

**Настройка аппаратных и программных средств,
необходимых для работы с ЭП в WEB-портале ММПК
«Бронка»**

СОДЕРЖАНИЕ

1	Введение	3
2	Настройка программных средств и компонентов	3
2.1	Базовое программное обеспечение.....	3
2.2	Установка сертификата электронной подписи	3
2.3	Установка корневого сертификата Удостоверяющего центра	7
2.4	Настройка браузера	12

1 Введение

Данный документ содержит перечень технических требований, предъявляемых к рабочему месту пользователя WEB-портала ММПК «Бронка», для работы с сертификатом электронной подписи.

2 Настройка программных средств и компонентов

2.1 Базовое программное обеспечение

Для использования алгоритмов криптографической защиты информации с использованием сертификата электронной подписи на клиентской рабочей станции должно быть установлено следующее базовое программное обеспечение:

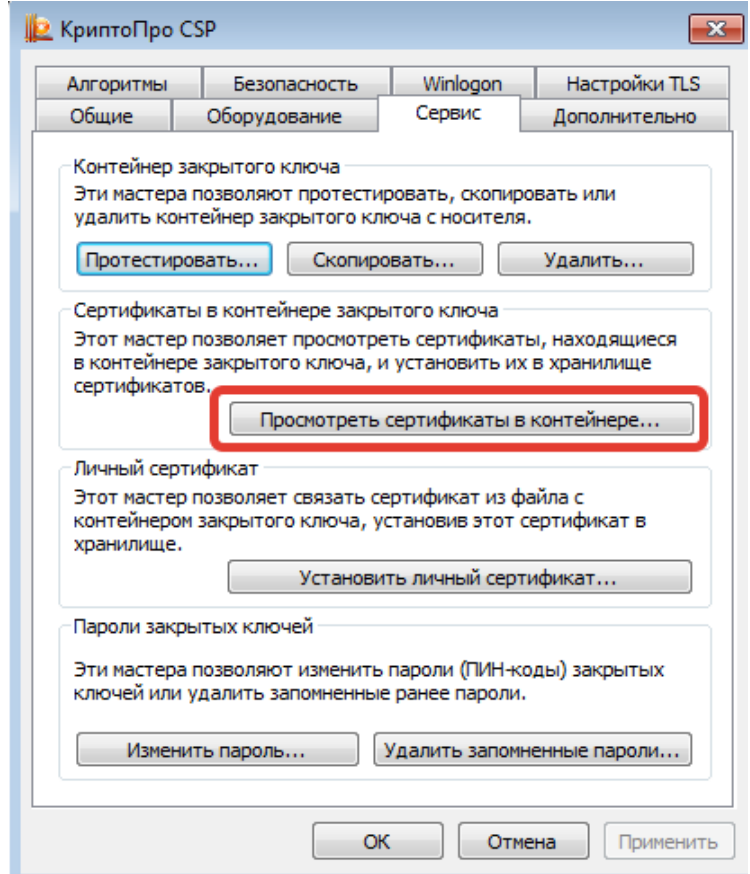
- Драйвер электронного идентификатора RuToken.
Актуальную версию драйвера можно скачать с сайта производителя: <http://www.rutoken.ru/support/download/drivers-for-windows/>
- Криптопровайдер КриптоПро CSP версии 4.0 и выше. Пробную версию программного обеспечения, действительную в течение 90 дней, можно скачать с сайта производителя: <https://www.cryptopro.ru/downloads/>. Для дальнейшего использования необходимо приобрести лицензию.
- Плагин КриптоПро ЭЦП Browser plug-in, позволяющий работать с сертификатом электронной подписи через браузер. Программное обеспечение не требует лицензии, его можно скачать с сайта производителя: https://www.cryptopro.ru/products/cades/plugin/get_2_0

2.2 Установка сертификата электронной подписи

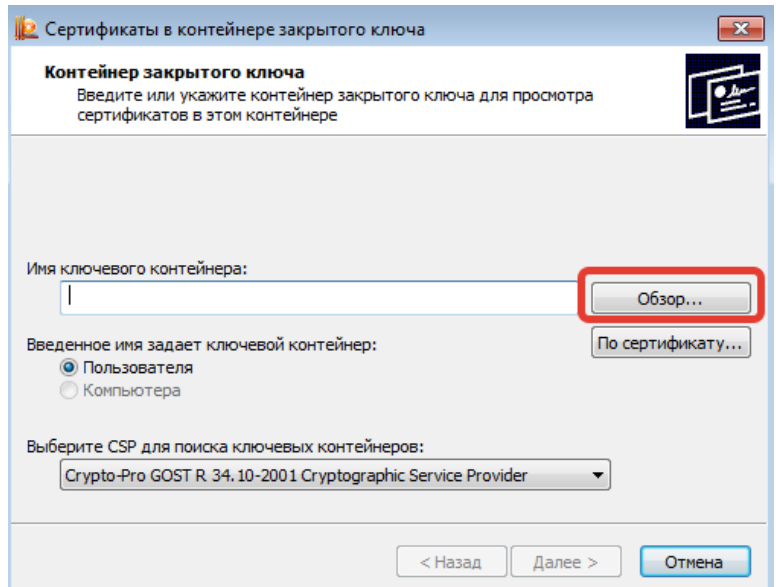
Установка сертификата электронной подписи на клиентское рабочее место выполняется однократно при начале работы. Для установки необходимо произвести следующую последовательность действий:

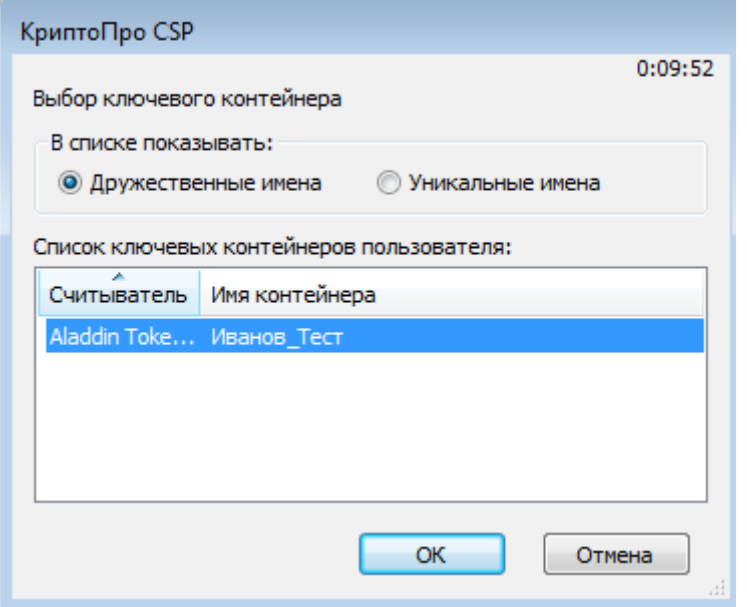
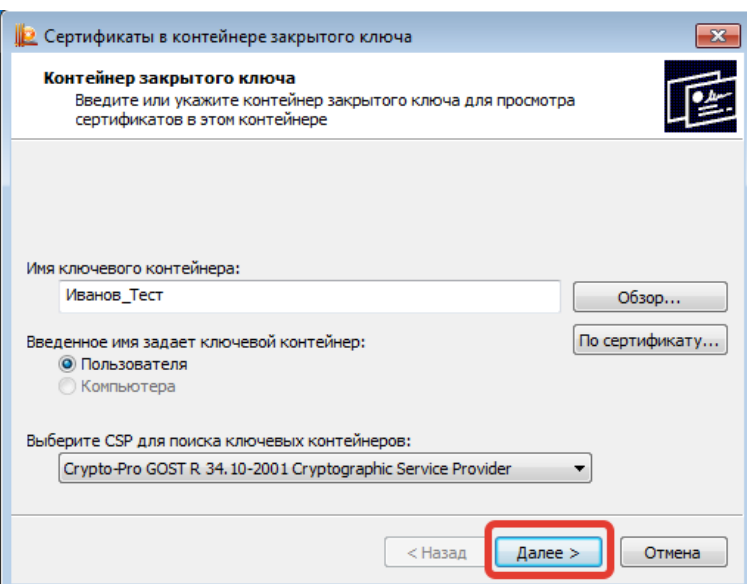
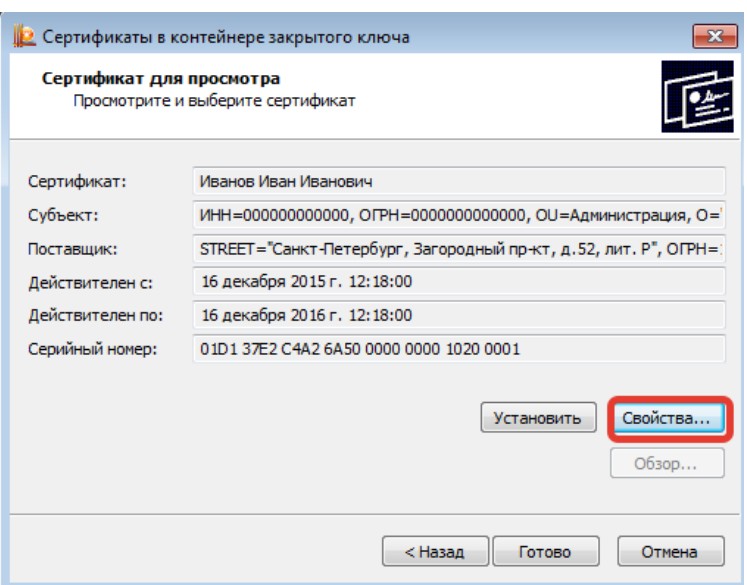
Вставить электронный идентификатор RuToken, на который записан сертификат электронной подписи пользователя, в USB-порт компьютера.	
--	--

