

Введение

Данная инструкция представляет собой пошаговое руководство по использованию программного обеспечения рабочих станций для защищенного подключения к сетевым ресурсам МИИТ через сеть Интернет с использованием цифровых сертификатов, хранящихся на носителях Aladdin eToken.

При составлении руководства использовались следующие программное и аппаратное обеспечение:

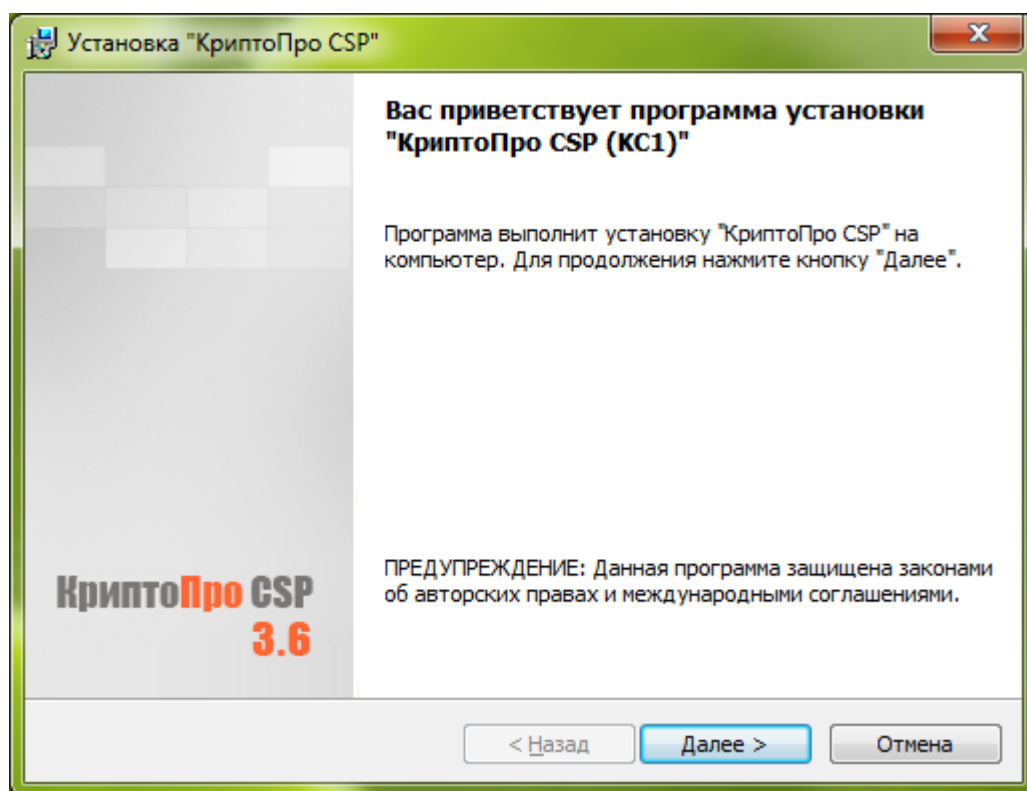
Наименование	Версия
Шлюз удаленного доступа Check Point Connectra 9072	R66.1 с поддержкой алгоритмов шифрования по ГОСТ
Криптопровайдер КриптоПро CSP	3.6.1 KC1 (русская версия)
Носители Aladdin eToken	PRO 72k (Java)
ПО eToken PKI Client	5.1.x SP1
ОС Microsoft Windows	7 Корпоративная

Веб-портал Connectra должен позволять пользователям проходить аутентификацию по сертификату, хранящемуся на eToken, с дальнейшим построением защищенного туннеля (с использованием отечественных алгоритмов шифрования) для доступа к ресурсам сети МИИТ.

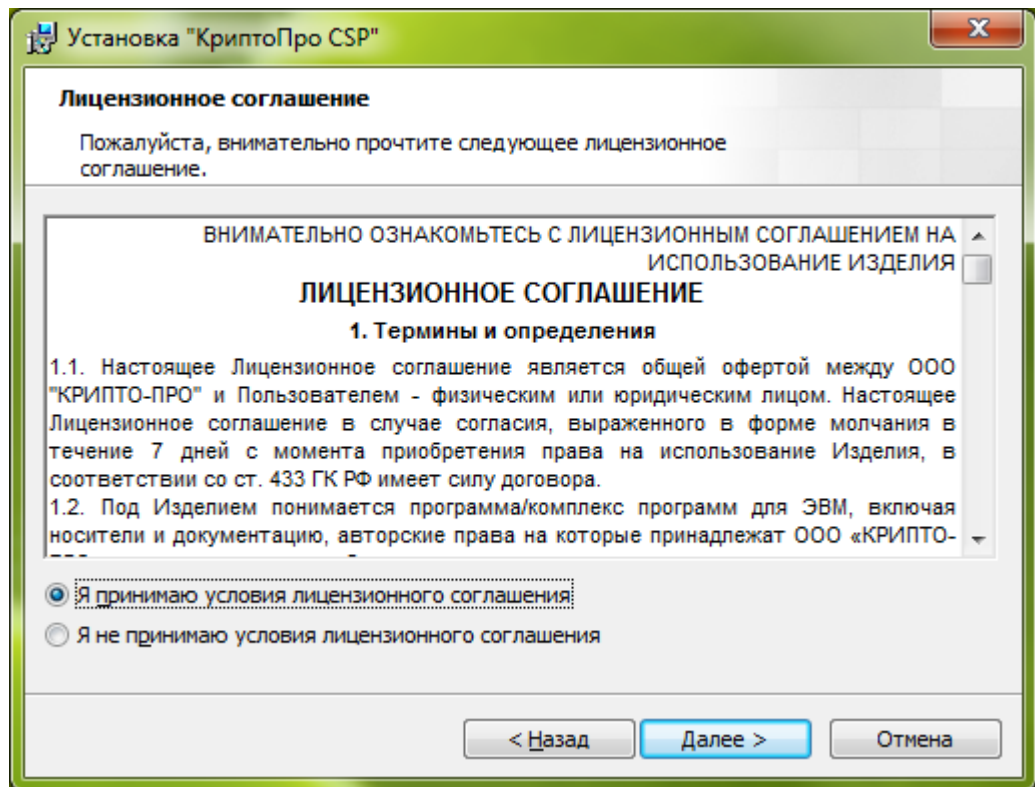
Установка и настройка ПО

Установка КриптоПро CSP

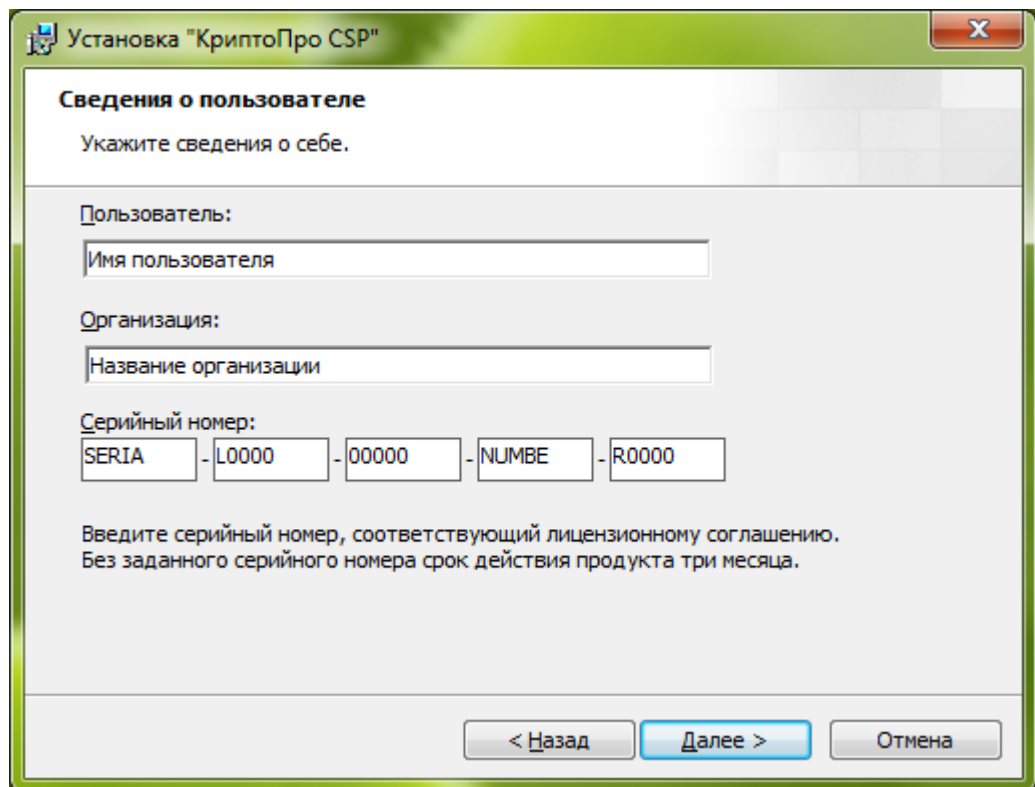
1. Запустите файл дистрибутива КриптоПро CSP.



