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

Санкт-Петербург

2019

СОДЕРЖАНИЕ

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

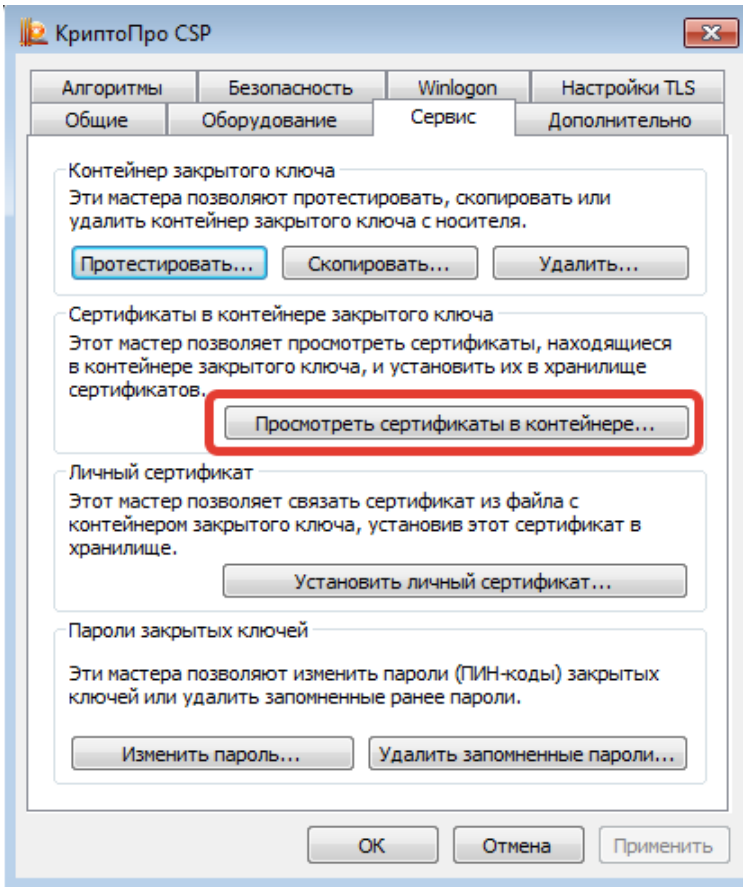
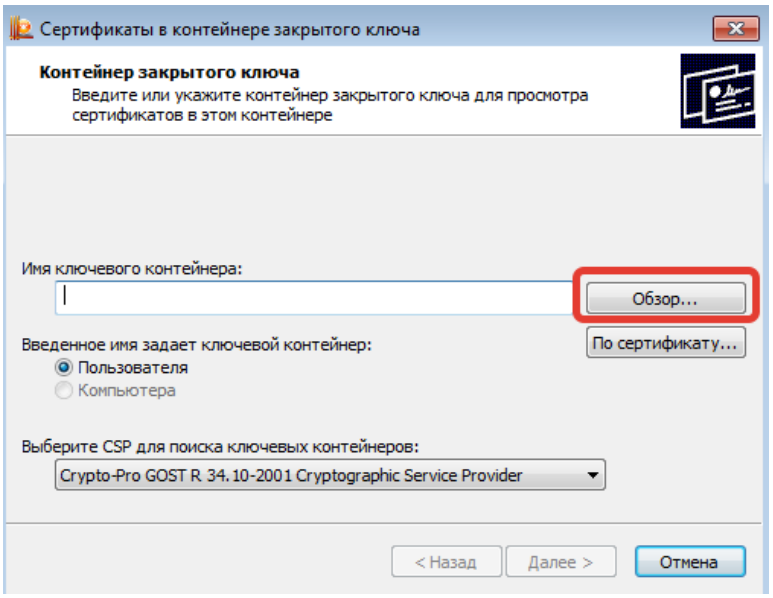
Для использования алгоритмов криптографической защиты информации с использованием сертификата электронной подписи на клиентской рабочей станции должно быть установлено следующее базовое программное обеспечение:

