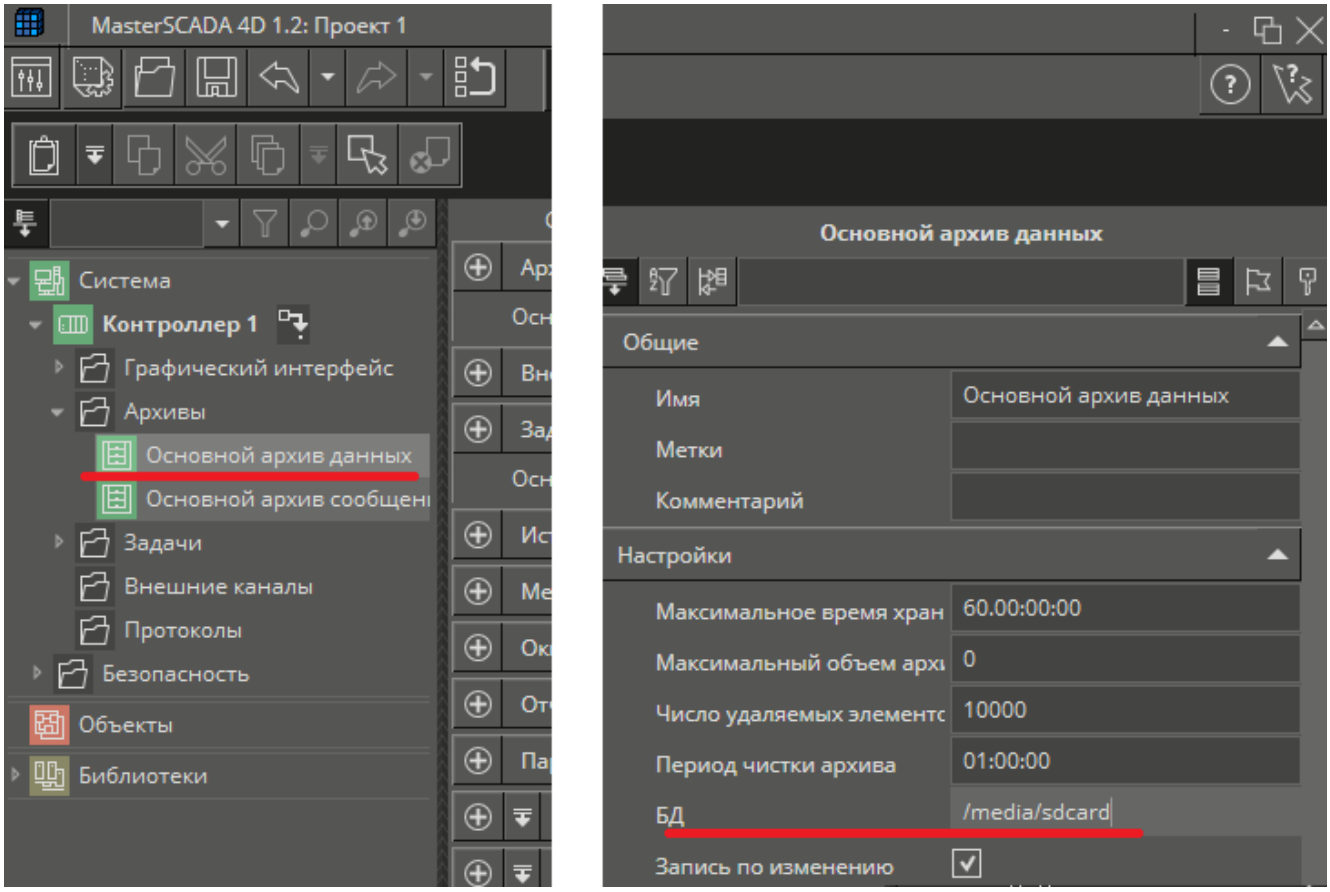


Рисунок 27.2. Фрагменты окна среды разработки MasterSCADA 4D с элементами настройки архива (дерево объектов слева и настройки архивирования справа.). Архивирование производится по изменению на внешнюю SD-карту.

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 Рис. 26.2 и Рис.26.3. Если габариты USB-накопителя препятствуют закрытию контроллера, то следует использовать кабель-удлинитель.

Для сохранения резервной копии следует нажать кнопку «Скачать резервную копию» (см. Рисунок 26.1) после чего открывается диалоговое окно Рис. 28.

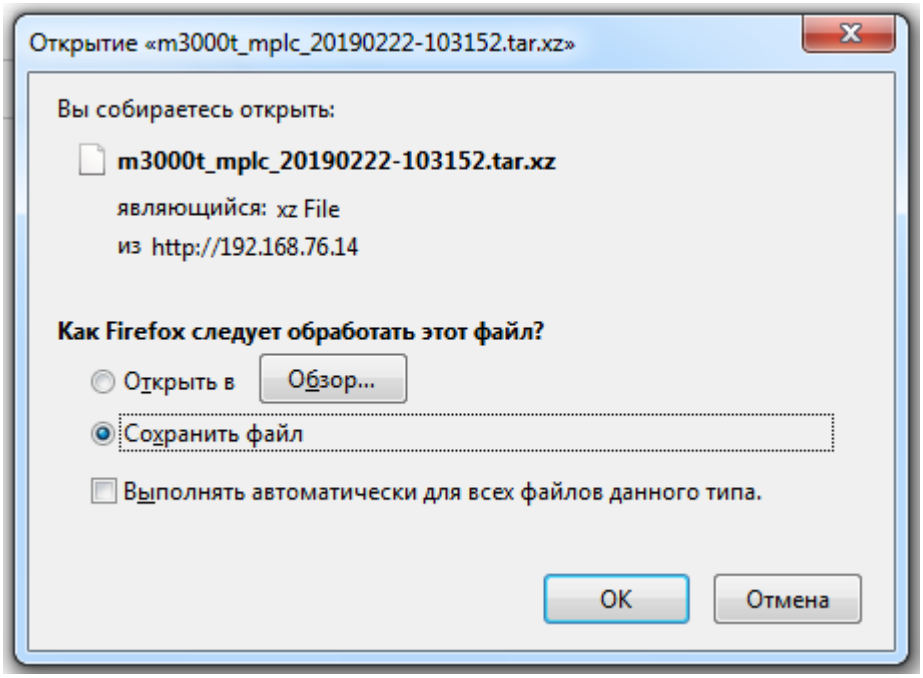


Рисунок 28. Диалоговое окно сохранения резервной копии.

При нажатии клавиши «Ок» производится сохранение файла. Процесс и результат загрузки можно просмотреть в окне «Загрузки» Рис. 29

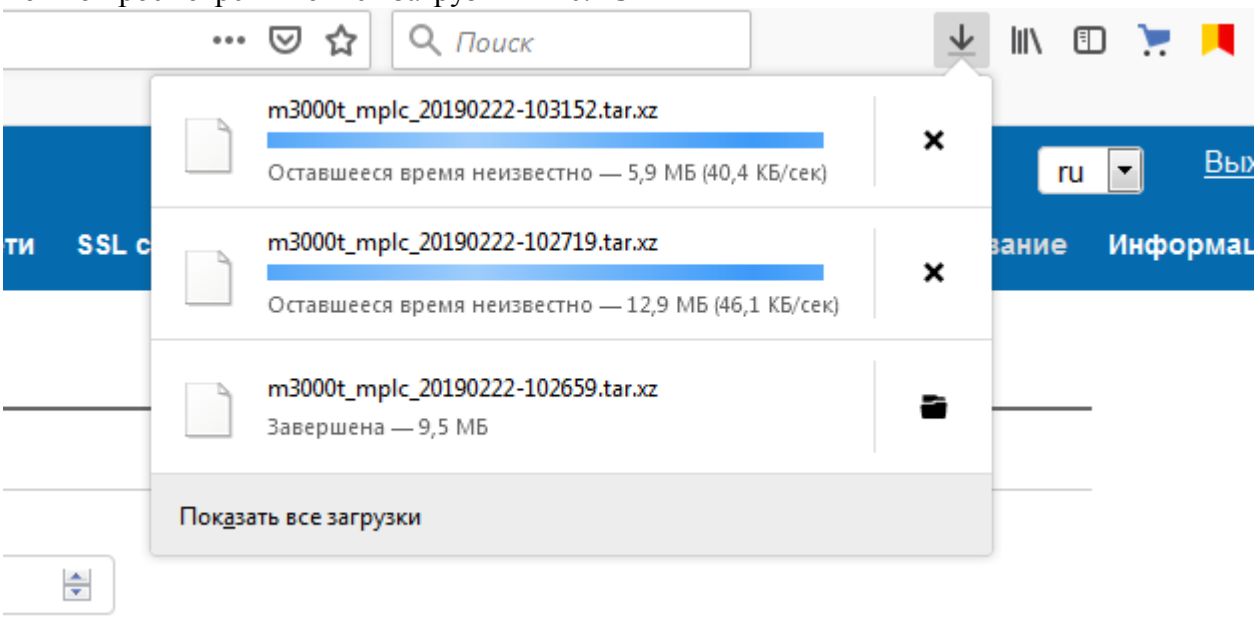


Рисунок 29. Окно загрузки резервной копии.

Для восстановления резервной копии нажимаем кнопку «Восстановить резервную копию» после чего открывается диалоговое окно поиска искомого файла и при двойном клике ЛКМ происходит его загрузка и восстановление резервной копии.