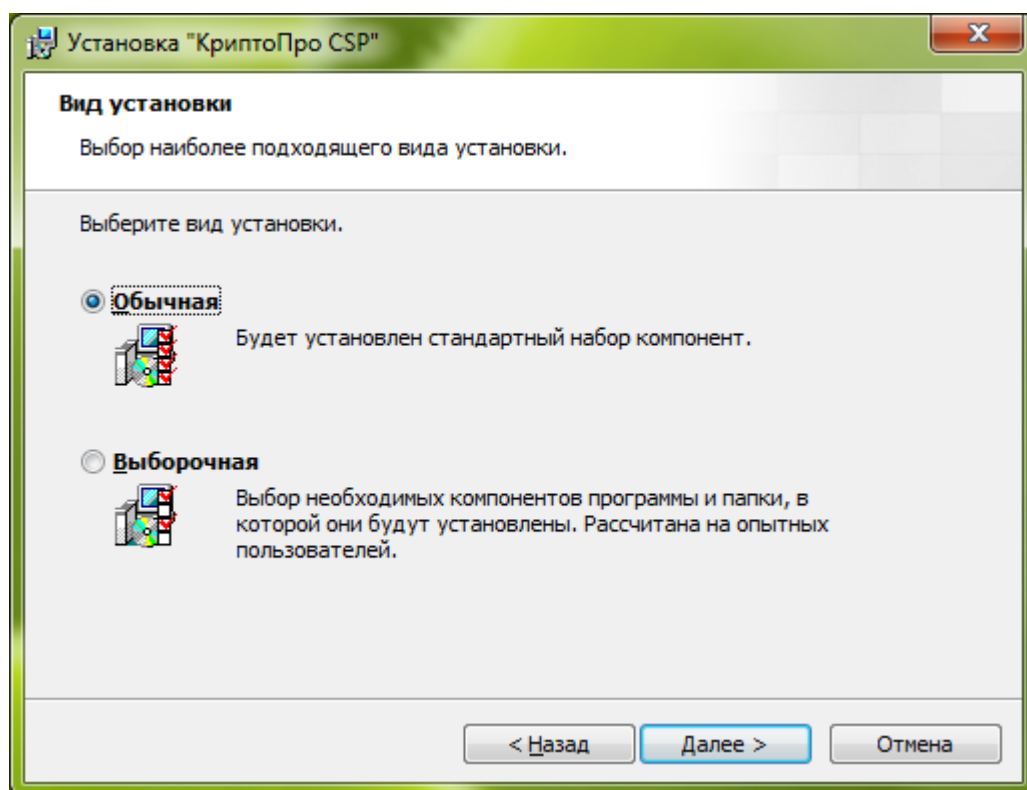
2. Ознакомьтесь с лицензией на программное обеспечение КриптоПро CSP и выразите свое согласие с ней, выбрав пункт «Я принимаю условия лицензионного соглашения».



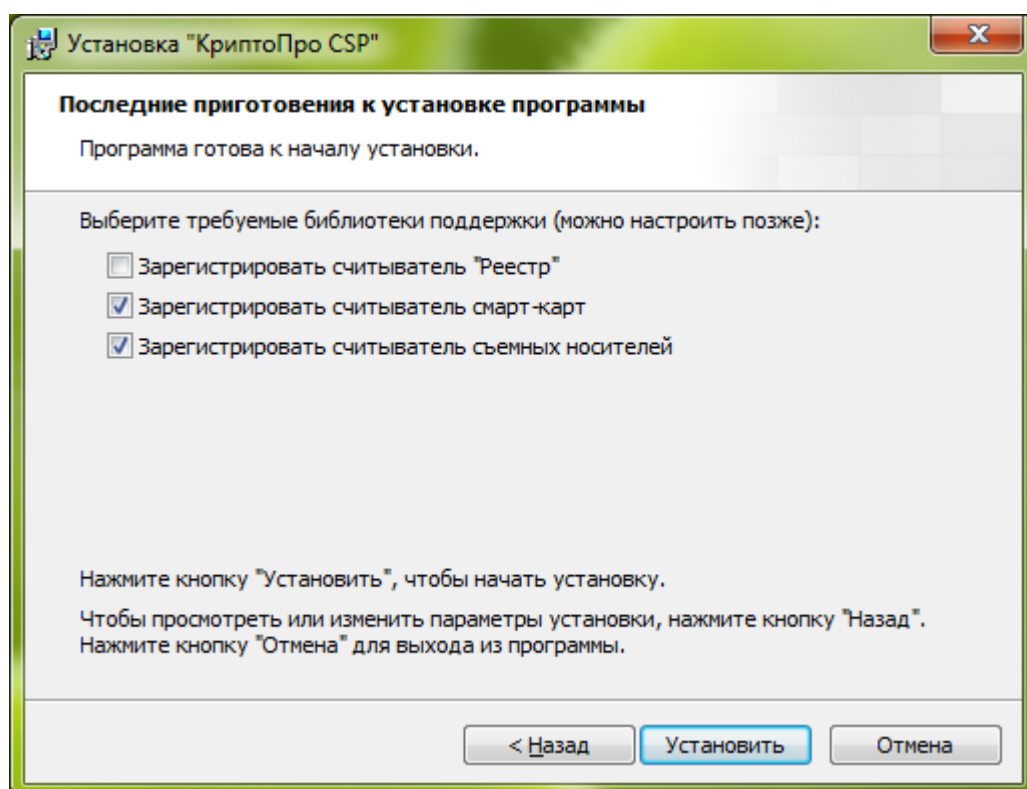
3. Введите сведения о себе и серийный номер лицензии на КриптоПро CSP.



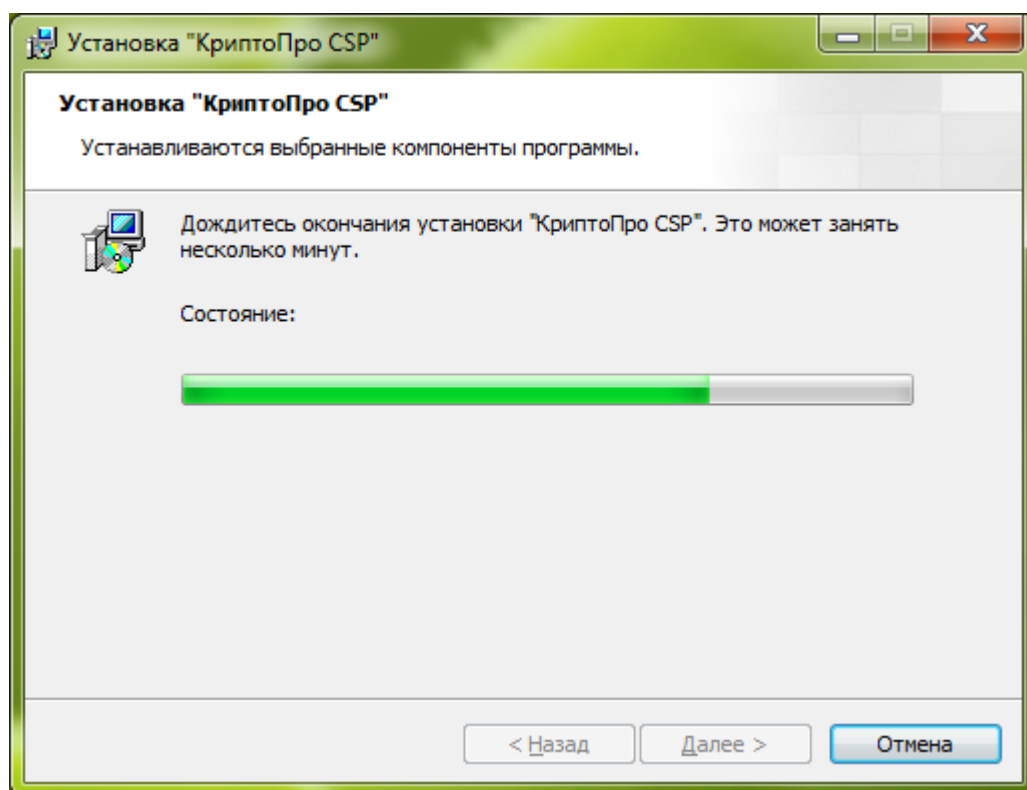
4. Выберите тип установки – «обычная».