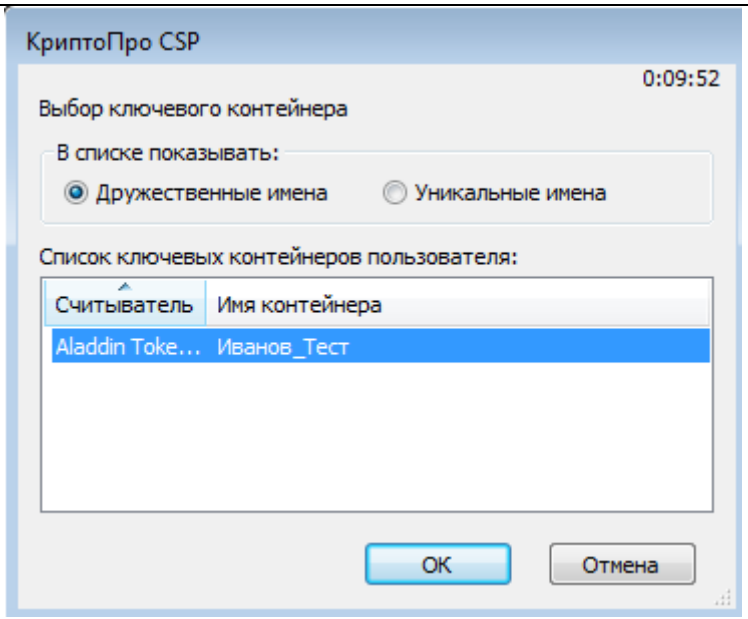
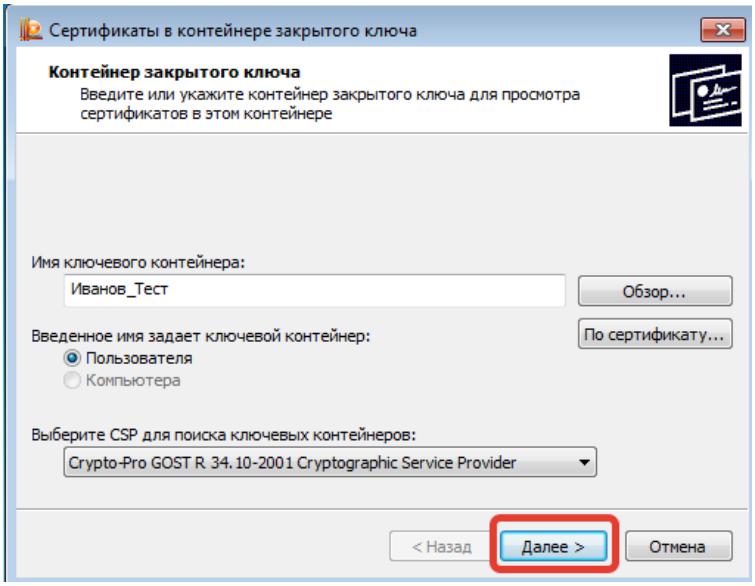
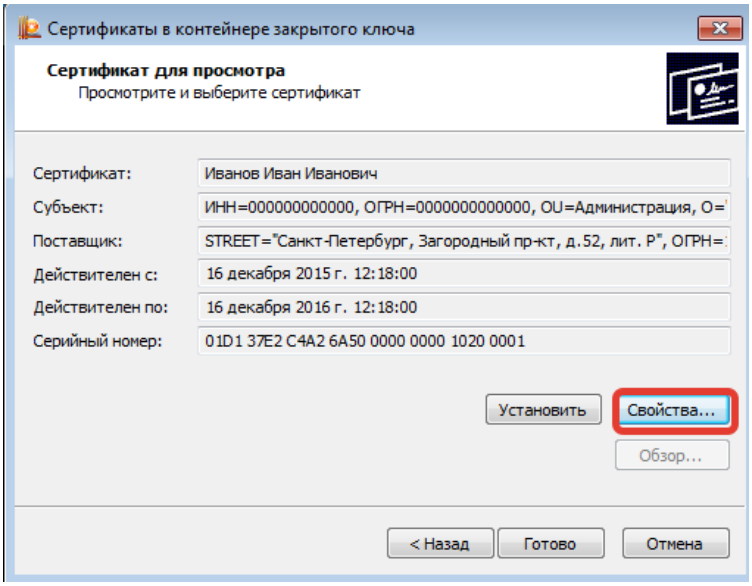
- Драйвер электронного идентификатора RuToken.
  Актуальную версию драйвера можно скачать с сайта производителя: http://www.rutoken.ru/support/download/drivers-for-windows/
- Криптопровайдер КриптоПро CSP версии 4.0 и выше. Пробную версию программного обеспечения, действительную в течение 90 дней, можно 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