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 и при нажатии клавиши «Получить код» будет выведено сообщение, содержащее код активации, который вместе с номером лицензии (восьмизначное число на марке на процессорном модуле контроллера) и названием организации необходимо отправить по электронному адресу scada@insat.ru Рис 30. В ответ вы получите файл для активации лицензии.

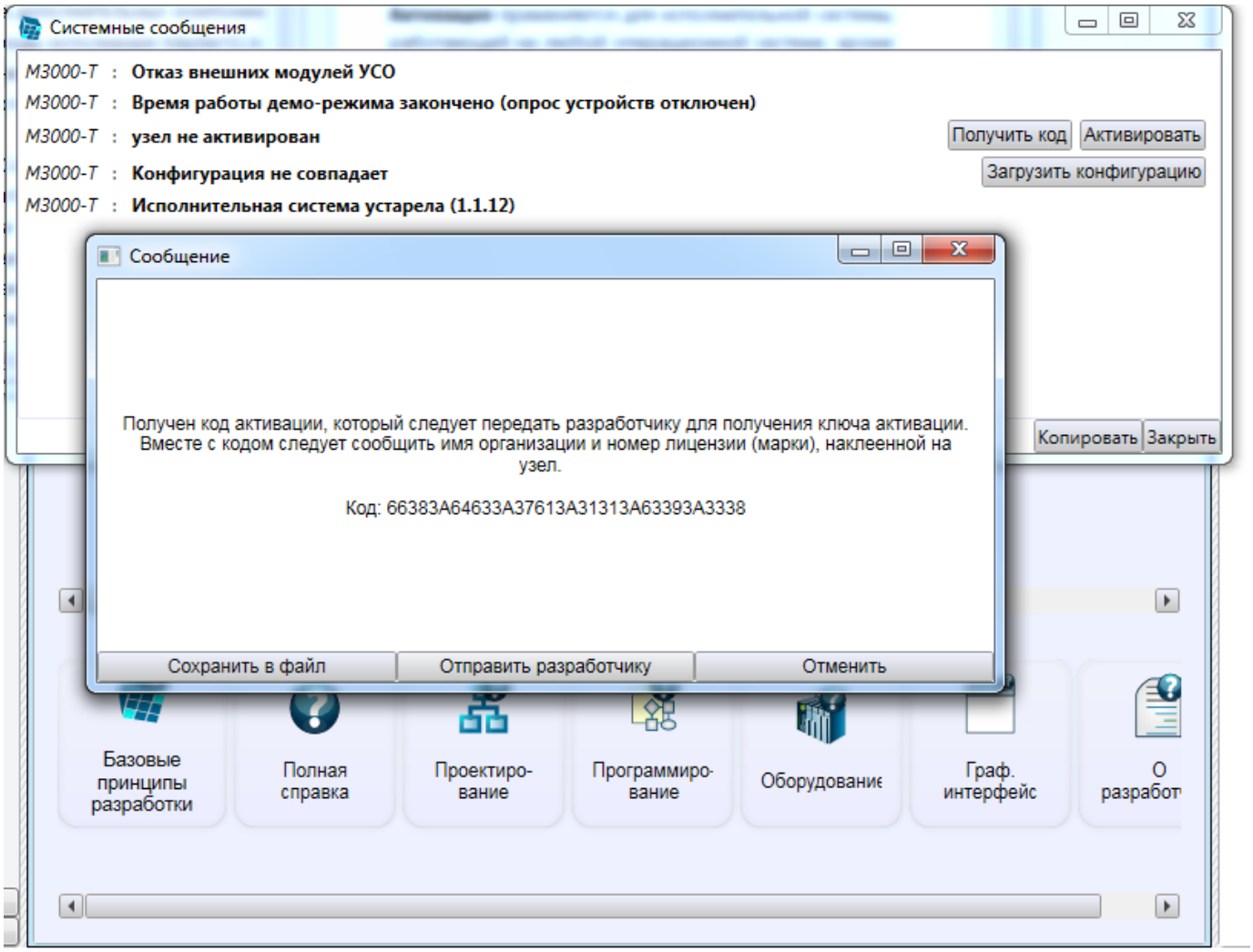


Рисунок 30. Окно системного сообщения об окончании демо-режима и окно с кодом активации.

Активировать полученный ключ возможно во вкладке «MPLC» вкладки «Сервисное обслуживание» нажатием кнопки Лицензия Master PLC и далее на клавишу «Ок» в открывающемся окне «Открытие «mplc.key»» Рис. 31.

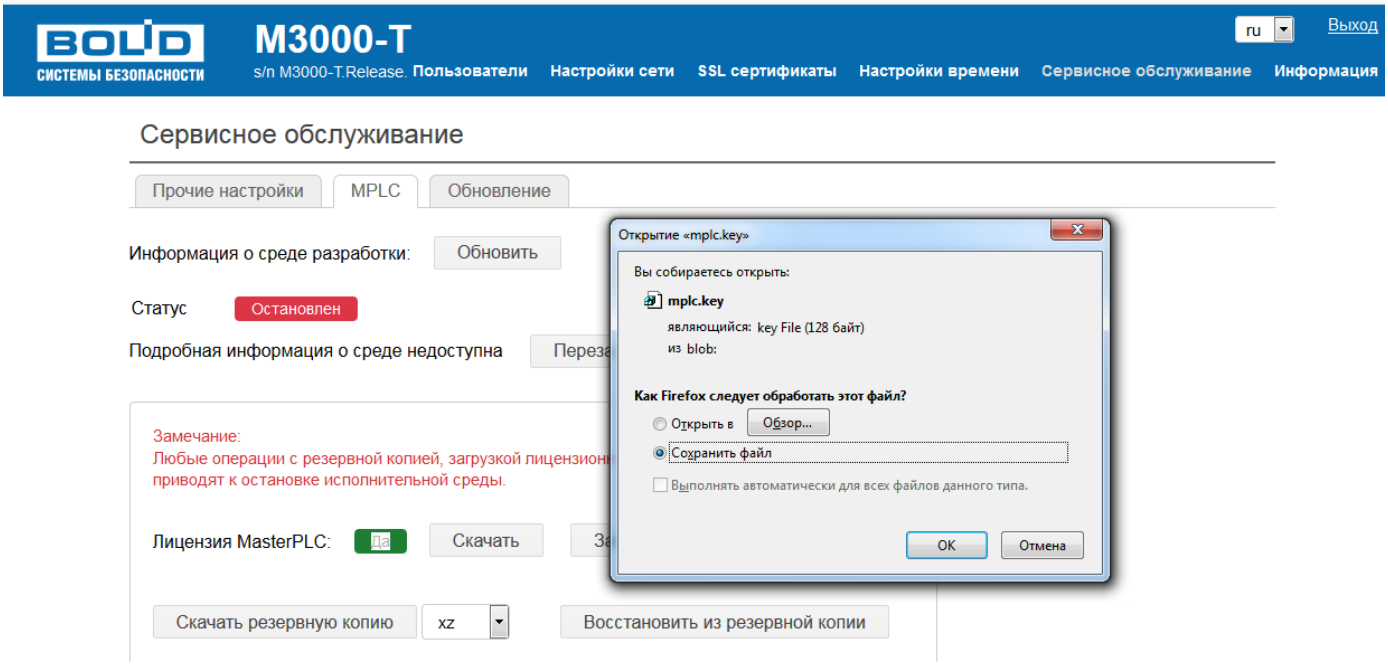


Рисунок 31. Диалоговое окно открытия файла лицензии.

5.5.2 Вкладка «Обновление».

Вкладка предназначена для обновления прошивки контроллера. Внешний вид вкладки представлен на Рис. 32.1