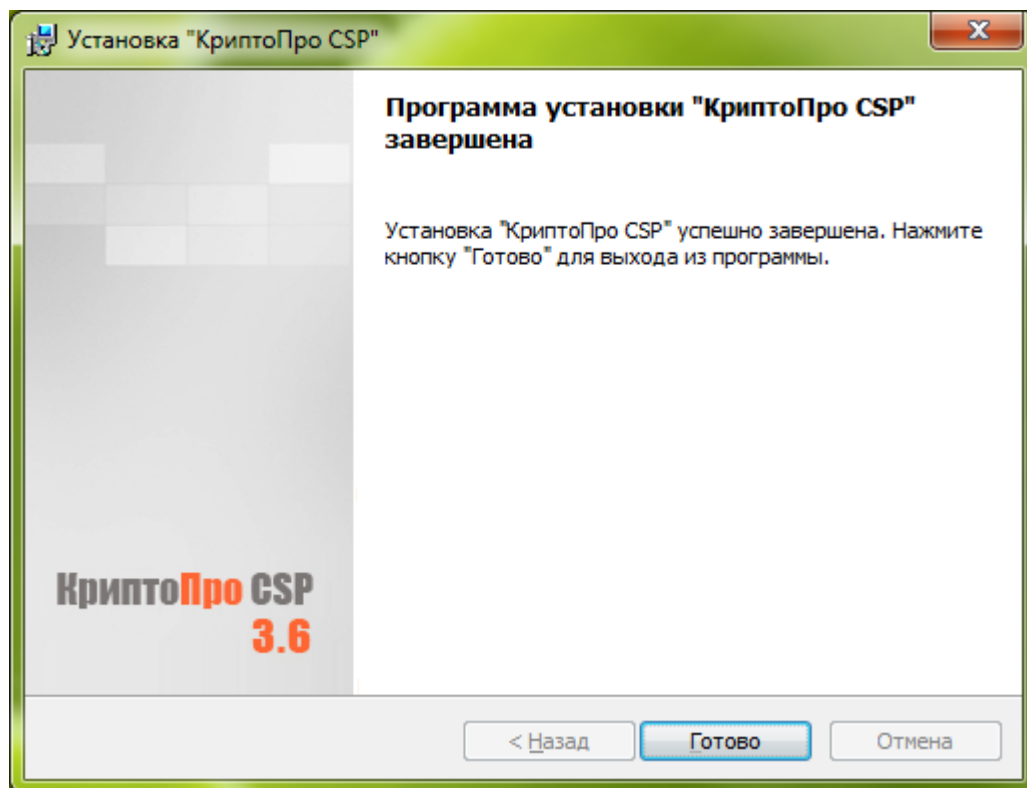
5. Выберите пункты «Зарегистрировать считыватель смарт-карт» и «Зарегистрировать считыватель съемных носителей».

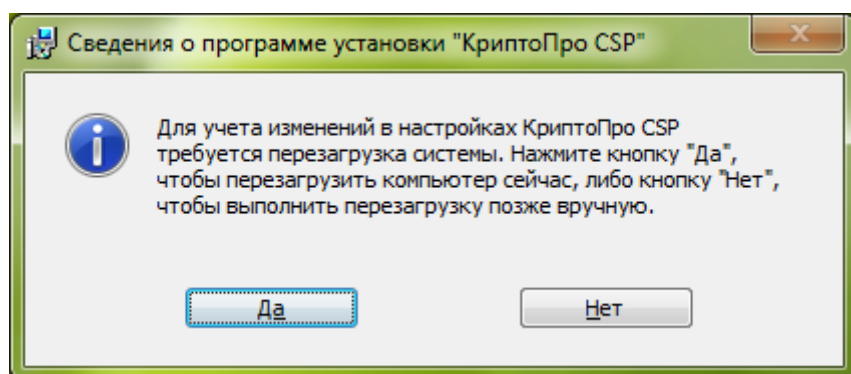


6. Затем начнется процесс установки программного обеспечения.



- После установки Вам будет предложено перезагрузить компьютер. Согласитесь, либо откажитесь и перезагрузитесь самостоятельно позже, до начала использования КриптоПро CSP. Рекомендуется перезагрузиться сразу.

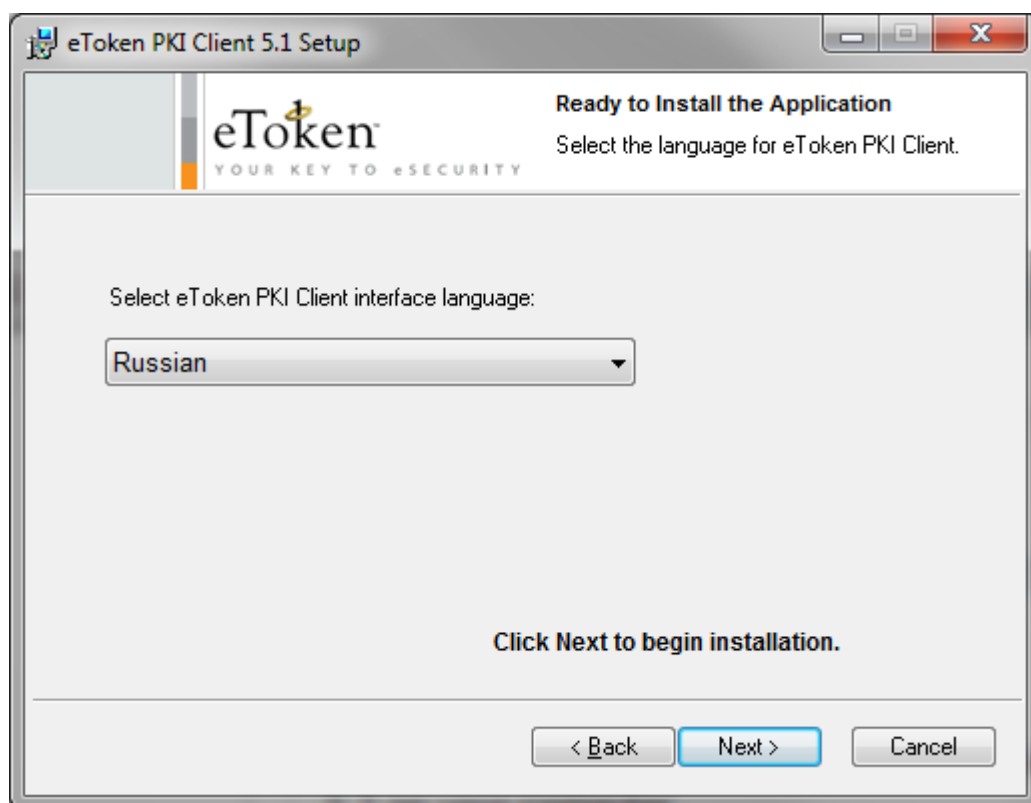
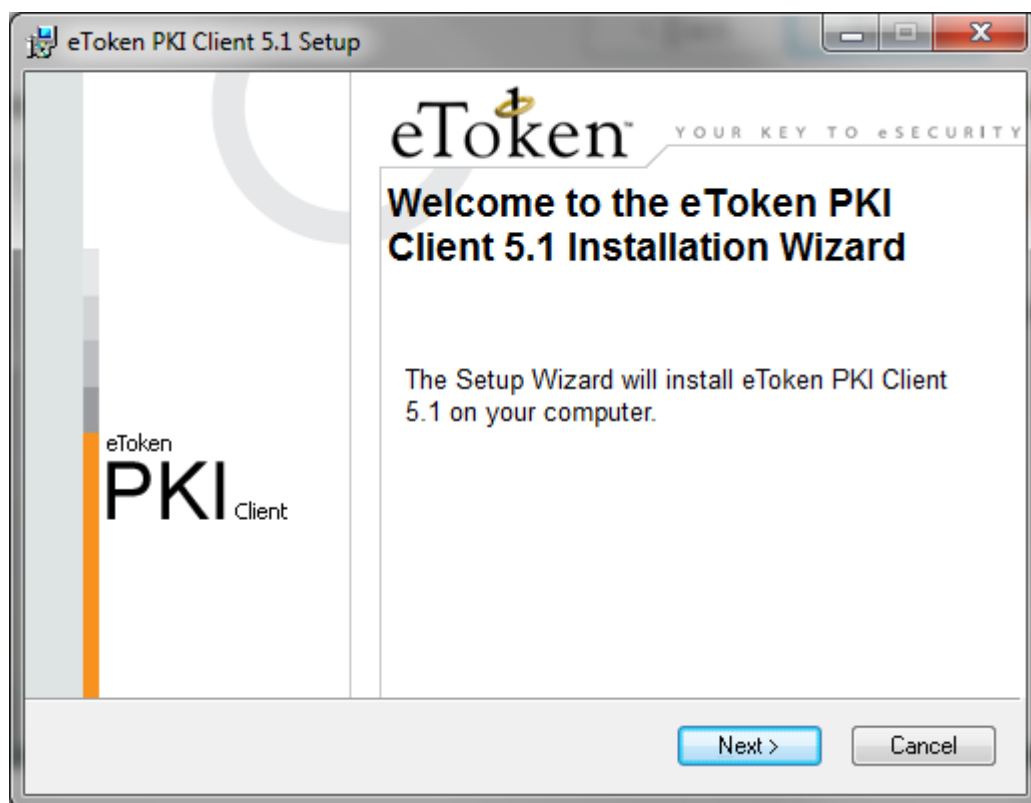