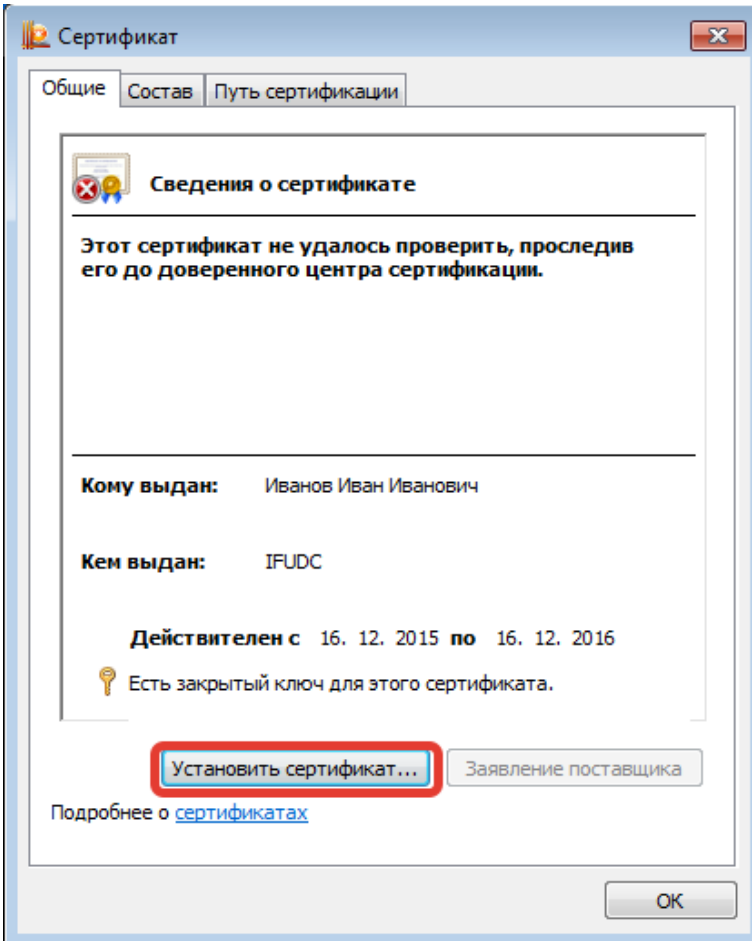
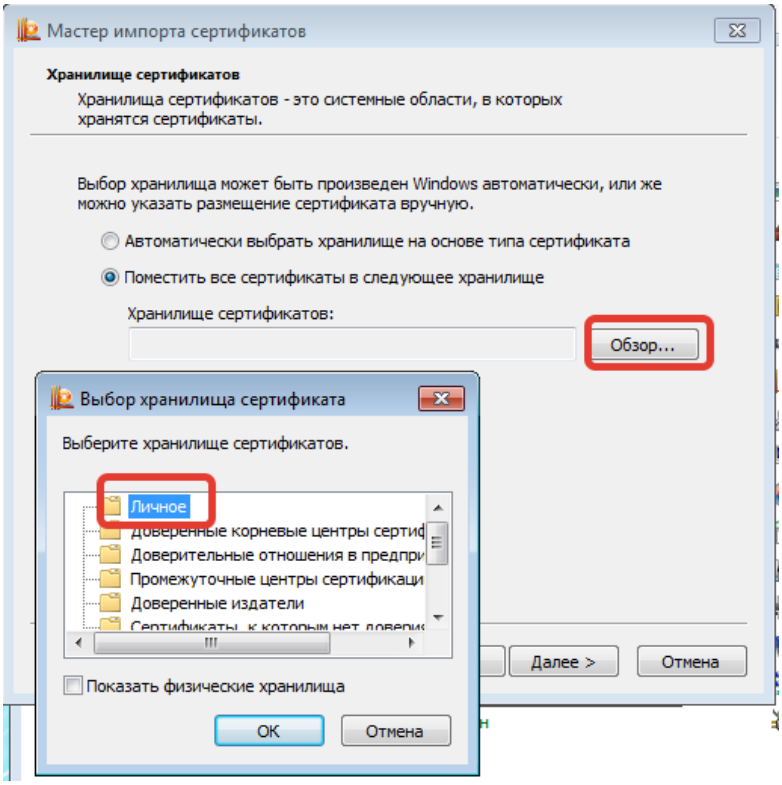
2.2 Установка сертификата электронной подписи