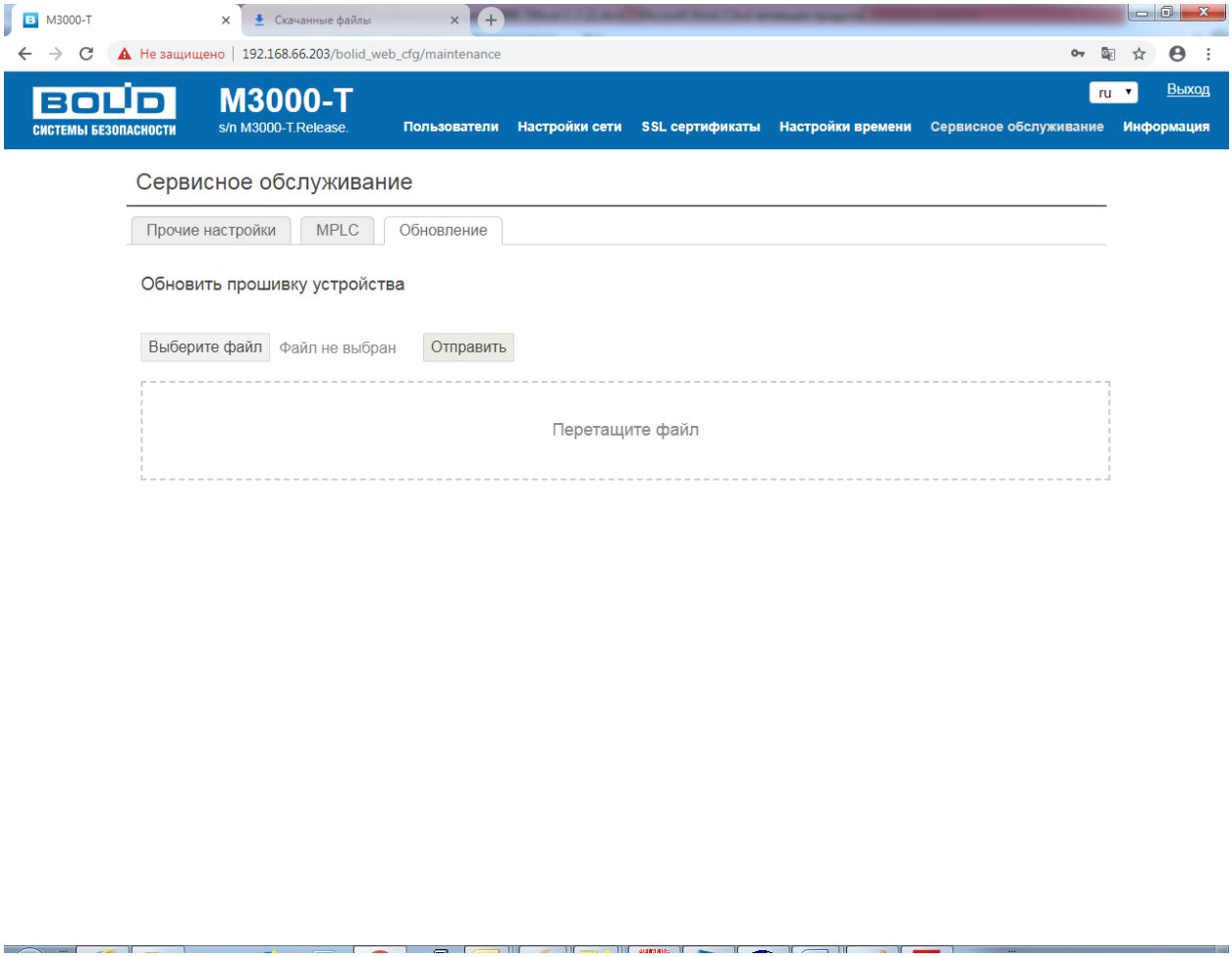


Рисунок 32.1. Вкладка «Обновление»

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

Список доступных прошивок, их ключевые особенности и рекомендуемые обновления доступны на сайте http://bolid.ru на вкладке «Скачать» страницы соответствующего прибора.

Обновление прошивки осуществляется через веб-интерфейс контроллера. В веб интерфейсе скачанный файл загружается в конвертер на вкладке «Обновление» страницы «Сервисное обслуживание». Необходимо нажать кнопку «Обзор», выбрать файл прошивки и нажать кнопку «Отправить»:

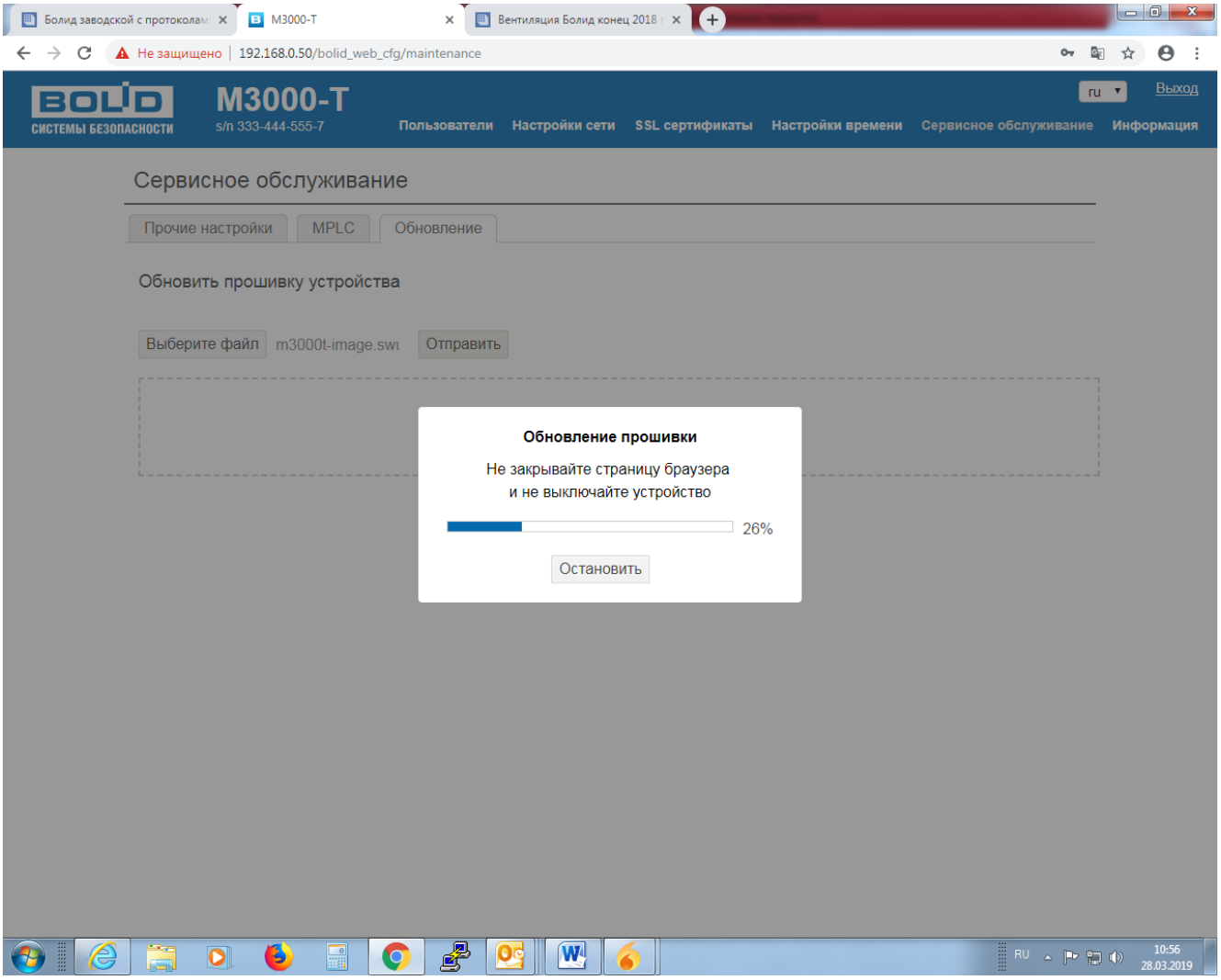


Рисунок 32.2. Обновление прошивки на устройстве через веб-интерфейс

В процессе обновления прошивки на экран выводится соответствующе сообщение и процент выполнения Рисунок 32.3. Процесс обновления можно остановить, нажав соответствующую клавишу «Остановить».

При удачном обновлении прошивки происходит автоматическая перезагрузка прибора, при этом связь с прибором теряется. После перезагрузки происходит автоматическое восстановление связи.

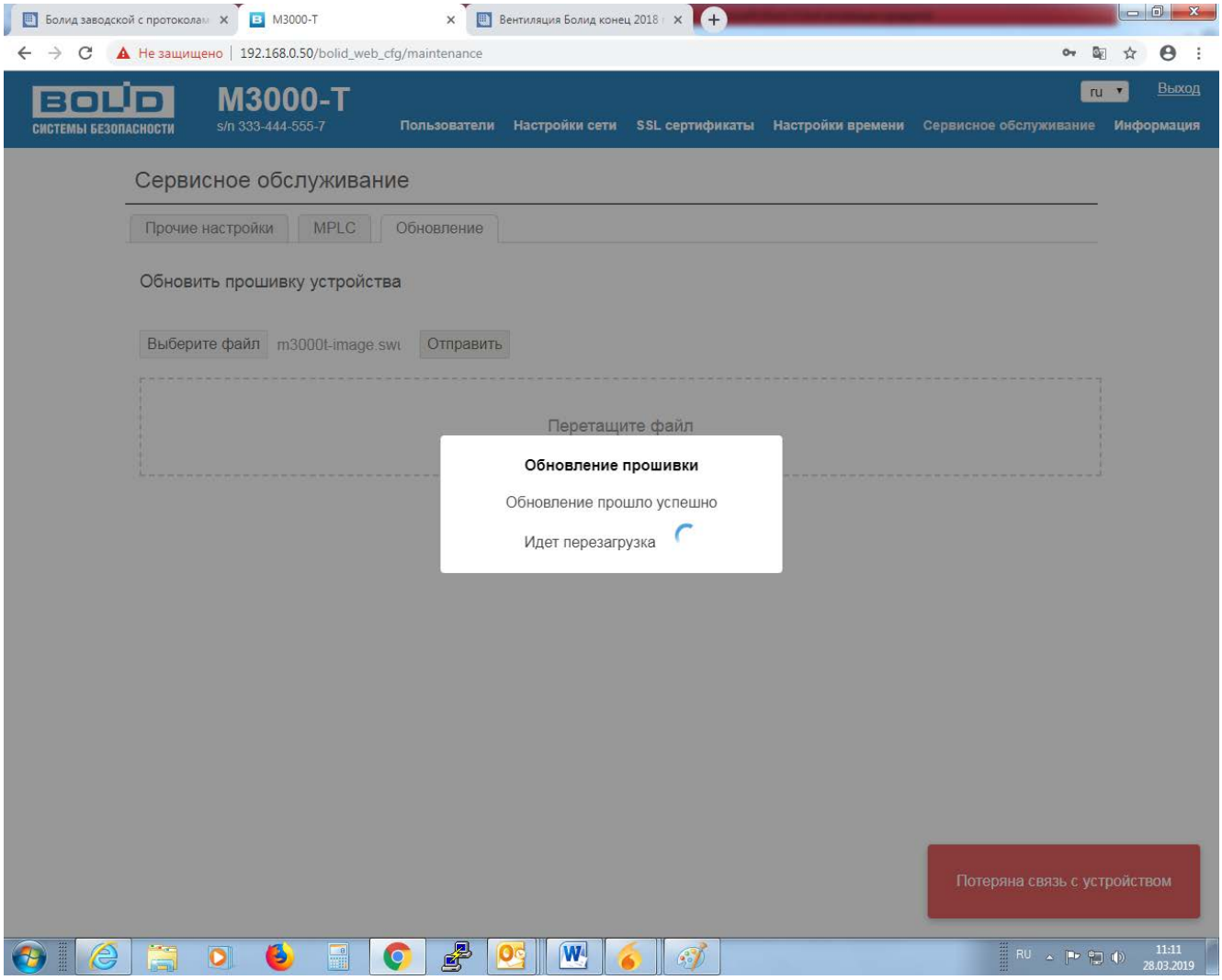


Рисунок 32.3. Обновление прошивки на устройстве через веб-интерфейс. Перезагрузка.