Открыть «Крипто-Про CSP».
Перейти на вкладку «Сервис» и выбрать команду «Просмотреть сертификаты в контейнере»

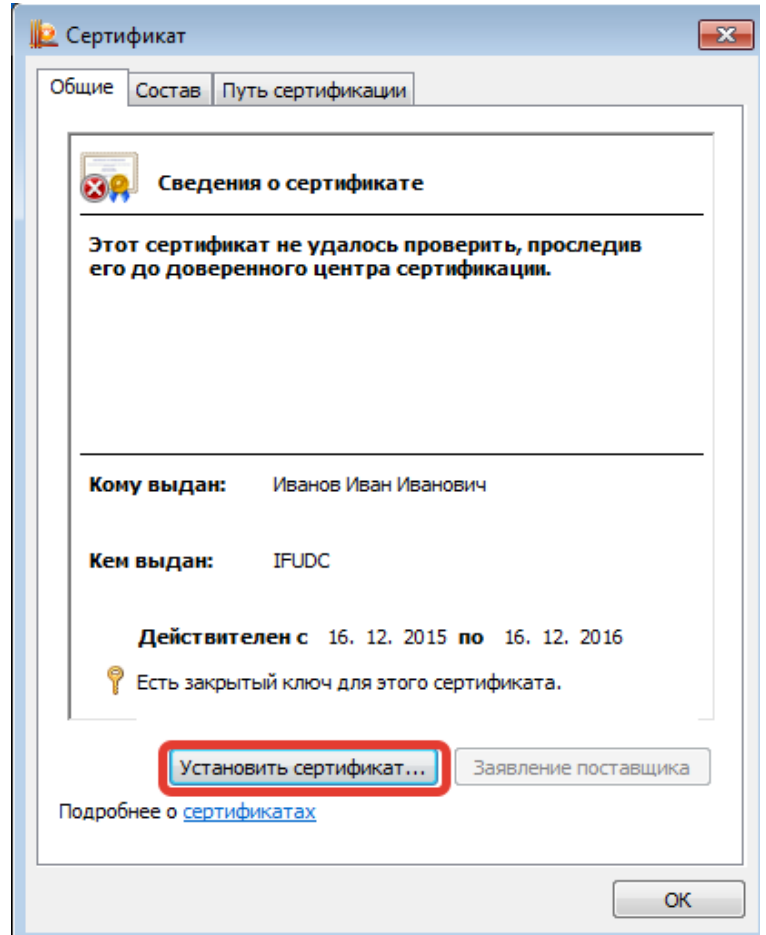


В открывшемся окне нажать кнопку «Обзор» и выбрать вставленный электронный идентификатор. Для подтверждения нажать кнопку «ОК»