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»	

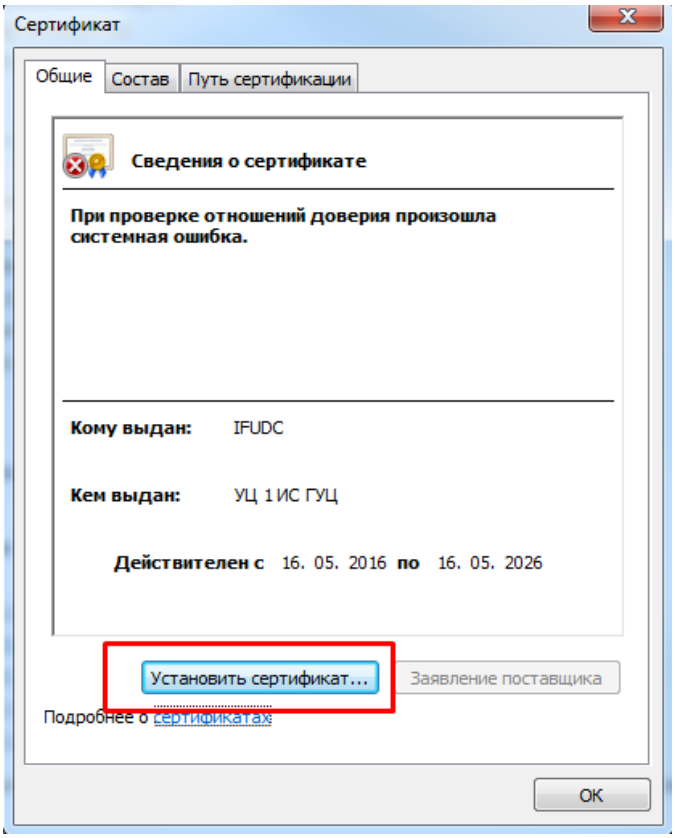
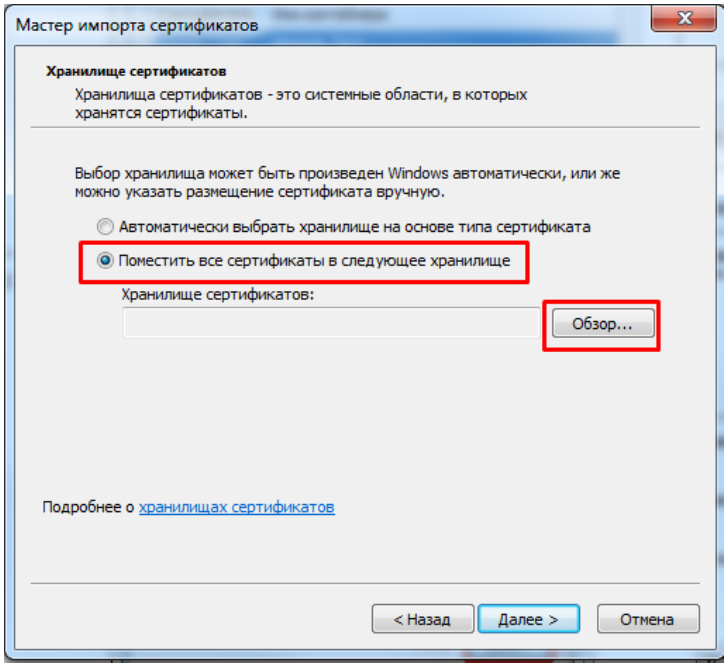
	
Нажать кнопку «Далее»	
В окне «Сертификат для просмотра» нажать кнопку «Свойства»	