5.6 Страница «Информация»

Страница «Информация» содержит сведения об аппаратной части и программном обеспечении данного экземпляра изделия и его серийный номер. Внешний вид страницы представлен на Рис. 33.

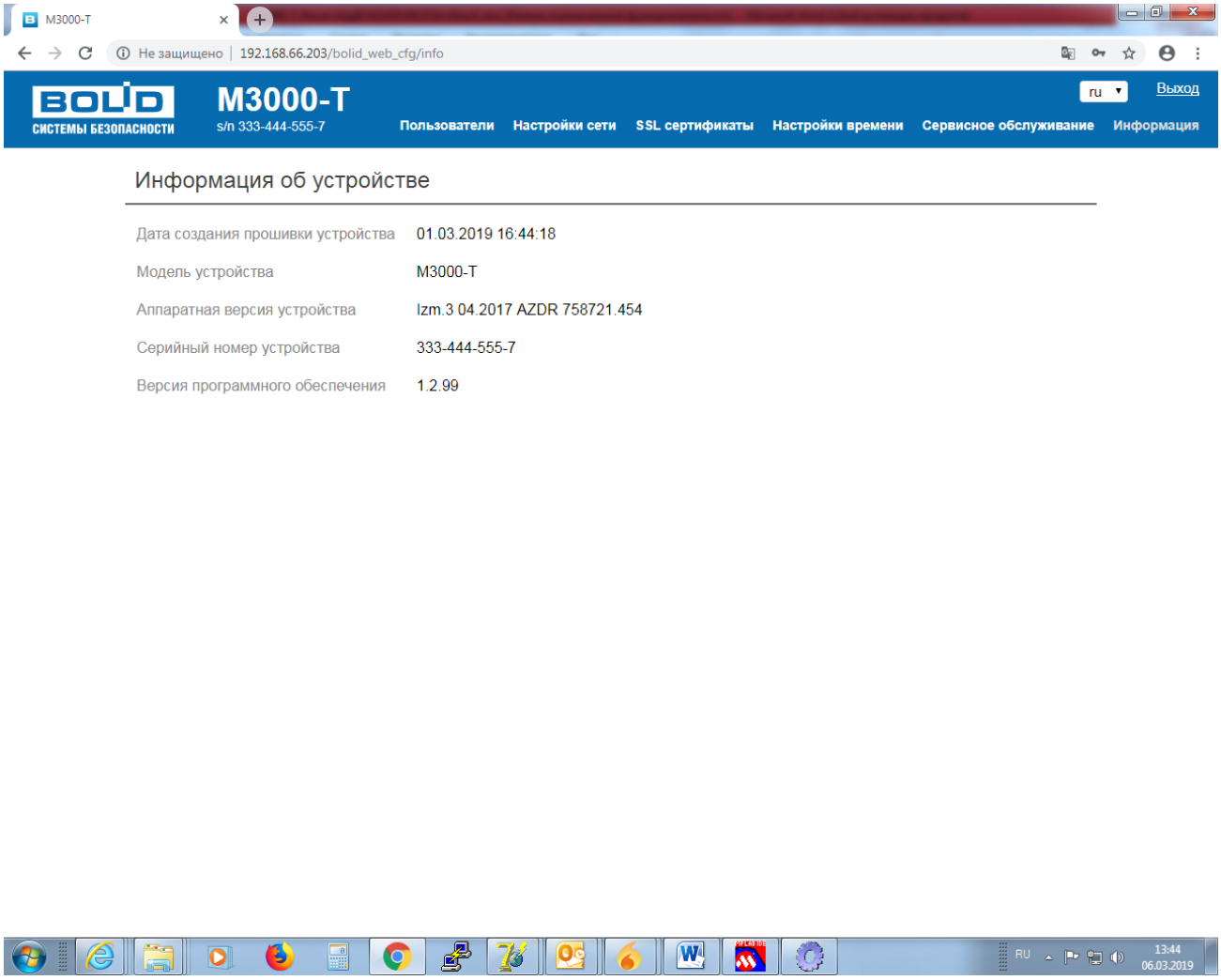


Рисунок 33. Страница «Информация»

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 (пинг) между компьютером и контроллером.

Учитывая, что заводские настройки контроллера 192.168.0.50 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, например, такие как представлены на Рисунке 34.

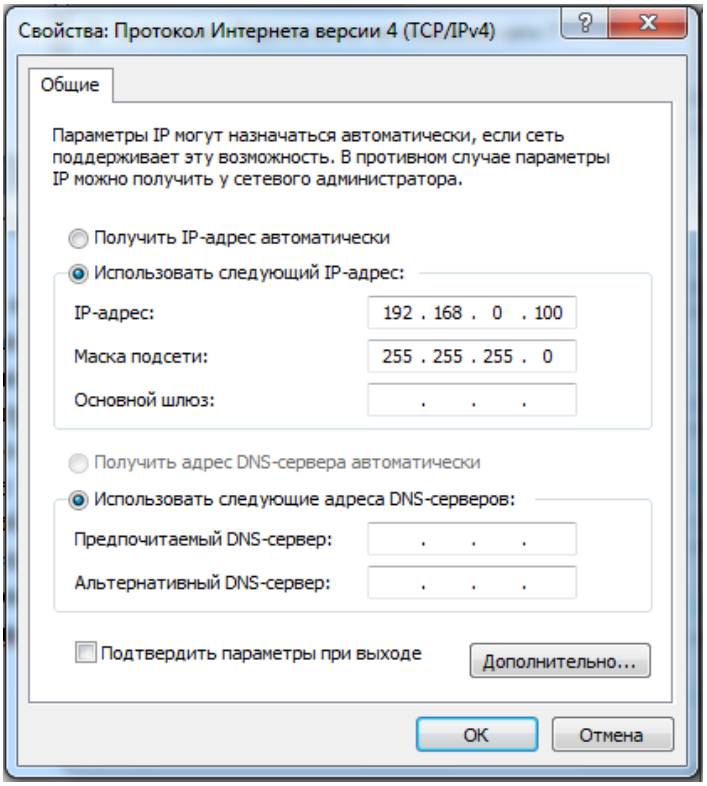


Рисунок 34. Сетевой адрес компьютера и маска подсети

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

- нажать «**Win+r**» и в появившемся окне «**Выполнить**» в поле «**Открыть**», см. Рисунок 35, ввести «**cmd**»:

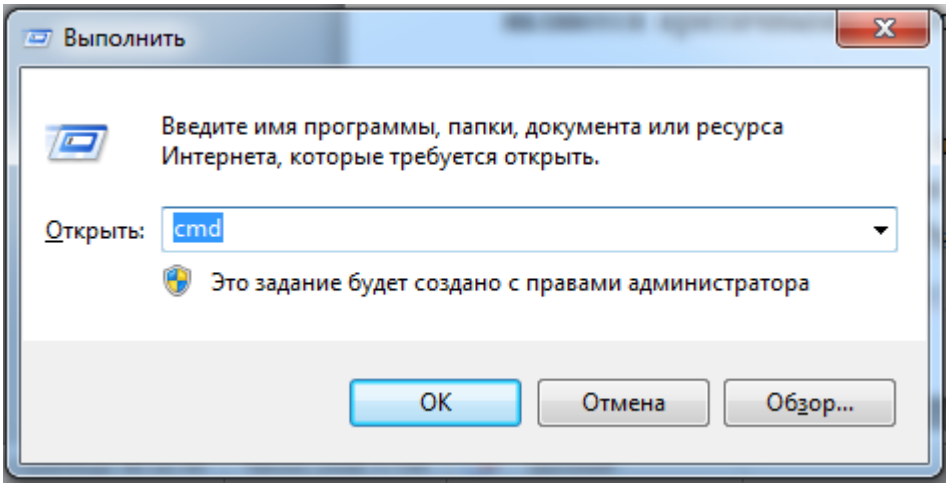


Рисунок 35. Окно «Выполнить»

- нажать «ОК». В появившейся командной строке», см. Рисунок 36, вводим команду «ping», пробел и адрес контроллера «192.168.0.50»:

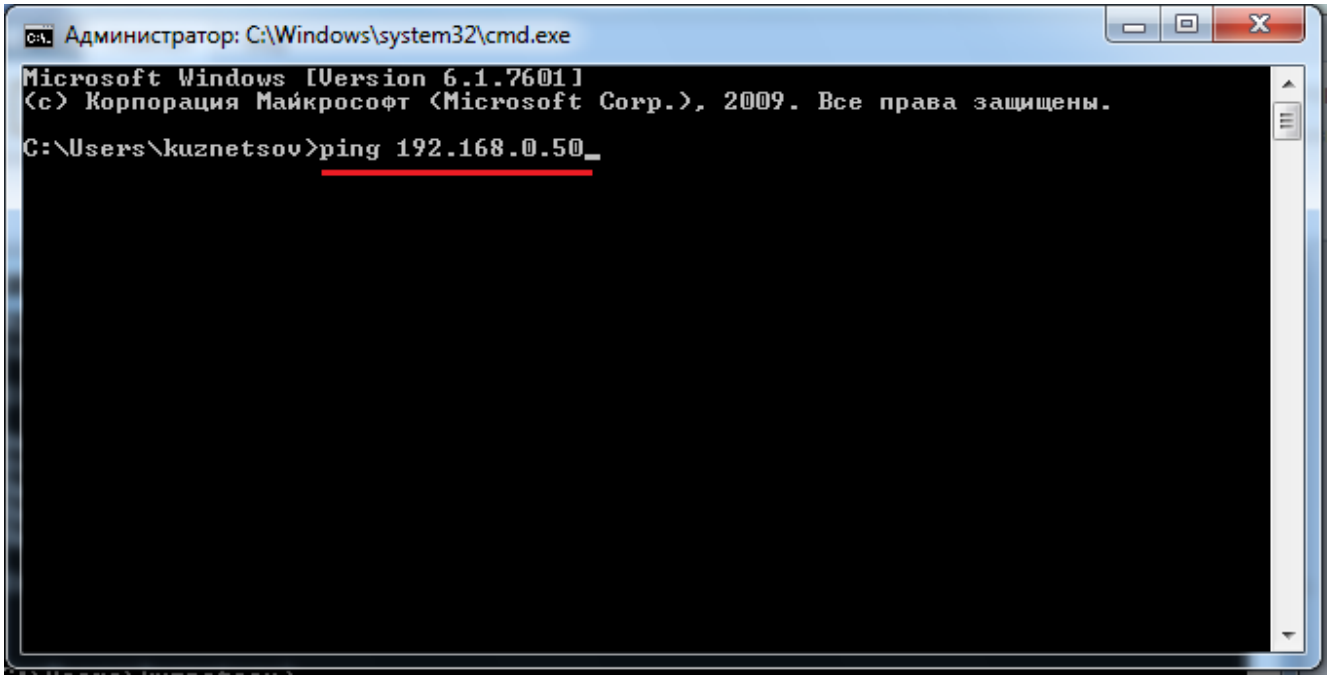


Рисунок 36. Окно «Администратор»

- нажимаем «Enter» и получаем информацию по наличию и качеству связи, см. Рисунок 37:

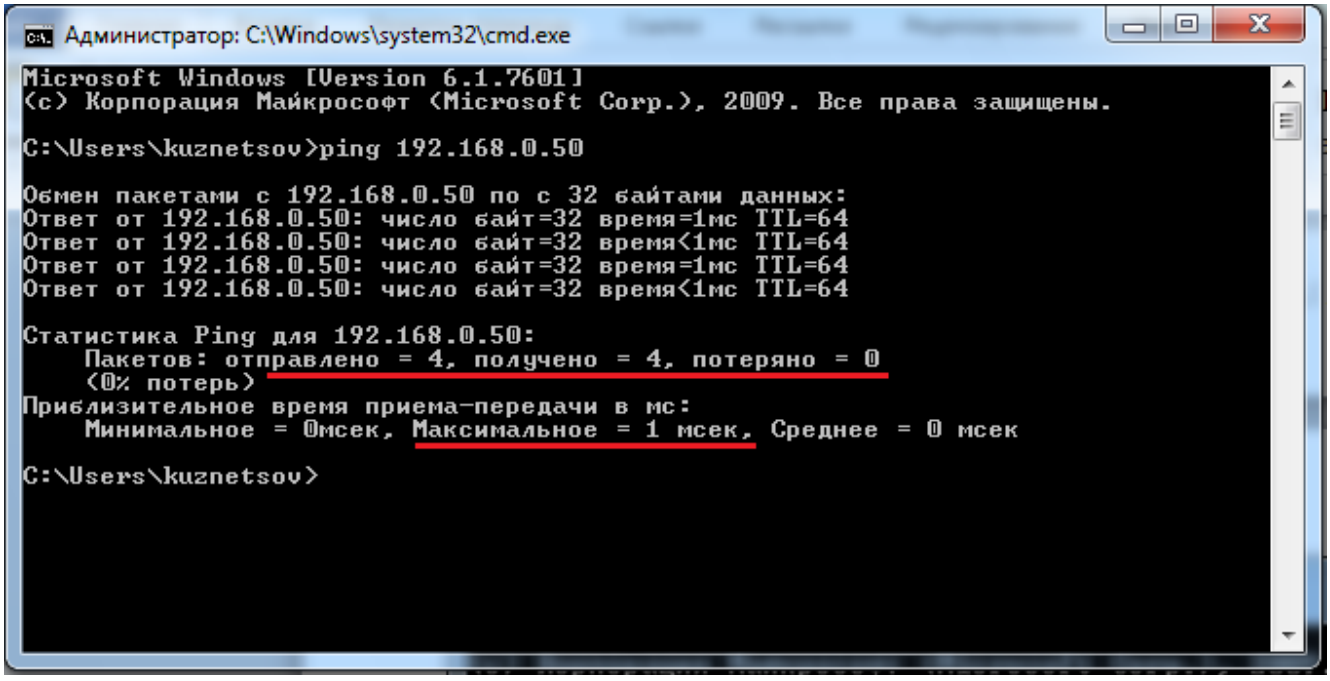


Рисунок 37. Окно «Администратор». Статистика обмена пакетами.

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 указать IP-адрес контроллера (см. Рис. 38) и нажать кнопку «Open».

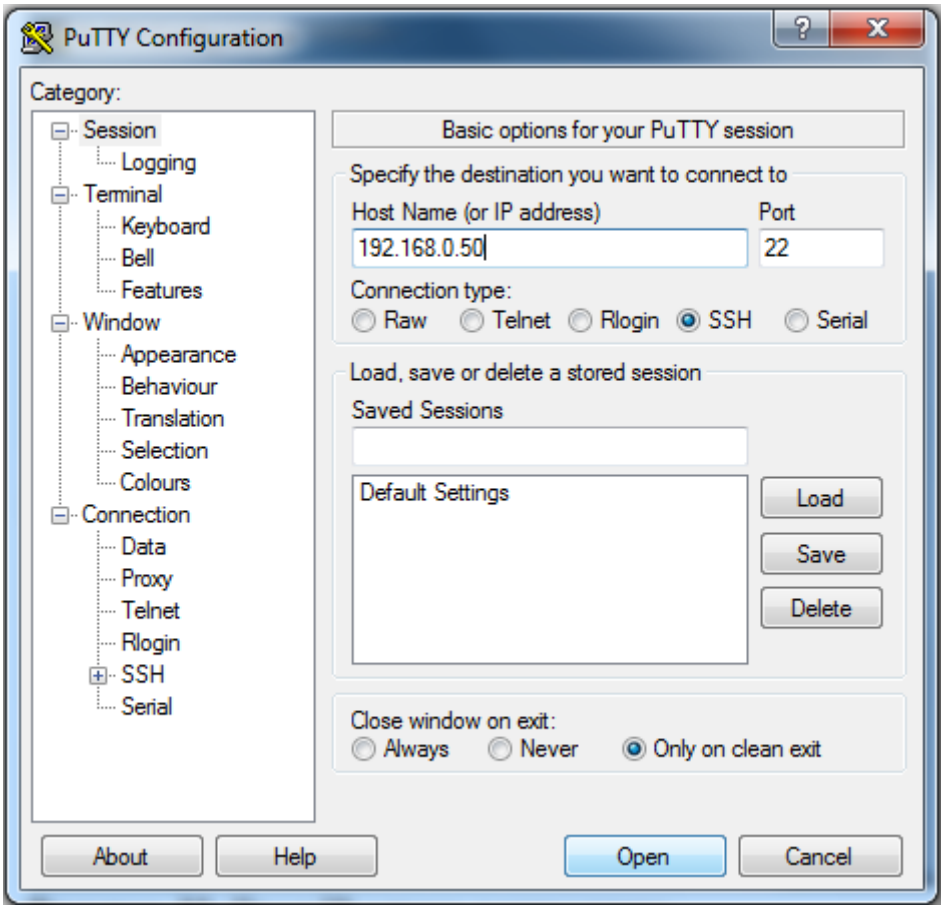


Рисунок 38. Ввод IP-адреса контроллера

В открывающемся окне при первом подключении выводится сообщение о возможной угрозе безопасности (См. рис. 39). Для продолжения процесса установки следует нажать «Да».

Рисунок 39. Сообщение о возможной угрозе безопасности.