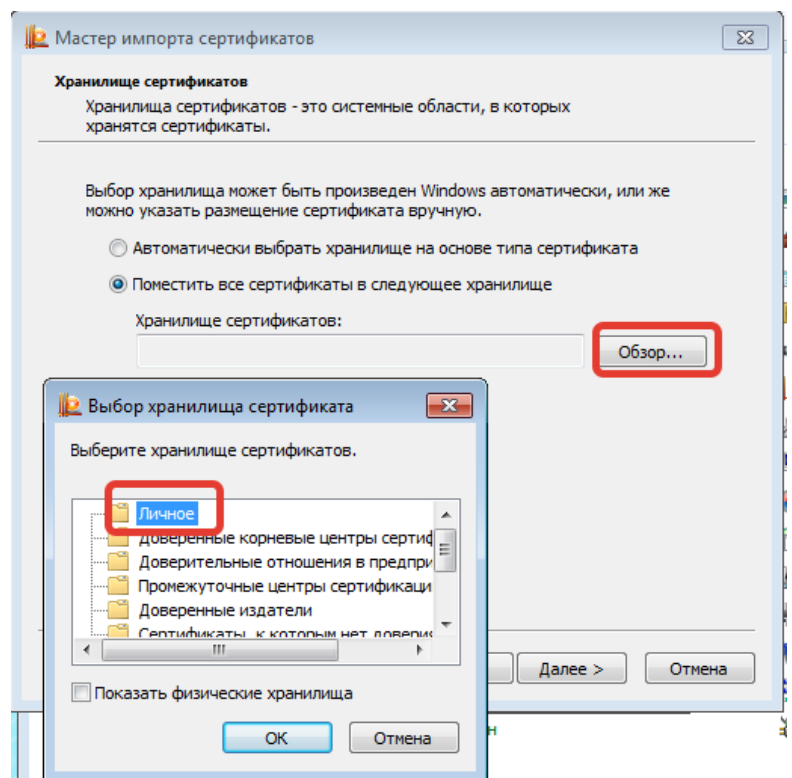


	 <p>КриптоПро CSP 0:09:52</p> <p>Выбор ключевого контейнера</p> <p>В списке показывать: <input checked="" type="radio"/> Дружественные имена <input type="radio"/> Уникальные имена</p> <p>Список ключевых контейнеров пользователя:</p> <table border="1"><thead><tr><th>Считыватель</th><th>Имя контейнера</th></tr></thead><tbody><tr><td>Aladdin Token...</td><td>Иванов_Тест</td></tr></tbody></table> <p>OK Отмена</p>	Считыватель	Имя контейнера	Aladdin Token...	Иванов_Тест
Считыватель	Имя контейнера				
Aladdin Token...	Иванов_Тест				
<p>Нажать кнопку «Далее»</p>	 <p>Сертификаты в контейнере закрытого ключа</p> <p>Контейнер закрытого ключа Введите или укажите контейнер закрытого ключа для просмотра сертификатов в этом контейнере</p> <p>Имя ключевого контейнера: Иванов_Тест Обзор...</p> <p>Введенное имя задает ключевой контейнер: <input checked="" type="radio"/> Пользователя <input type="radio"/> Компьютера По сертификату...</p> <p>Выберите CSP для поиска ключевых контейнеров: Crypto-Pro GOST R. 34.10-2001 Cryptographic Service Provider</p> <p>< Назад Далее > Отмена</p>				
<p>В окне «Сертификат для просмотра» нажать кнопку «Свойства»</p>	 <p>Сертификаты в контейнере закрытого ключа</p> <p>Сертификат для просмотра Просмотрите и выберите сертификат</p> <p>Сертификат: Иванов Иван Иванович</p> <p>Субъект: ИНН=000000000000, ОГРН=0000000000000, OU=Администрация, О=</p> <p>Поставщик: STREET="Санкт-Петербург, Загородный пр-кт, д.52, лит. Р", ОГРН=</p> <p>Действителен с: 16 декабря 2015 г. 12:18:00</p> <p>Действителен по: 16 декабря 2016 г. 12:18:00</p> <p>Серийный номер: 01D1 37E2 C4A2 6A50 0000 0000 1020 0001</p> <p>Установить Свойства... Обзор...</p> <p>< Назад Готово Отмена</p>				

В окне «Сертификат» нажать кнопку «Установить сертификат»



Выбрать хранилище сертификатов «Личное», нажать на кнопку «Далее». После установки сертификата Система выдаст сообщение об успешном импорте.

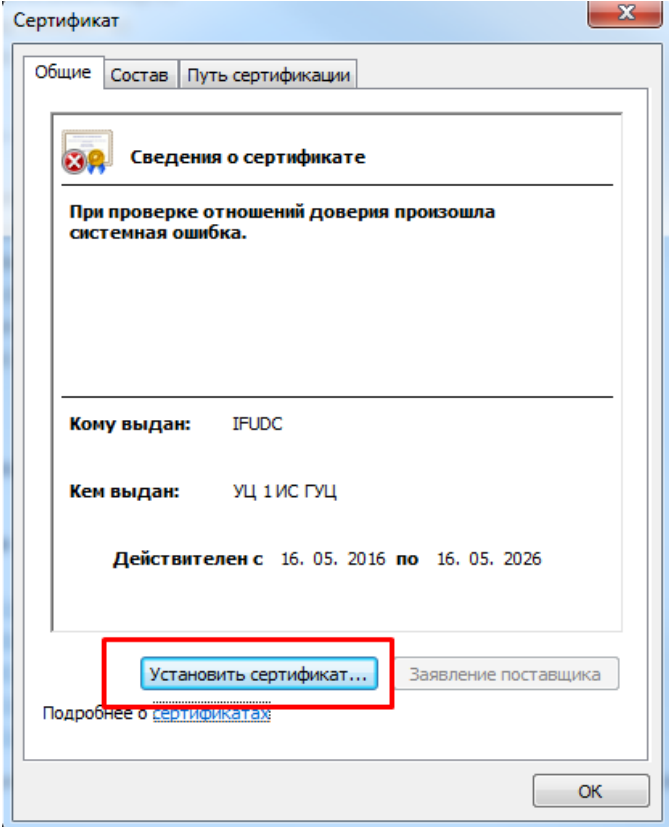
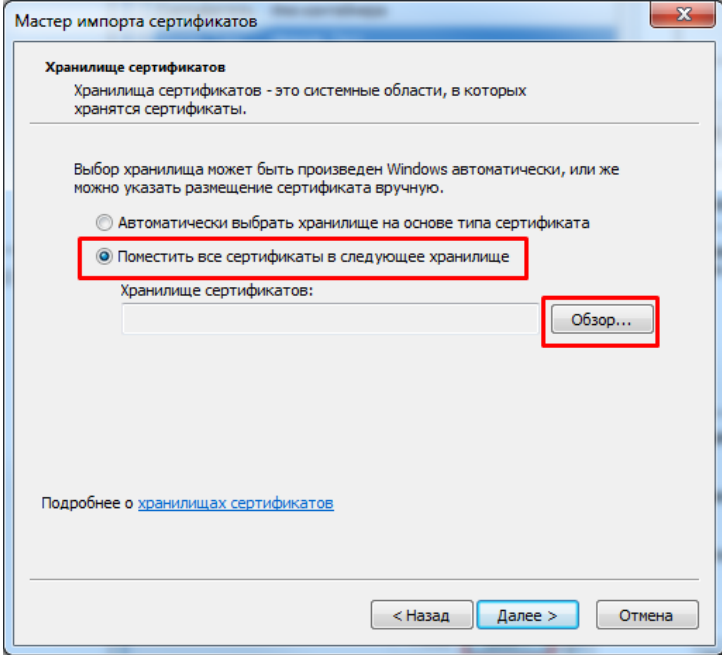