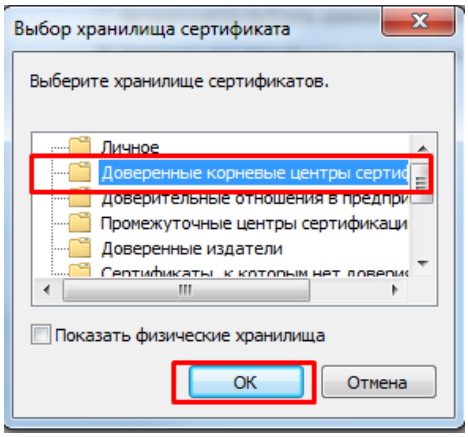
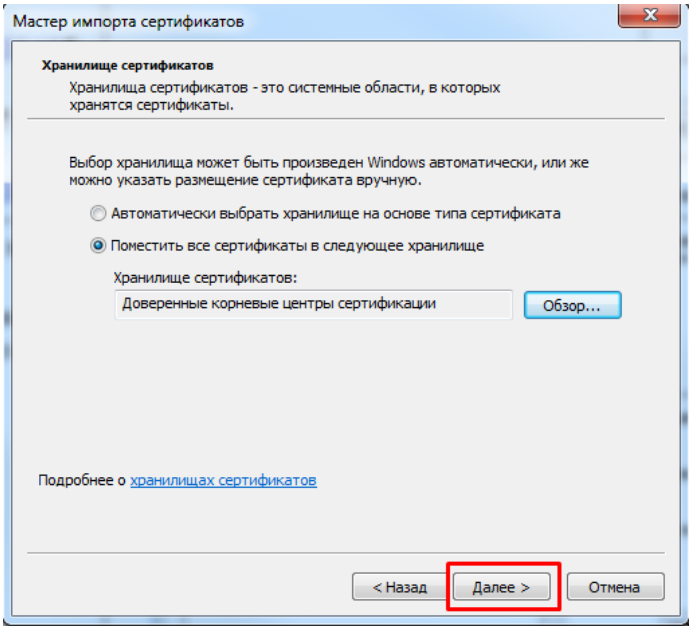
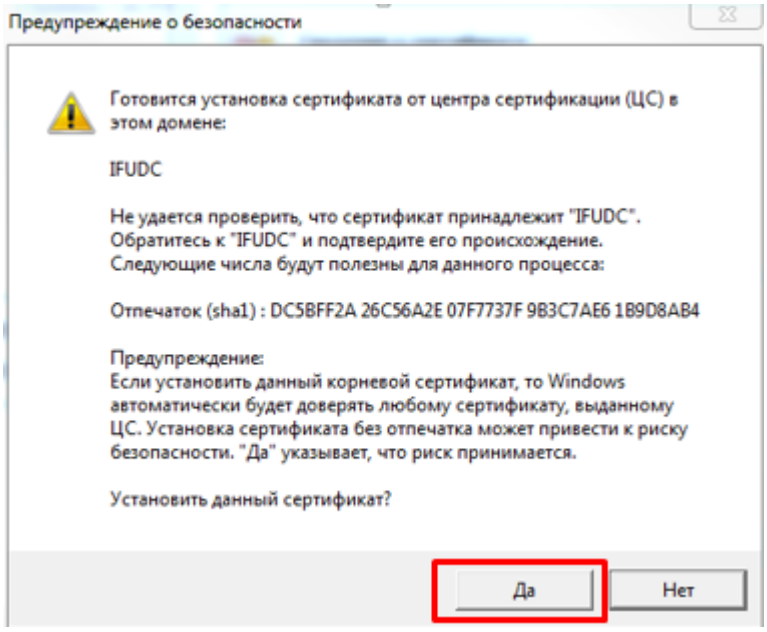
В окне «Сертификат» нажать кнопку «Установить сертификат»	
Выбрать хранилище сертификатов «Личное», нажать на кнопку «Далее». После установки сертификата Система выдаст сообщение об успешном импорте.	
Закрыть все окна Крипто-Про	