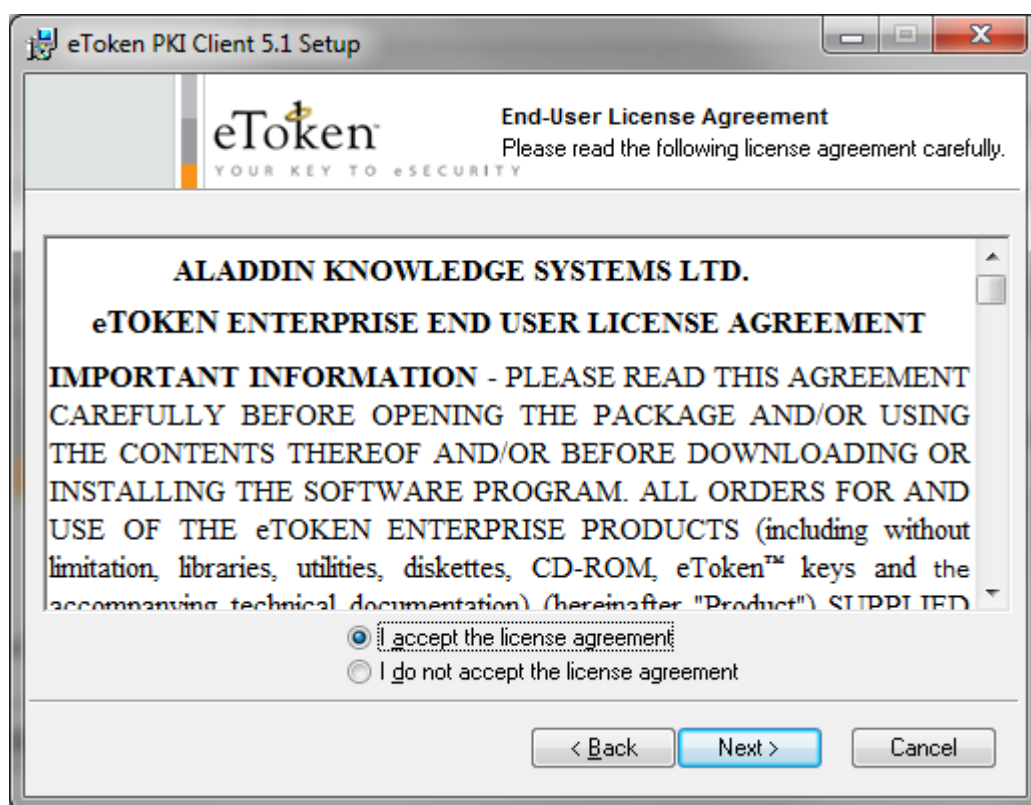
8. После перезагрузки ПО КриптоПро CSP готово к использованию.

Установка eToken PKI Client

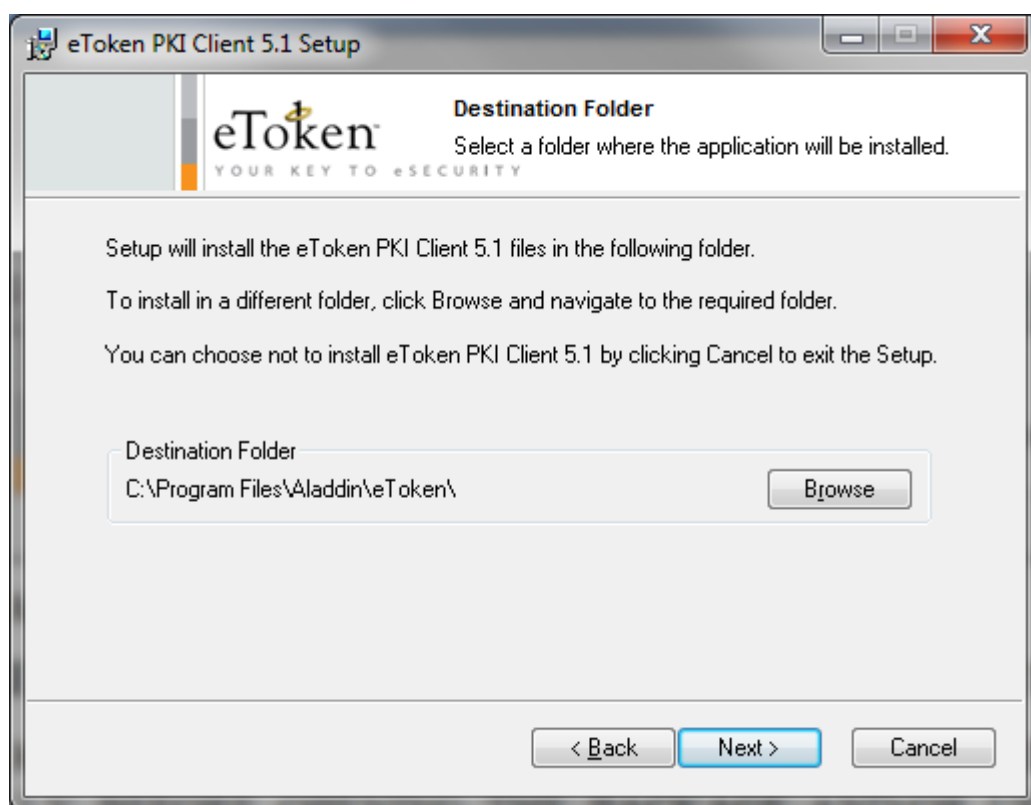
1. Запустите файл дистрибутива eToken PKI Client. Вам будет предложено выбрать язык интерфейса установки. Выберите один из предложенных языков (далее используется русский).