На экране монитора появится текстовое окно для ввода логина (см. Рис. 40). После ввода логина появится текстовое окно для ввода пароля (см. Рис. 41) и система запросит ввод пароля (без отображения вводимых символов пароля).

Рисунок 40. Окно ввода логина.

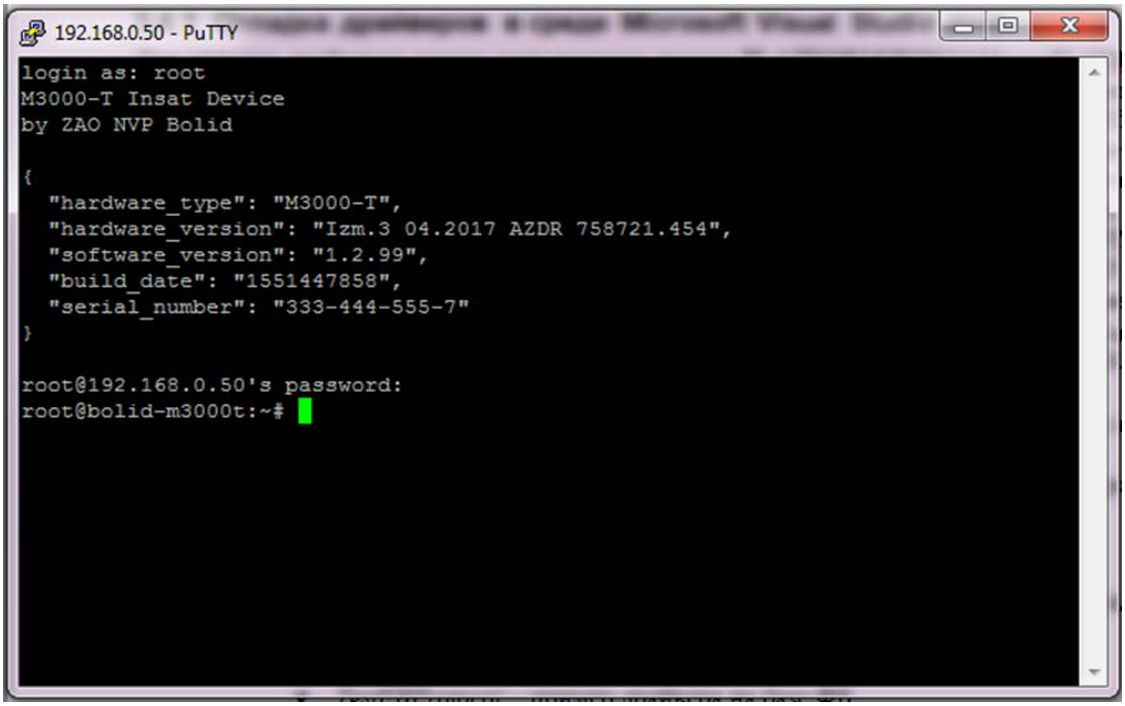


Рисунок 41. Окно ввода пароля.

Дальнейшая настройка контроллера производится согласно п.6.2.1 настоящего руководства.

6.2 Установка связи по интерфейсу RS232-D через COM-порт

При установке связи по интерфейсу RS232-D через COM-порт:

– в программе «PuTTY» выбрать тип соединения «Serial»,

– в разделе «Serial» выбрать настройки: 115200 8; N; 1; (см. Рис. 42),
– в разделе «Session» ввести номер COM-порта, к которому подключен контроллер (см. Рис.33) и нажать кнопку «Open».

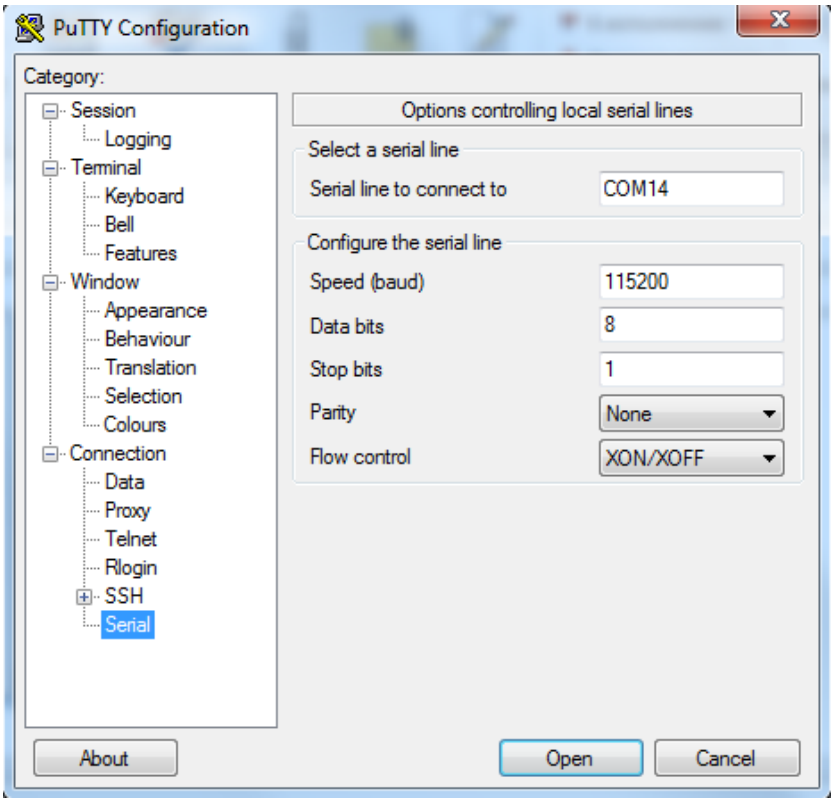


Рисунок 42. Установка параметров COM-порта

В открывающемся окне установить параметры соединения согласно Рис. 43 и нажать «Open».

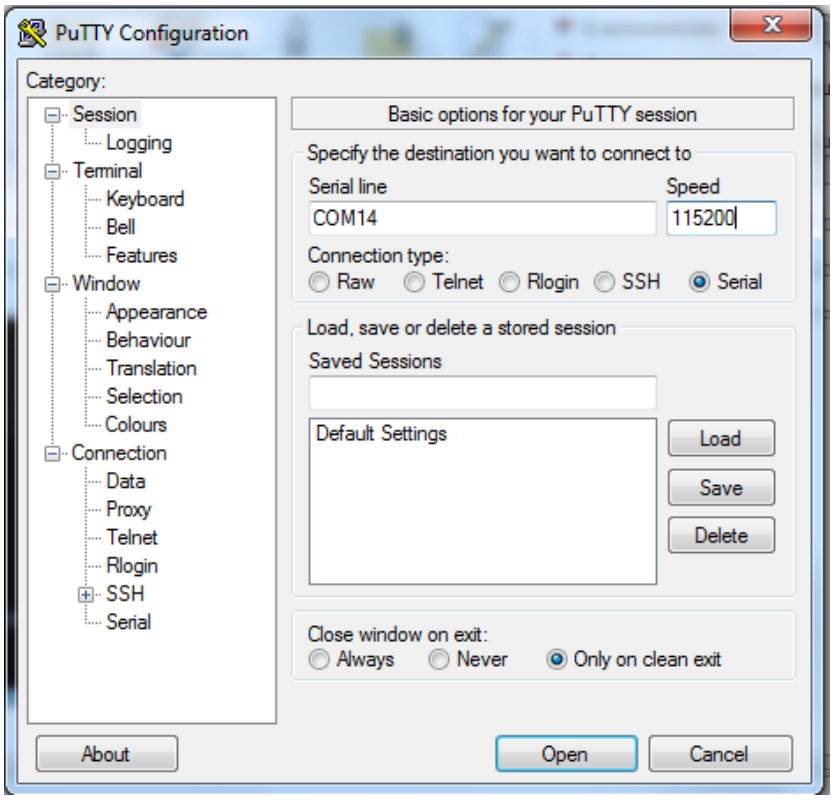


Рисунок 43. Установка параметров соединения

Нажать «Open».

При запуске контроллера в открывающемся окне появляются служебная информация и диалоговое окно для ввода логина (см. Рис. 44). пароля (см. Рис. 45). После загрузки контроллера автоматическая выдача информации в порт прекращается. Дальнейшая настройка контроллера производится согласно п.6.2.1 настоящего руководства.