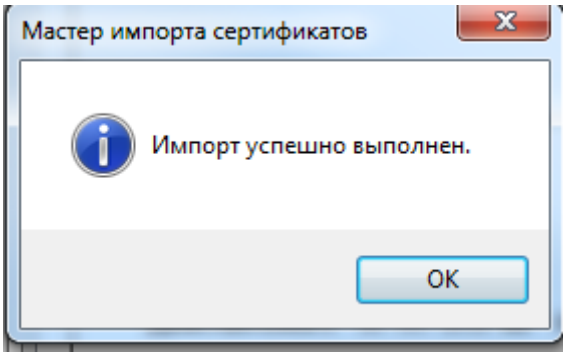
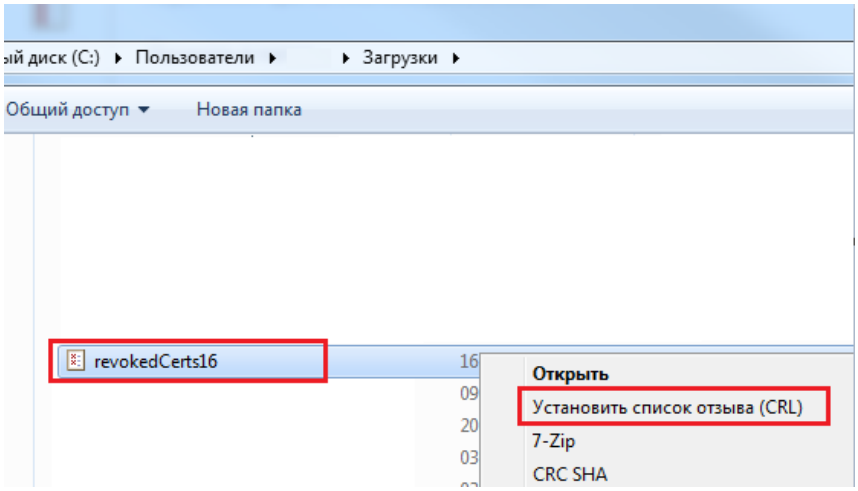
2.3 Установка корневого сертификата Удостоверяющего центра

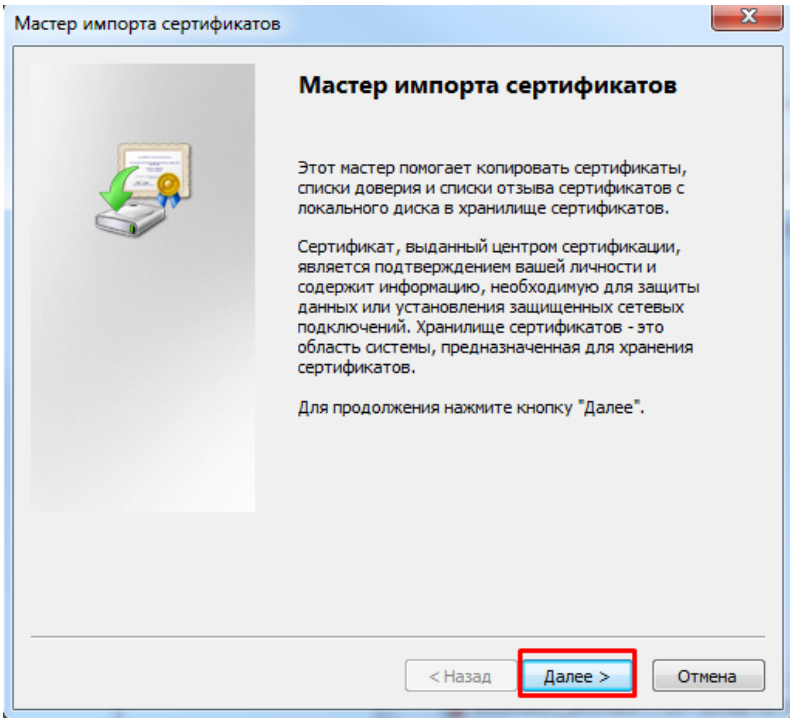
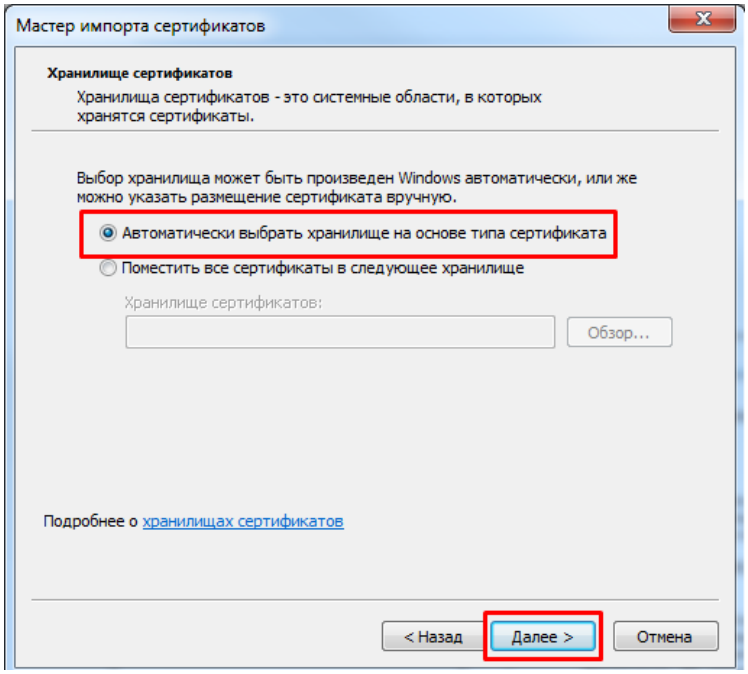
Установка корневых сертификатов Удостоверяющего центра на клиентское рабочее место выполняется однократно при начале работы. Для установки необходимо произвести следующую последовательность действий:

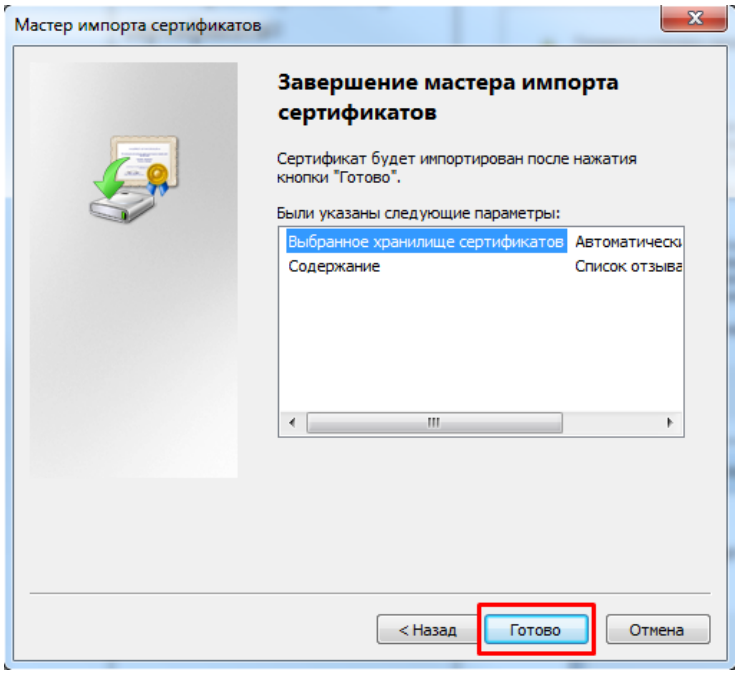
Скачать набор сертификатов Удостоверяющего центра, используя следующие ссылки:	
Для сертификатов по ГОСТ Р 34.10-2001 (выданные до 09.04.2019)	• https://www.if-spb.ru/files/IFUDC182.crt (корневой сертификат удостоверяющего центра) • http://www.if-spb.ru/files/guc.cer (корневой сертификат головного удостоверяющего 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)	• 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)

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

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

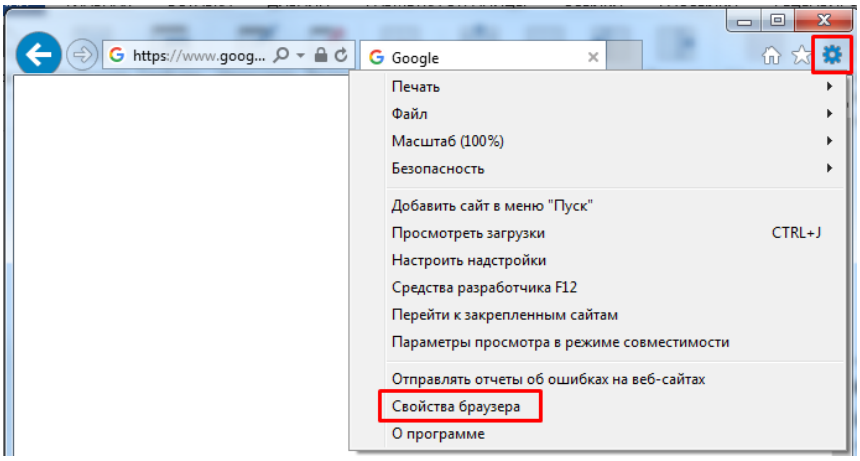
Закрыть все окна Мастера импорта сертификатов	
Повторить вышеописанную последовательность действий для установки второго сертификата	
Открыть загруженный файл «Список отозванных сертификатов» в Проводнике, нажать на нем правой клавишей мыши, выбрать пункт меню «Установить список отзыва (CRL)»	