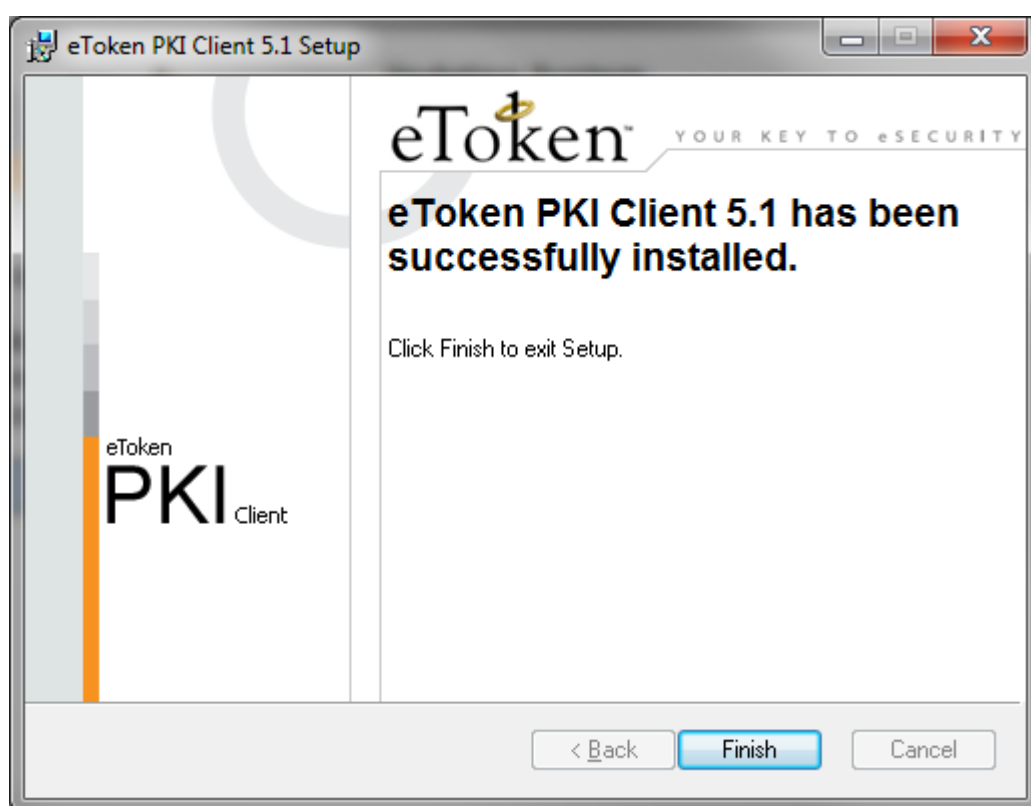
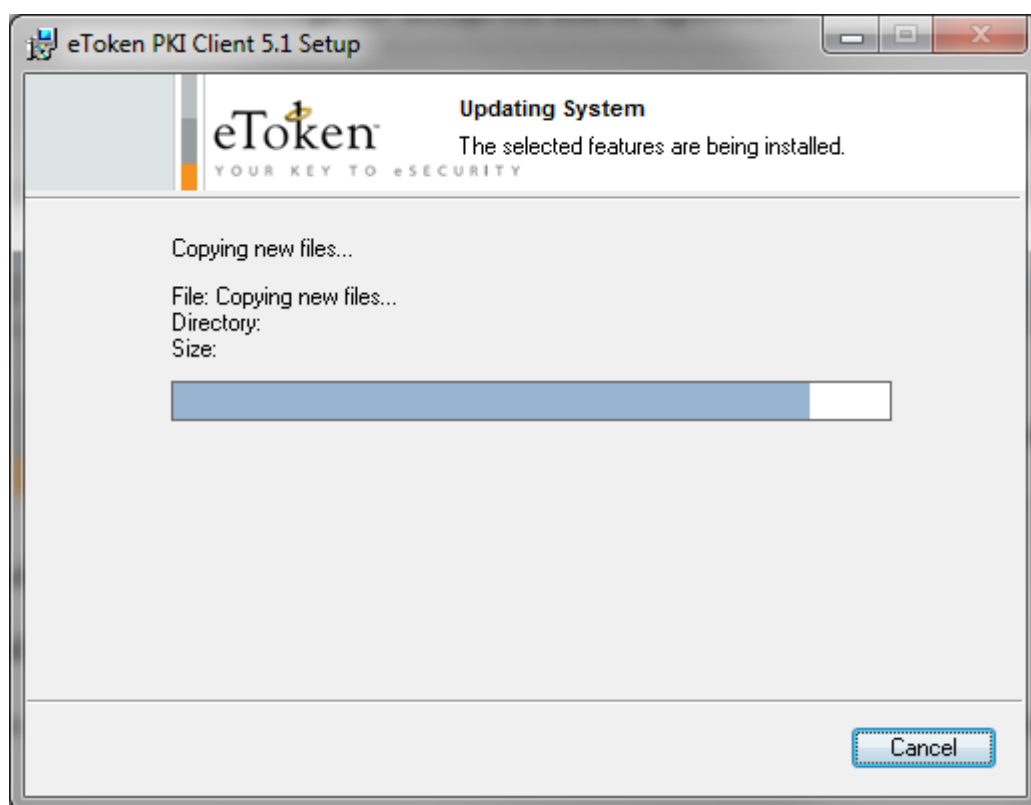
2. Ознакомьтесь с лицензией на программное обеспечение eToken PKI Client и выразите свое согласие с ней, выбрав пункт «I accept the license agreement».



3. После этого Вам будет предложен путь установки программы. Оставьте предложенный по умолчанию или выберите другой путь.

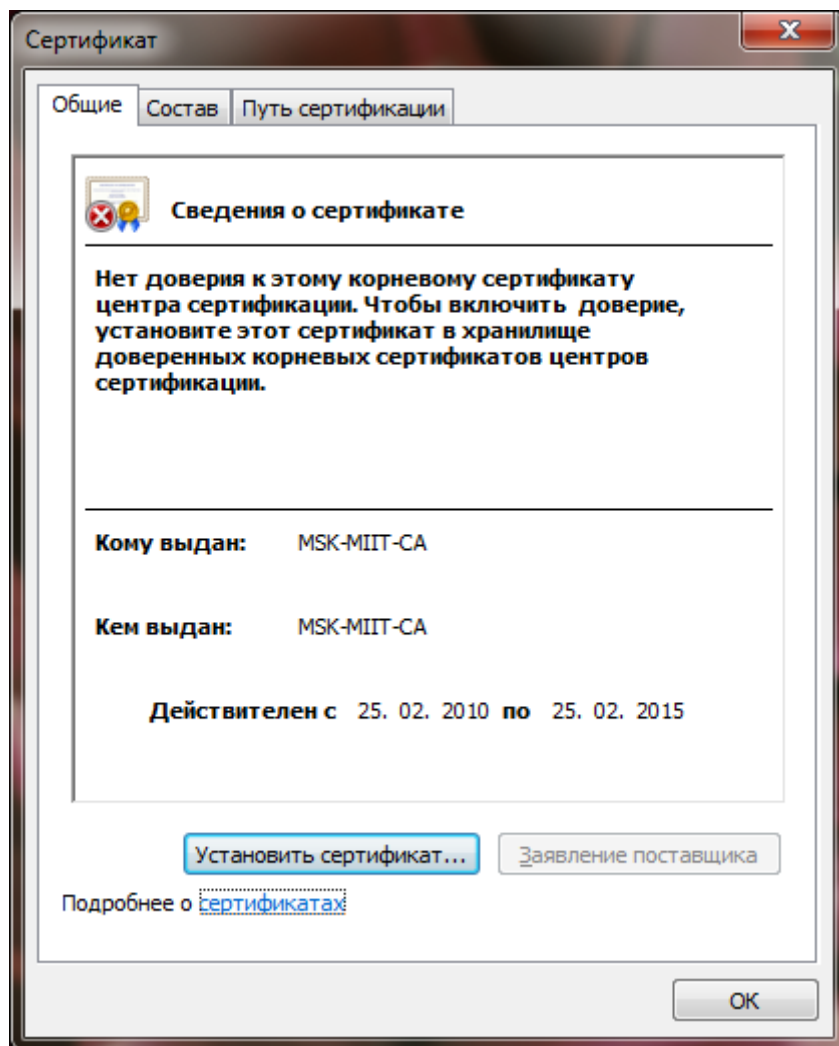


4. Затем начнется процесс установки программного обеспечения, по завершении которого ПО будет готово к использованию.