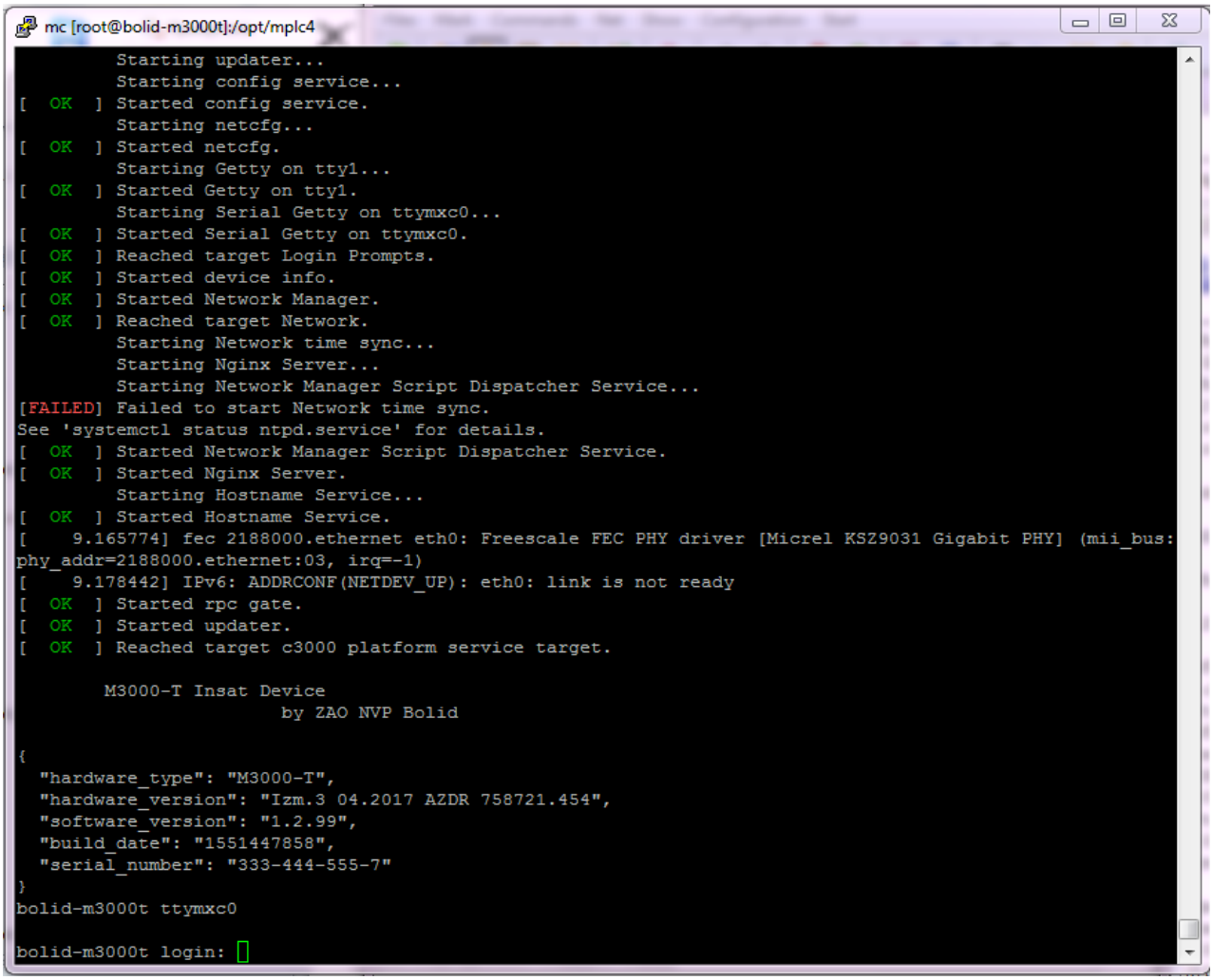


Рисунок 44. Окно ввода логина.

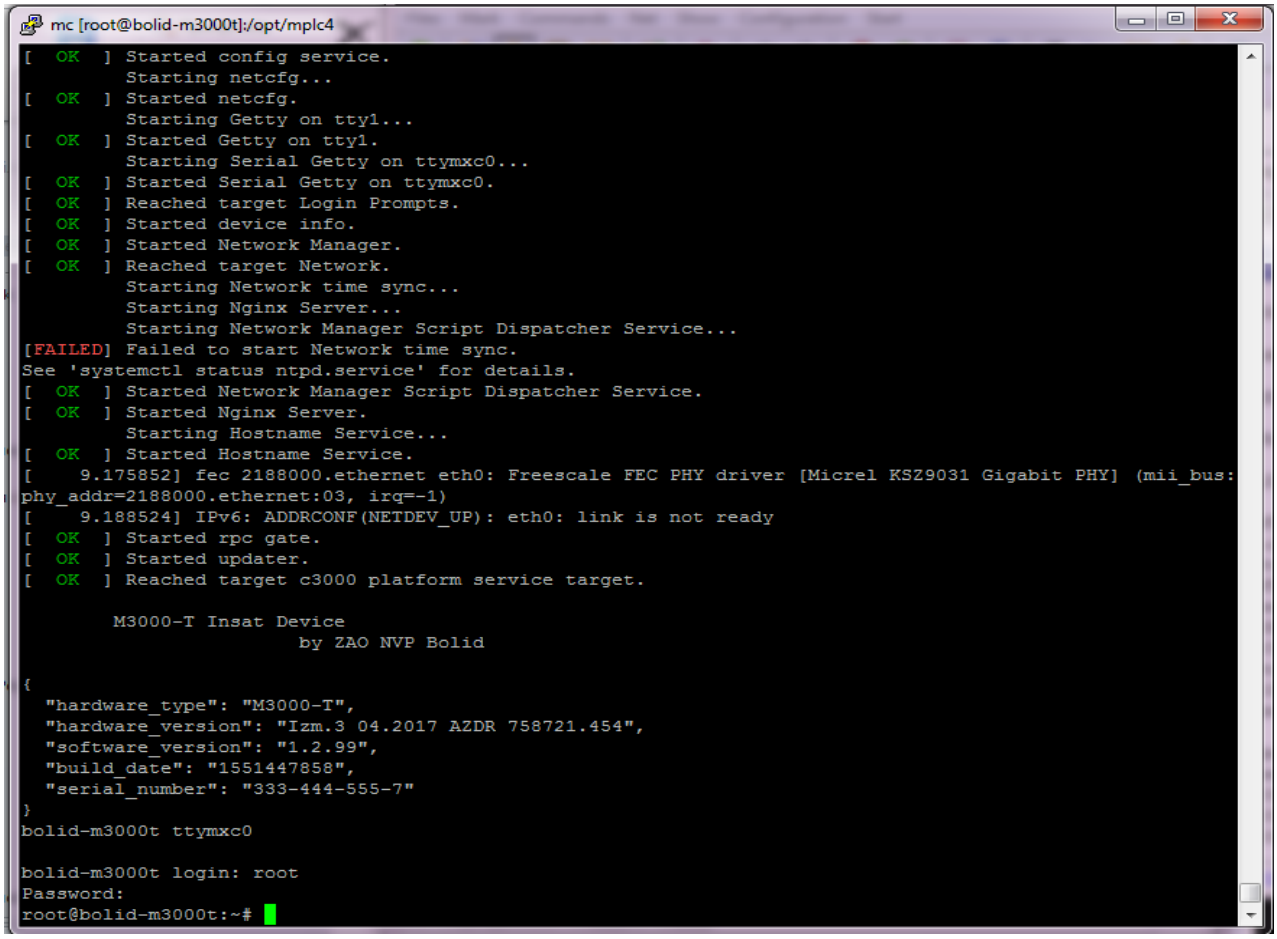


Рисунок 45. Диалоговое окно для ввода пароля

6.3 Сброс на заводские установки и специальные режимы включения, сброса и загрузки

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

- Длинное нажатие (тире или «1») – это удержание датчика вскрытия корпуса 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 нажатиями должна быть не менее 0,02 сек.
- Не нажатое в течение более 2 сек. состояние тампера является признаком конца набора комбинации.
- Нажатое более 6 сек. состояние тампера аннулирует комбинацию нажатий.

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:

- **полный сброс к заводским настройкам**: «точка» - «точка» - «точка» - «тире» - «тире» - «тире» - «точка» - «точка» - «точка»

- **сброс сетевых адресов на значения, указанные в инструкции**: - «тире» - «тире» - «тире» - «точка»

- **сброс пароля владельца на заводское значение**: «тире» - «тире» - «точка» - «точка» - «тире» - «тире» - «точка» - «точка»

Таблица 7.1 Специальные режимы включения, сброса и загрузки

Комбинация нажатий тампера	Режим
000111000	полный сброс устройства к заводским настройкам
1110	сброс сетевых адресов на значения, указанные в инструкции
11001100	сброс пароля владельца на заводское значение

7 КОНФИГУРИРОВАНИЕ

7.1 Использование по назначению

Перед использованием ПЛК необходимо запрограммировать, т.е. создать пользовательскую программу. Созданная пользовательская программа, может быть сохранена в энергонезависимой Flash-памяти контроллера и запускаться на выполнение 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.

7.2 Изменение начальной конфигурации контроллера

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

7.2.1 Работа с операционной системой Linux в консольном режиме.

Для консольного доступа к системе Linux используется порт 232D. 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 отладочный 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 «login»: «**root**» (по умолчанию) («**admin**» в http(s)),

в поле ввода пароля «Password»: **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.

7.2.2 Изменение версии программного обеспечения.

Изменение версии программного обеспечения контроллера производится из окна Вэб-браузера (См. п 5.5.2 «Обновление» настоящего Руководства). Изменение версии программного обеспечения контроллера с использованием CD-карточек, как это было в предыдущих версиях, более не поддерживается.

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 Ethernet (при установке соответствующих сетевых настроек 192.168.0.1/24).

9 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И РЕМОНТ

Работы по техническому обслуживанию выполняются не реже 1 раза в год обслуживающим персоналом, имеющим группу электробезопасности не ниже 3.

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 п.8 настоящего руководства;
- проверку надёжности крепления контроллера, состояния внешних монтажных проводов, контактных соединений;
- проверку оставшегося ресурса памяти по записи согласно пункта 5.5.1 настоящего Руководства (в пределах от 10 до 90%);
- 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 5.5.1 настоящего Руководства.

ВНИМАНИЕ!

Претензии без приложения акта предприятие-изготовитель не принимает.