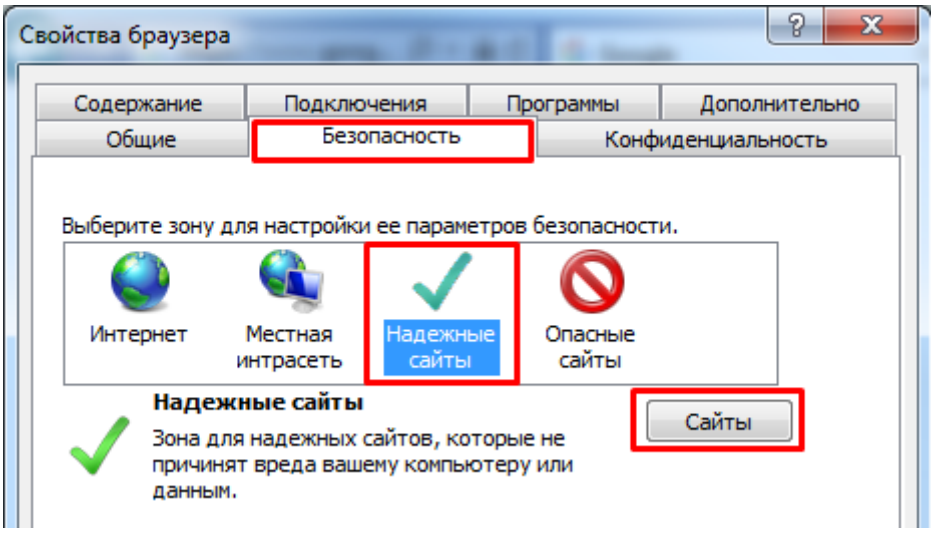
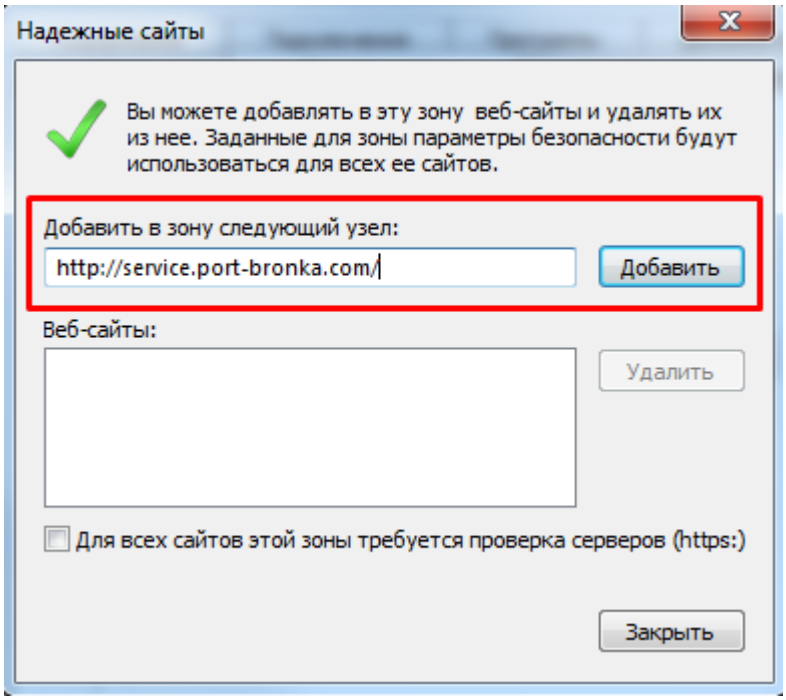
В открывшемся окне Мастера импорта сертификатов нажать «Далее»	
Выбрать пункт «Автоматически выбрать хранилище на основе типа сертификата», нажать «Далее»	

Подтвердить установку	
Закрыть 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»	

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