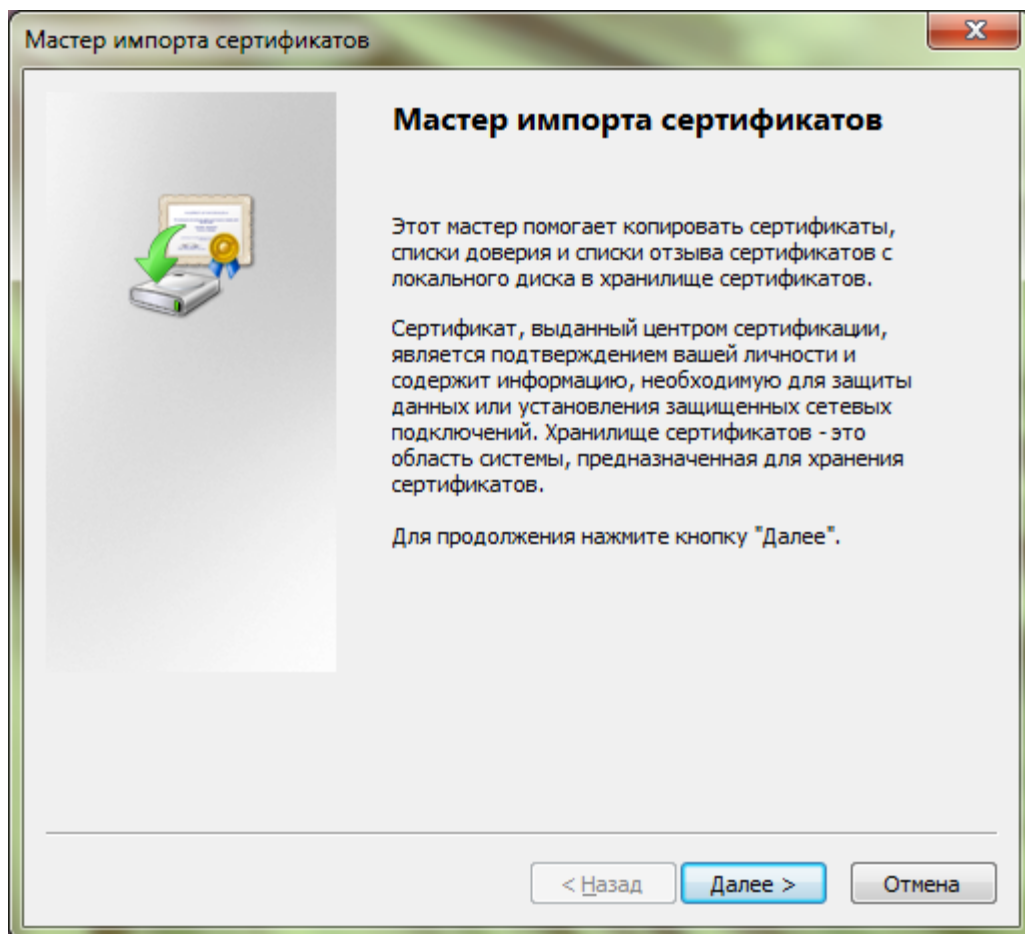


Установка сертификата корневого удостоверяющего центра

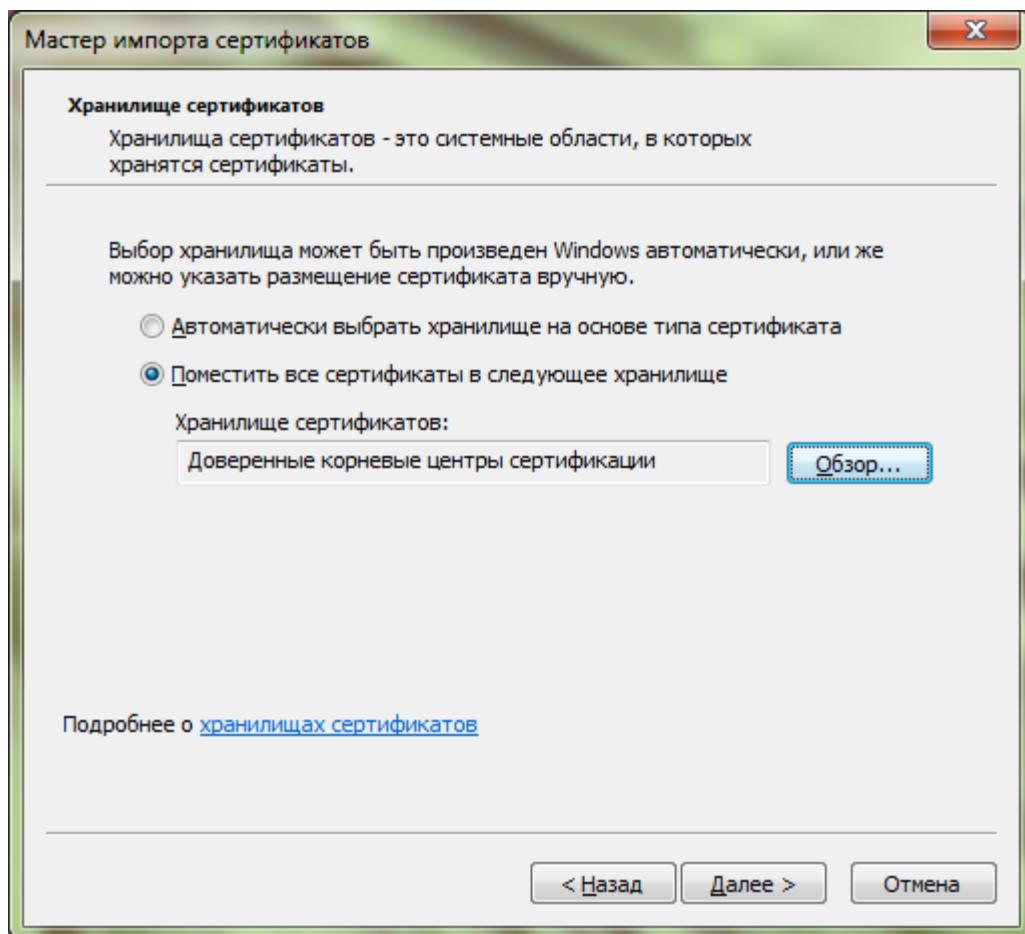
1. Получите от администратора файл с сертификатом корневого центра сертификации и запустите его. Затем нажмите «Установить сертификат».



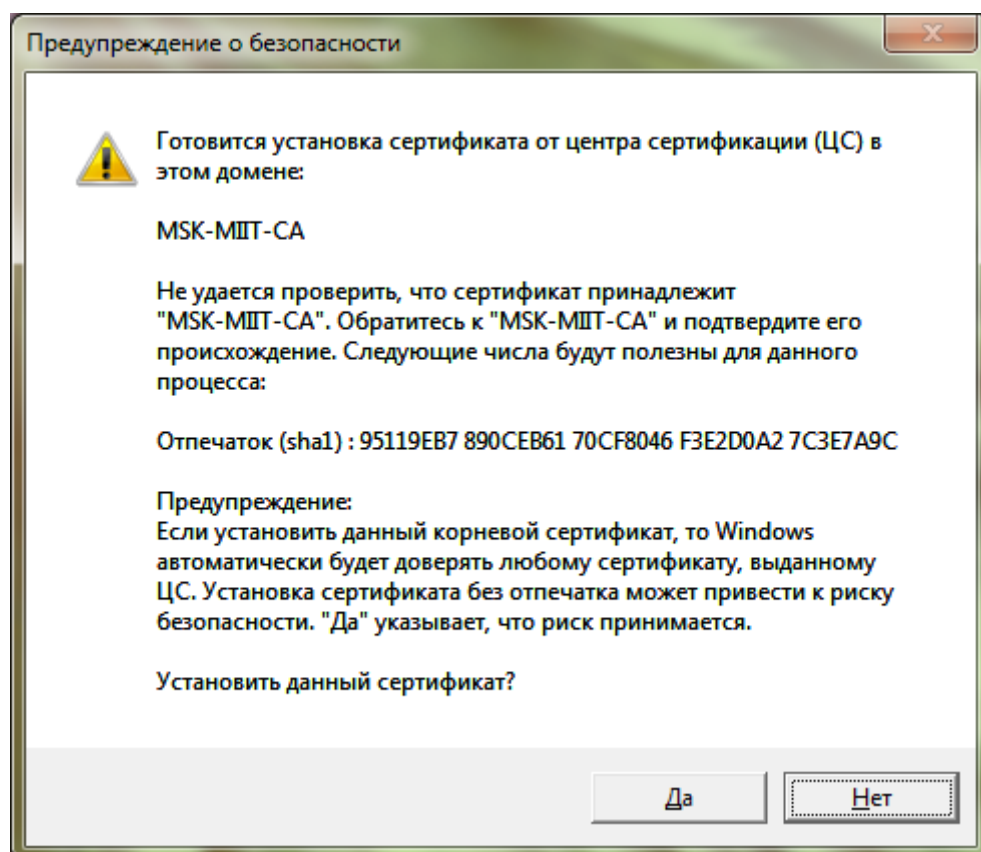
2. Запустится мастер импорта сертификатов.



3. Выберите пункт «Поместить все сертификаты в следующее хранилище» и нажмите кнопку «Обзор». Выберите «Доверенные корневые центры сертификации» и нажмите «Далее».