Выход контроллера из строя в результате несоблюдения потребителем правил монтажа или эксплуатации, в том числе в условиях повышения износа памяти в результате большого числа быстрых операций сохранения архивов, не является основанием для рекламации и гарантийного ремонта.

ВНИМАНИЕ!

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

Рекламации направлять по адресу:
ЗАО НВП «Болид», Россия, 141070, Московская область, г. Королёв, ул. Пионерская, 4.
Тел./факс: **(495) 775-71-55** (многоканальный). E-mail: info@bolid.ru

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

10 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Перечень возможных неисправностей и способов устранения приведён в таблице 11.1.

Таблица 9.1 Возможные неисправности 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.	1) Подключиться к контроллеру по порту RS232D и выставить IP-адрес. 2) Сбросить сетевые настройки 3) 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 RS485	Неправильно выставлены номера подключенных портов	Проверить номера портов в проекте

11 ТРАНСПОРТИРОВАНИЕ, ХРАНЕНИЕ, УТИЛИЗАЦИЯ

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

12 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.

13 СВЕДЕНИЯ О СЕРТИФИКАЦИИ ИЗДЕЛИЯ

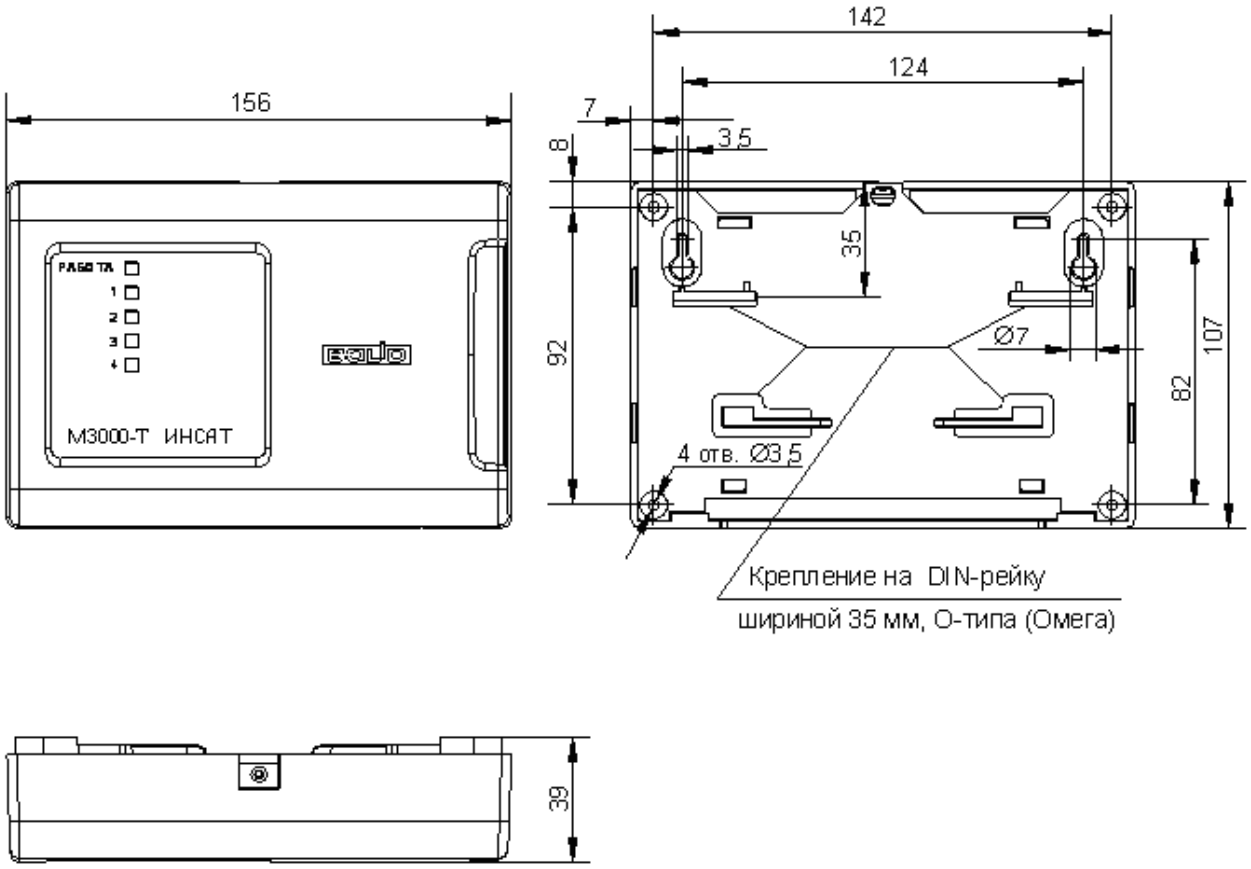
13.1 Контроллер соответствует требованиям Технического регламента Таможенного союза ТР ТС 020/2011 и имеет сертификат соответствия: ТС № RU C-RU.ME61.B.01549.

13.2 Производство контроллеров имеет сертификат соответствия ГОСТ Р ИСО 9001-2015 № РОСС RU.АБ66.К00003, выданный ОС СМК "ПОЖТЕСТ", 143903, г. Московская область, г. Балашиха, мкр. ВНИИПО, д. 12.

ИСО 9001

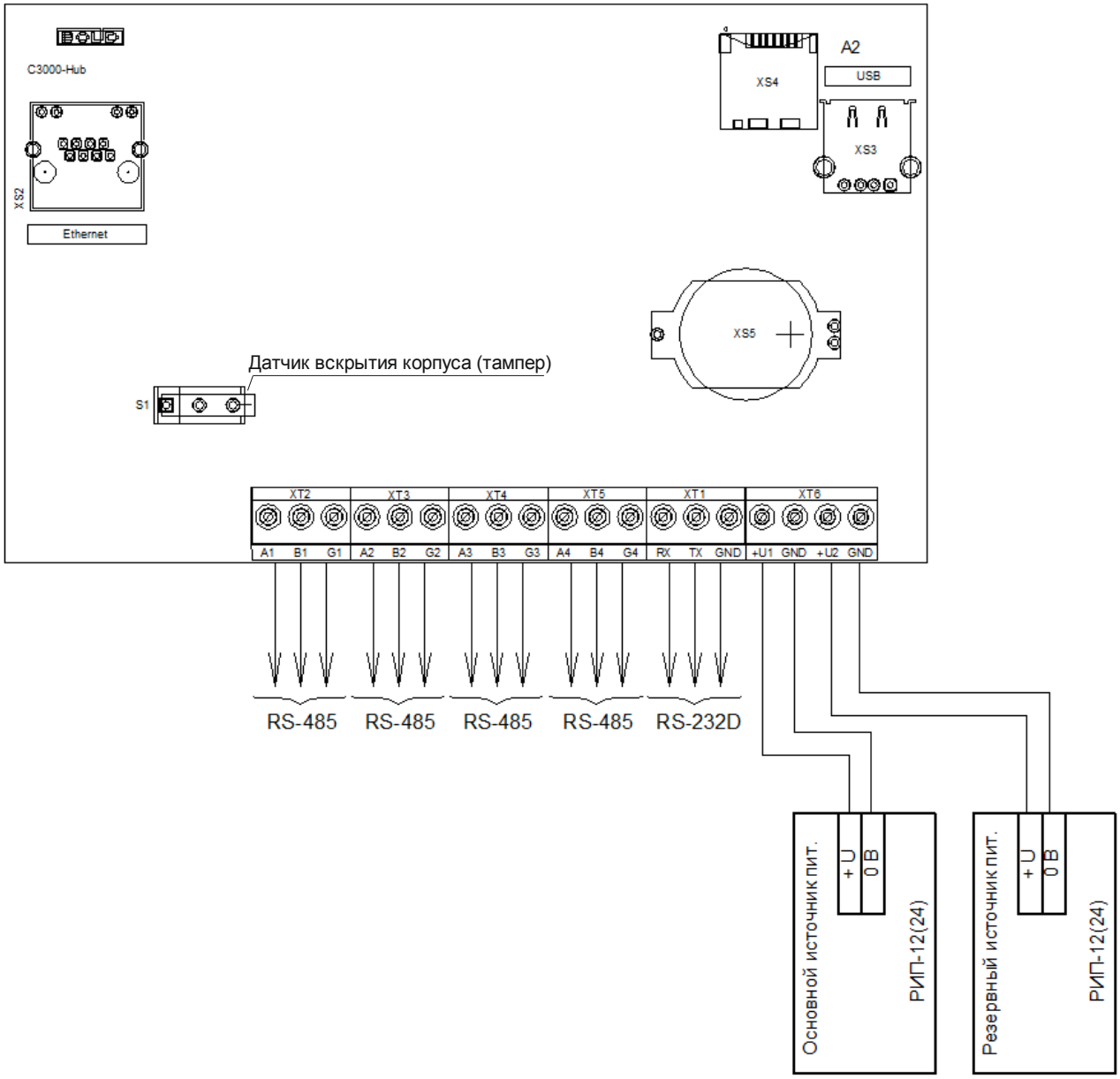
ПРИЛОЖЕНИЕ А

Габаритные и установочные размеры контроллера «М3000-Т Инсат»



ПРИЛОЖЕНИЕ Б

Схемы внешних подключений



XS2 – разъём для подключения Ethernet-кабеля;
XS3 – разъём для подключения USB-накопителя;
XS4 – слот для подключения SD-карты.