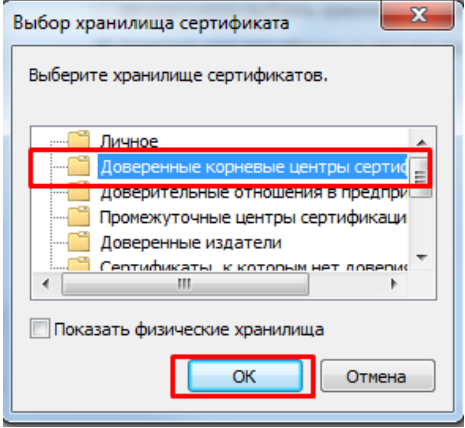
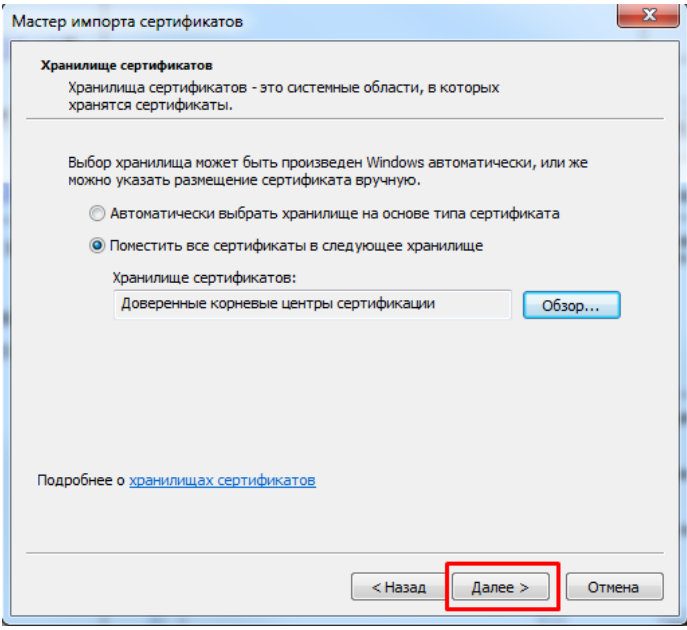
Закрывать все окна Крипто-Про