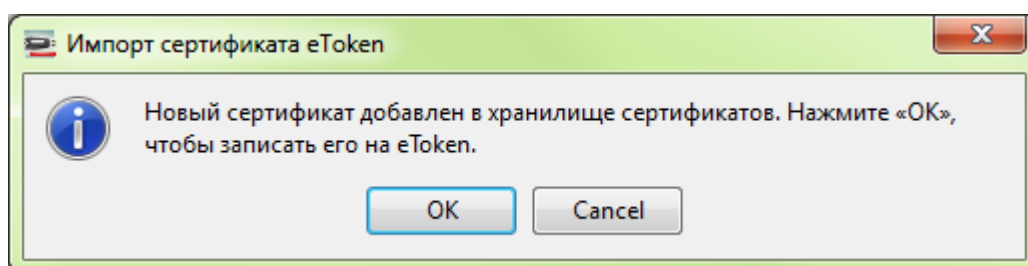
4. Появится окно с запросом установки сертификата центра сертификации:



5. Проверьте правильность имени корневого центра сертификации и отпечаток сертификата (имя должно быть «MSK-MIIT-CA», отпечаток – «95 11 9e b7 89 0c eb 61 70 cf 80 46 f3 e2 d0 a2 7c 3e 7a 9c»). После этого согласитесь с установкой.

Установка пользовательского сертификата

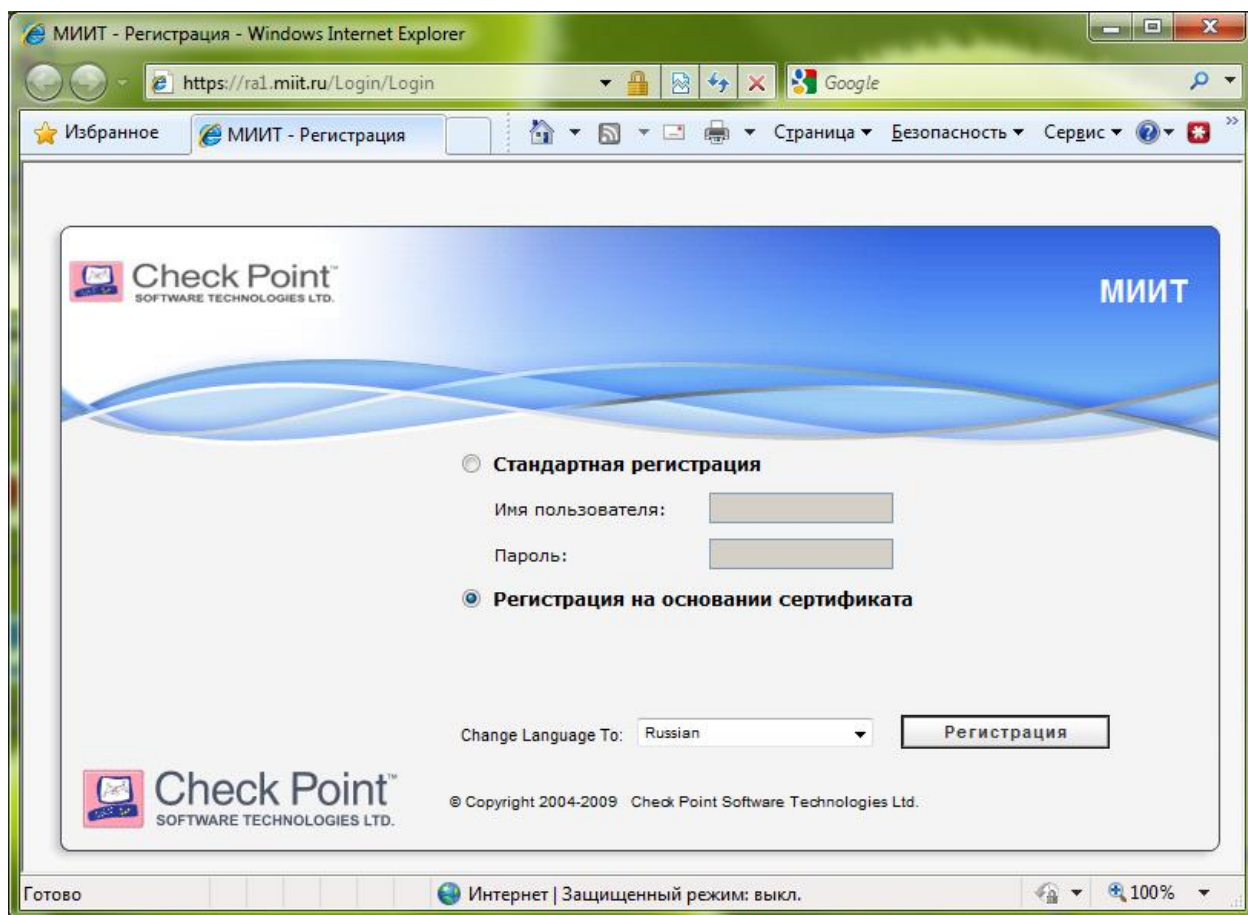
1. Вставьте ключевой носитель eToken в USB-порт Вашего компьютера. Сертификат пользователя установится автоматически в локальное хранилище.
2. При появлении сообщения вида



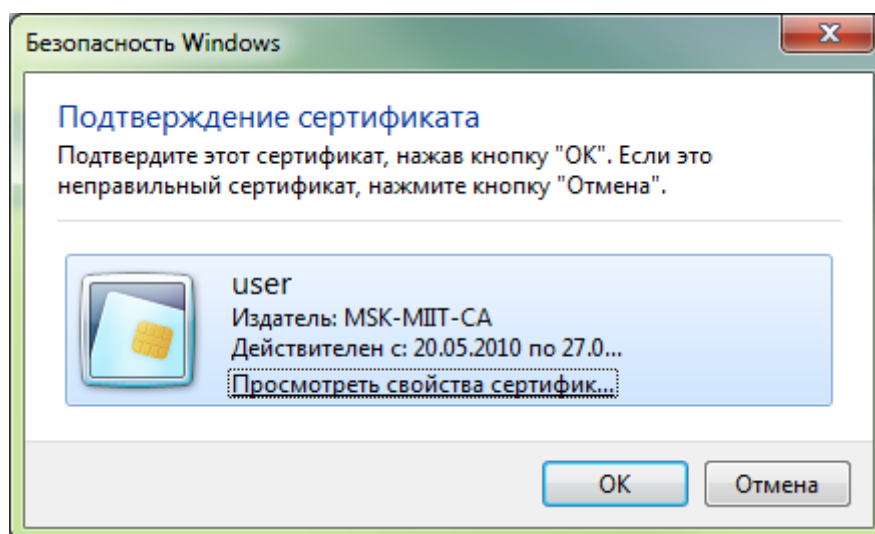
необходимо отказаться от установки, нажав кнопку «Отмена» («Cancel»).

Установка соединения с шлюзом удаленного доступа

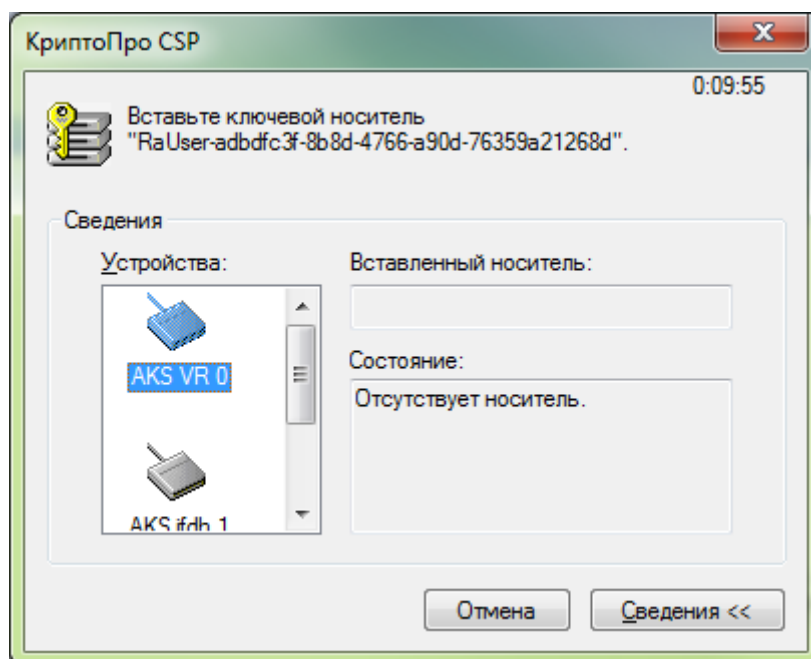
1. Откройте веб-браузер и введите в строке адреса `https://ra1.miit.ru`
2. На появившейся странице портала выберите пункт «Регистрация на основании сертификата» и нажмите кнопку «Регистрация».