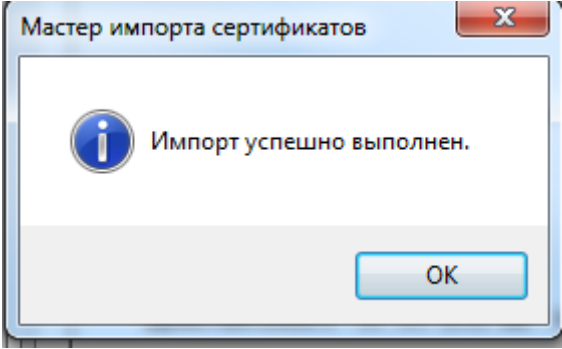
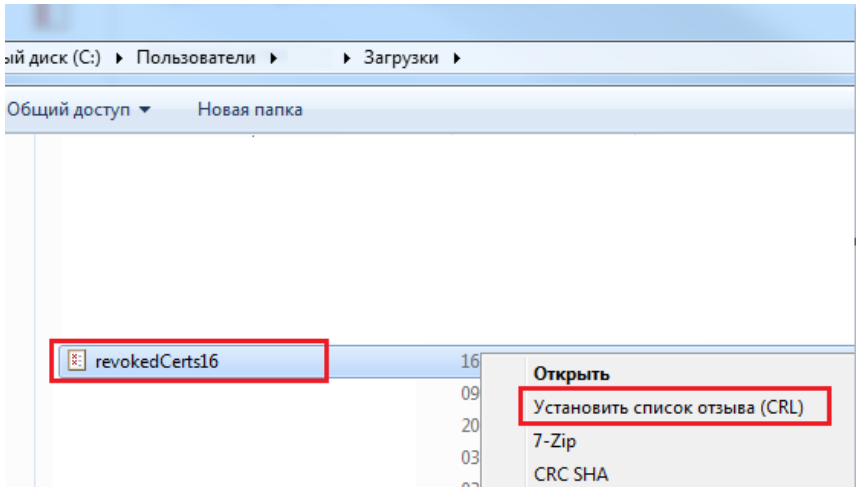
2.3 Установка корневого сертификата Удостоверяющего центра

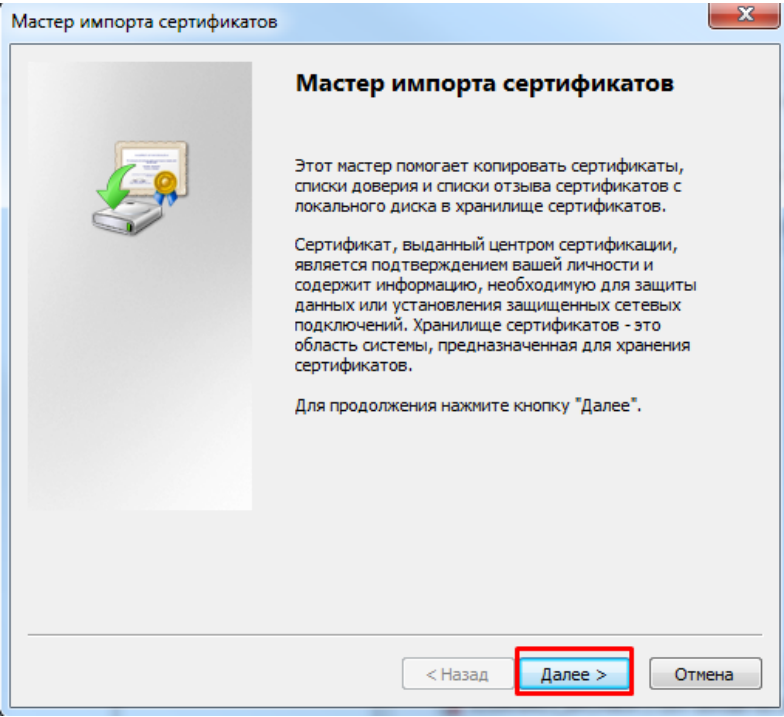
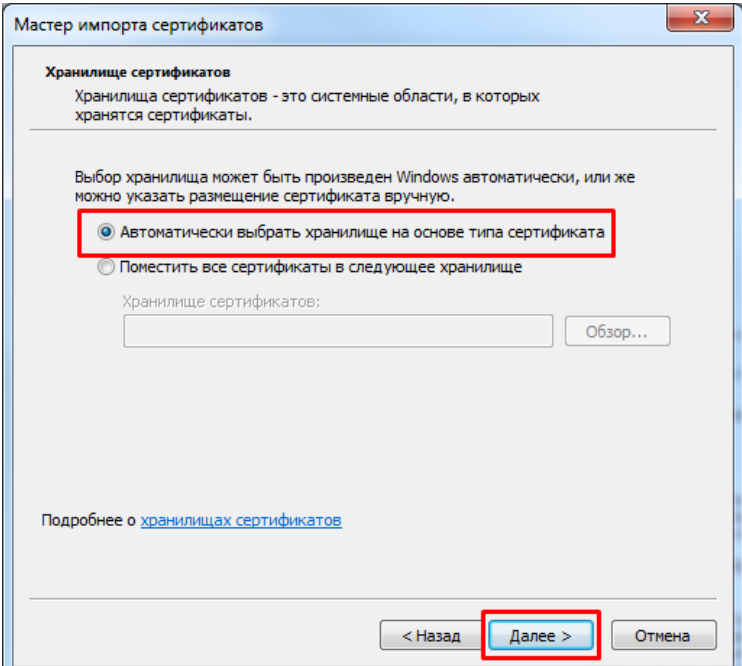
Установка корневых сертификатов Удостоверяющего центра на клиентское рабочее место выполняется однократно при начале работы. Для установки необходимо произвести следующую последовательность действий:

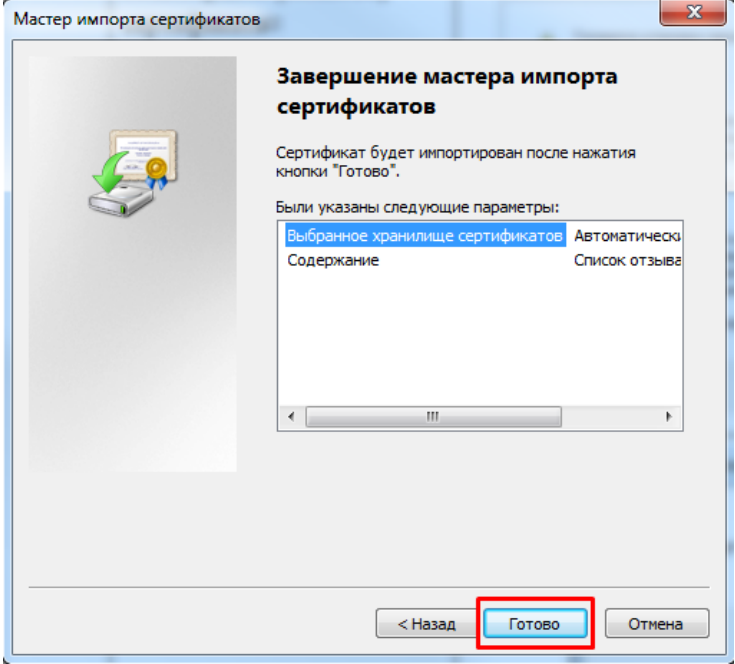
Скачать набор сертификатов Удостоверяющего центра, используя следующие ссылки:	
Для сертификатов по ГОСТ Р 34.10-2001 (выданные до 09.04.2019)	<ul style="list-style-type: none">• https://www.if-spb.ru/files/IFUDC182.crt (корневой сертификат удостоверяющего центра)• http://www.if-spb.ru/files/guc.cer (корневой сертификат головного удостоверяющего центра Минкомсвязи РФ)• https://www.if-spb.ru/files/revokedCerts182.crl (список отозванных сертификатов)
Для сертификатов, по ГОСТ Р 34.10-2012 (выданные после 09.04.2019)	<ul style="list-style-type: none">• https://www.if-spb.ru/files/IFUDC183.crt (корневой сертификат удостоверяющего центра)• https://www.if-spb.ru/files/mincom_gost_2012.cer (корневой сертификат головного удостоверяющего центра Минкомсвязи РФ)• https://www.if-spb.ru/files/revokedCerts183.crl (список отозванных сертификатов)

<p>Запустить первый файл, в открывшемся окне «Сертификат» нажать кнопку «Установить сертификат»</p>	
<p>Выбрать пункт «Поместить все сертификаты в следующее хранилище», нажать кнопку «Обзор»</p>	

<p>Выбрать хранилище сертификатов «Доверенные корневые центры сертификации», нажать кнопку «ОК»</p>	
<p>Нажать кнопку «Далее»</p>	
<p>Подтвердить установку сертификата</p>	

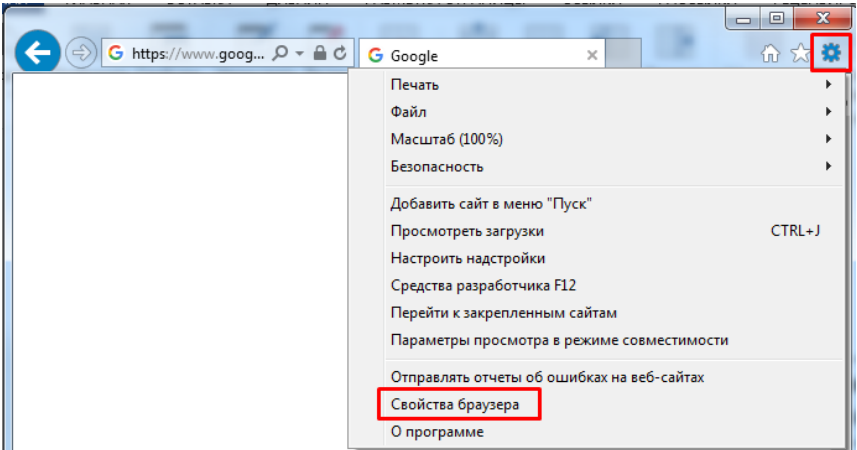
<p>Закрывать все окна Мастера импорта сертификатов</p>	
<p>Повторить вышеописанную последовательность действий для установки второго сертификата</p>	
<p>Открыть загруженный файл «Список отозванных сертификатов» в Проводнике, нажать на нем правой клавишей мыши, выбрать пункт меню «Установить список отзыва (CRL)»</p>	