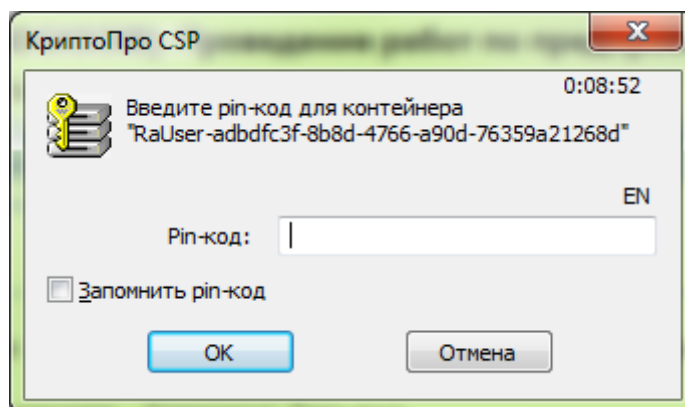
3. Появится запрос на предоставление сертификата пользователя. Выберите свой сертификат.



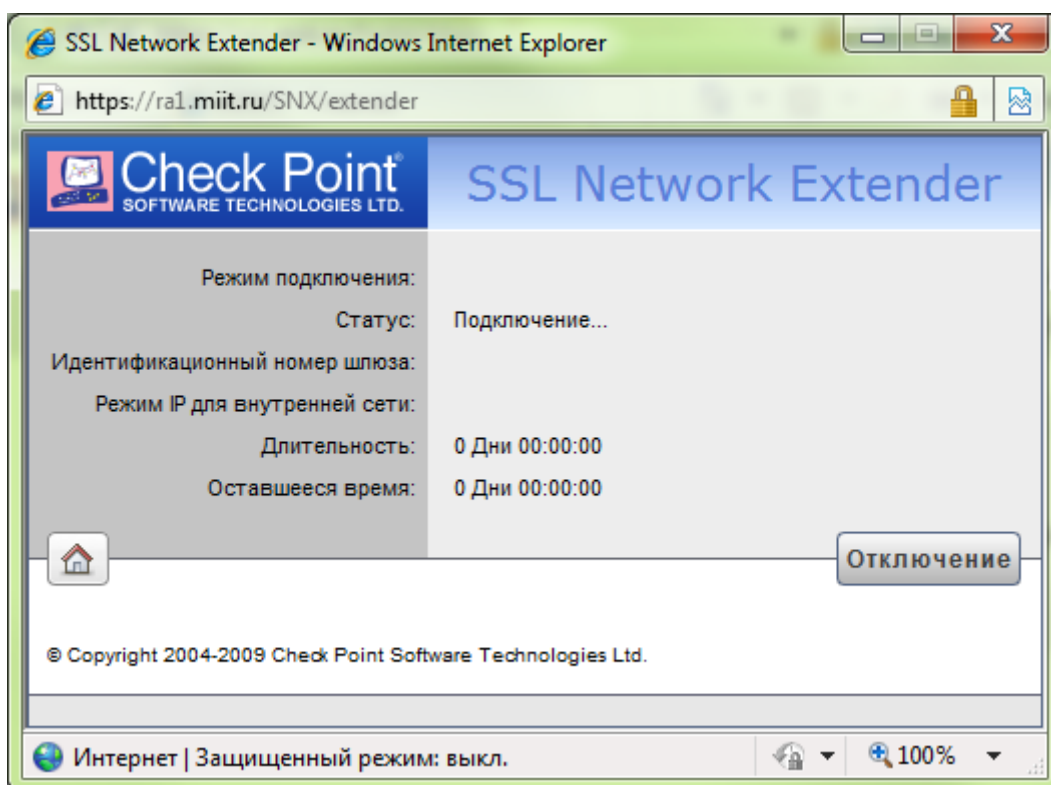
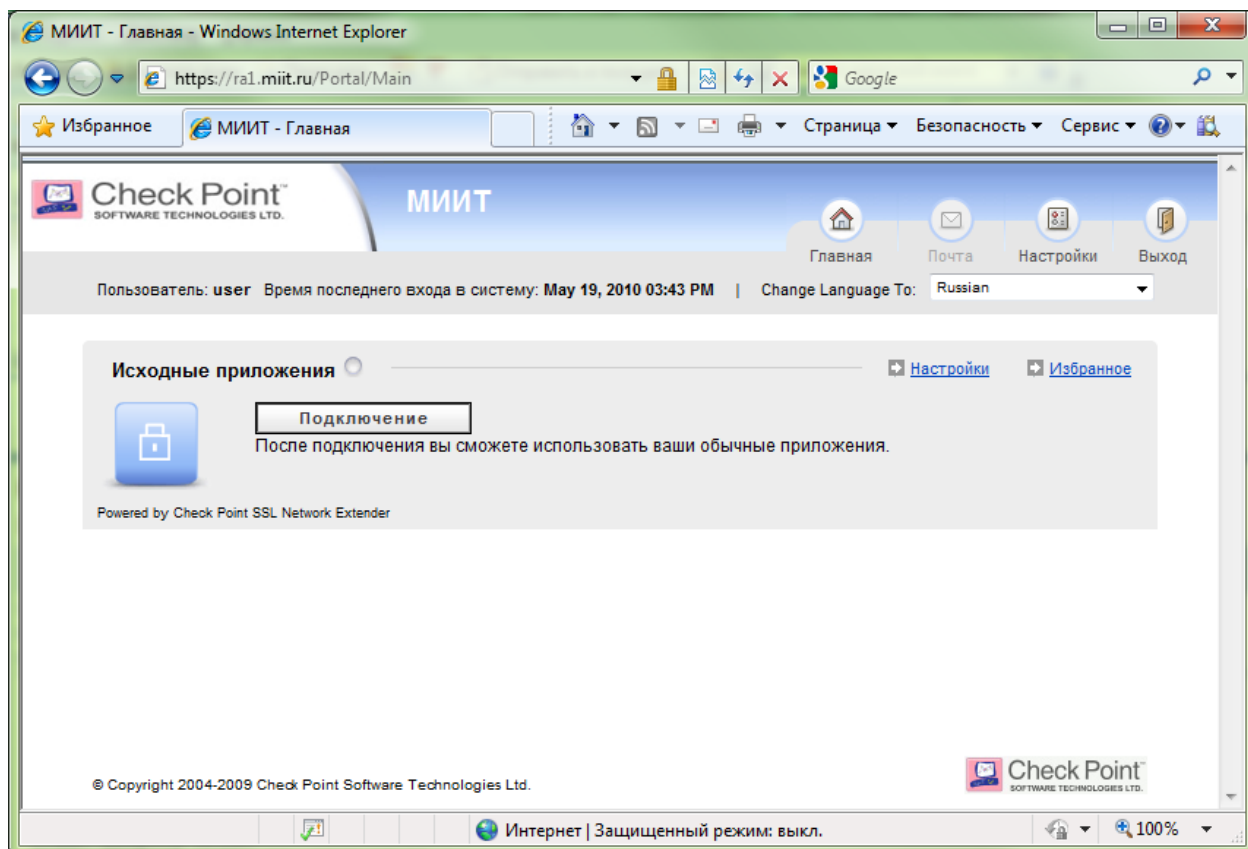
4. Если ключевой носитель eToken не вставлен в USB-порт компьютера, появится следующее сообщение:



5. Вставьте eToken в USB-порт, вышеприведенное сообщение исчезнет автоматически и будет запрошен PIN-код на ключевой носитель. Введите свой PIN-код.



6. В случае удачной аутентификации, Вы попадаете в закрытую часть портала и автоматически запустится установление защищенного соединения с шлюзом удаленного доступа. При первом запуске запустится процесс установки необходимых компонент.



7. Теперь Вы можете работать с ресурсами, доступ к которым разрешает шлюз удаленного доступа.
8. По завершении работы разорвите соединение со шлюзом, нажав кнопку «Отключение».