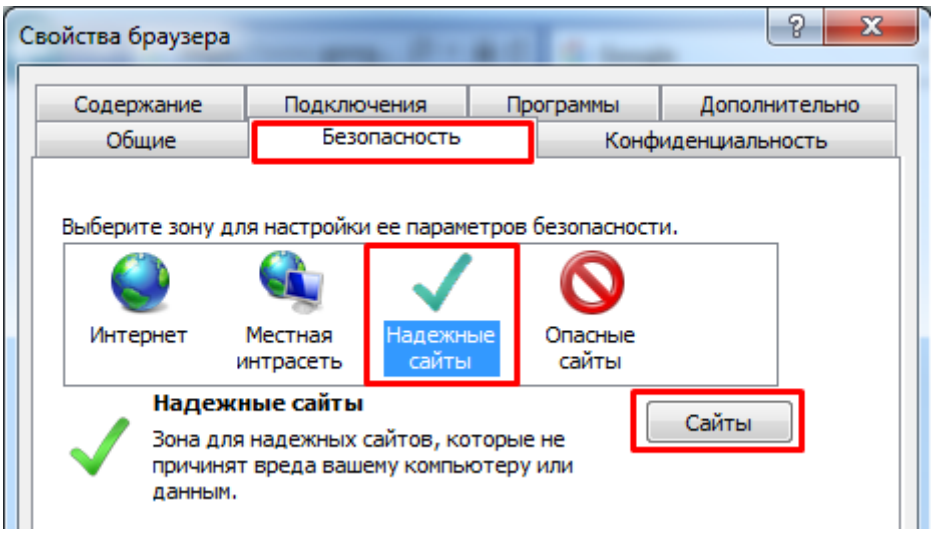
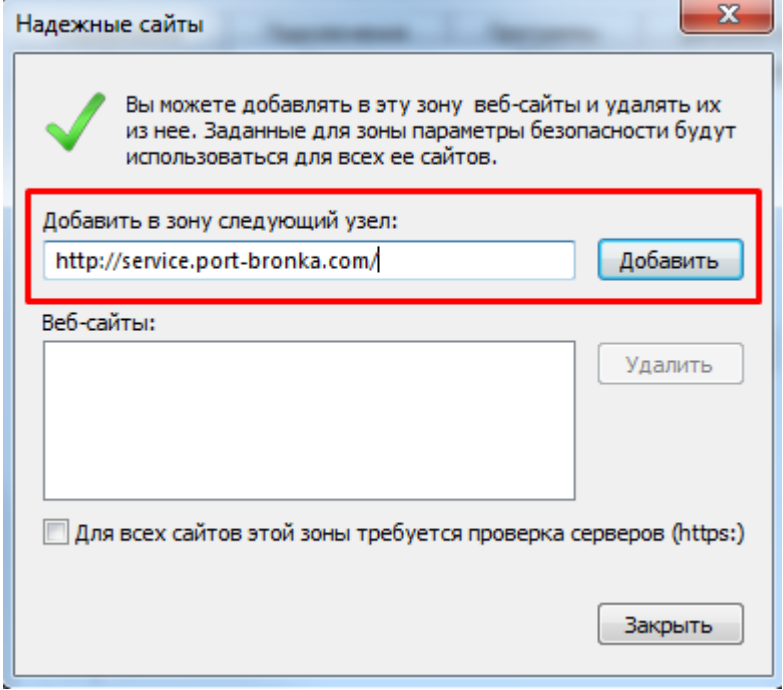
<p>В открывшемся окне Мастера импорта сертификатов нажать «Далее»</p>	
<p>Выбрать пункт «Автоматически выбрать хранилище на основе типа сертификата», нажать «Далее»</p>	

Подтвердить установку	
Закрывать все окна мастера импорта сертификатов	

2.4 Настройка браузера

Для корректной работы алгоритма криптографической защиты информации с использованием сертификата электронной подписи необходимо настроить браузер на клиентской рабочей станции. Требуется произвести следующую последовательность действий:

Открыть Internet Explorer	
Перейти в раздел «Настройки» - «Свойства браузера»	

<p>Открыть закладку «Безопасность», выделить значок «Надежные сайты», нажать кнопку «Сайты»</p>	
<p>Добавить адрес http://service.port-bronka.com/ в список надежных сайтов</p>	
<p>Закрывать все окна Internet Explorer</p>	