Инструкция по настройке АРМ пользователя удостоверяющего центра «ТОГУ Информационно-технический центр».

Тамбов 2009 г.

Содержание

1. Настройка рабочего места пользователя.

Перед началом работы с АРМами пользователя ЦР необходимо выполнить следующие процедуры:

- Получить от администратора ЦР или скачать с Web сервера ЦР дистрибутивы программного обеспечения СКЗИ «КриптоПро CSP»
- Установить СКЗИ «КриптоПро CSP»
- Установить сертификат ЦС
- Установить личный сертификат с ключевого носителя, полученного от администратора ЦР в случае регистрации пользователя в централизованном режиме.

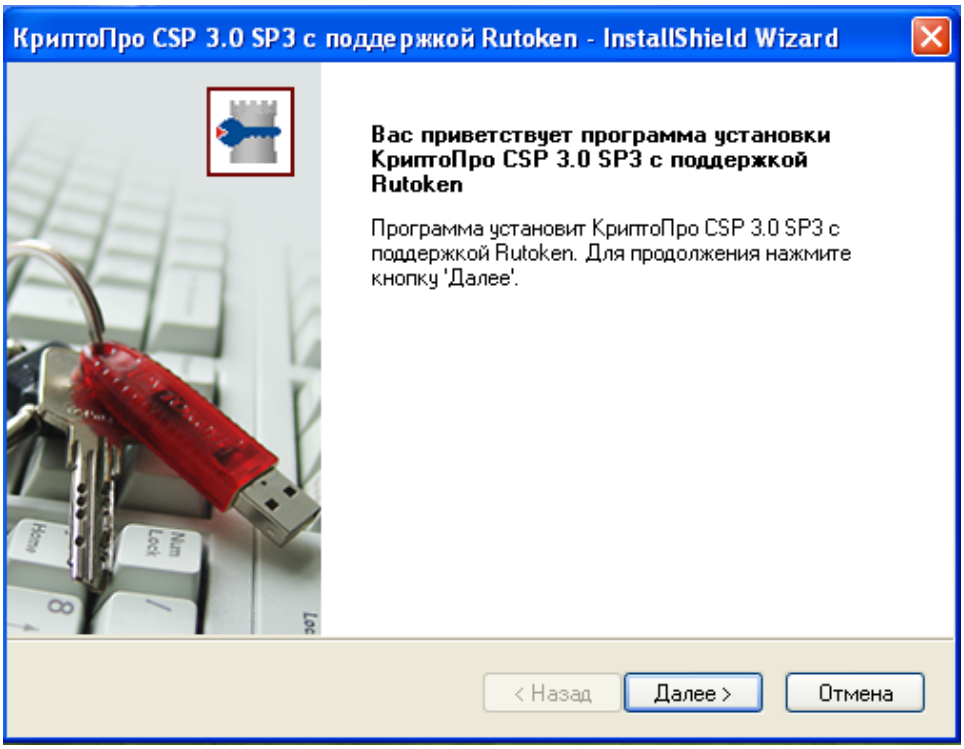
Процедура получения указанных компонент регламентируется политикой конкретного Удостоверяющего Центра. В том случае, если регламентом УЦ разрешена процедура регистрации пользователя в распределенном режиме, то Удостоверяющий Центр должен предоставить пользователю все необходимые компоненты для выполнения процедур настройки рабочего места пользователя.

2. Установка и настройка CSP 3.0 с поддержкой rutoken.

2.1 Установка

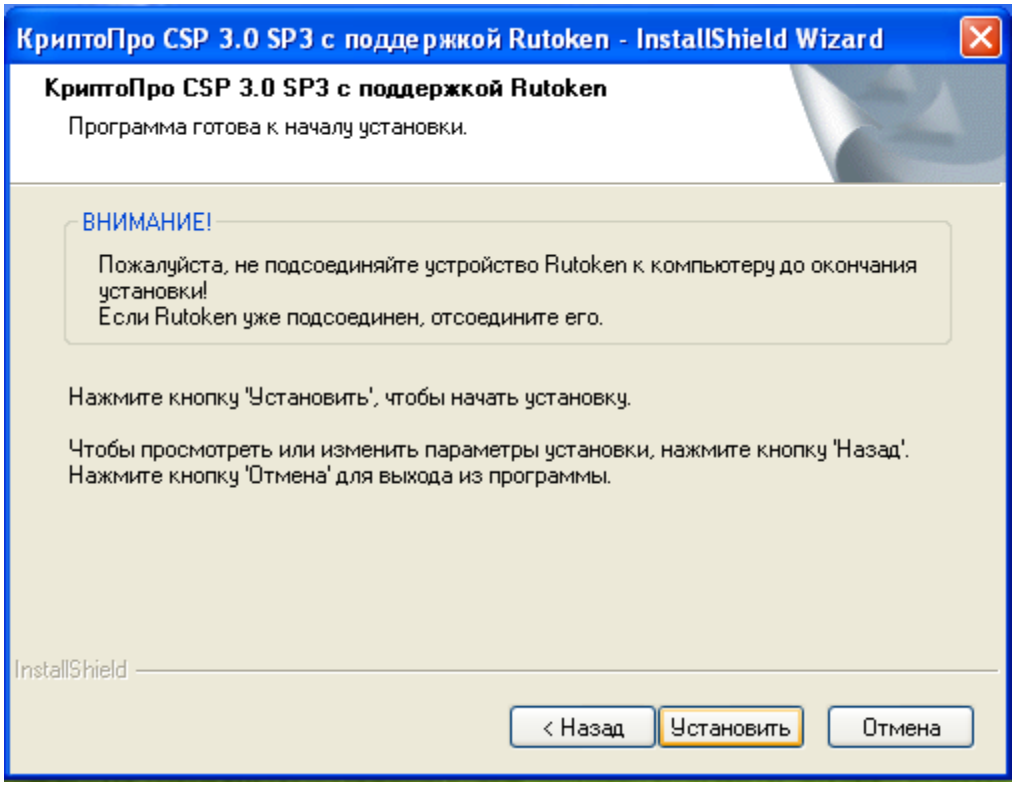
Для установки CSP 3.0 с поддержкой рутокена запустим установочный файл и далее следуем инструкциям установки (Рисунок 1).

Рисунок 1.



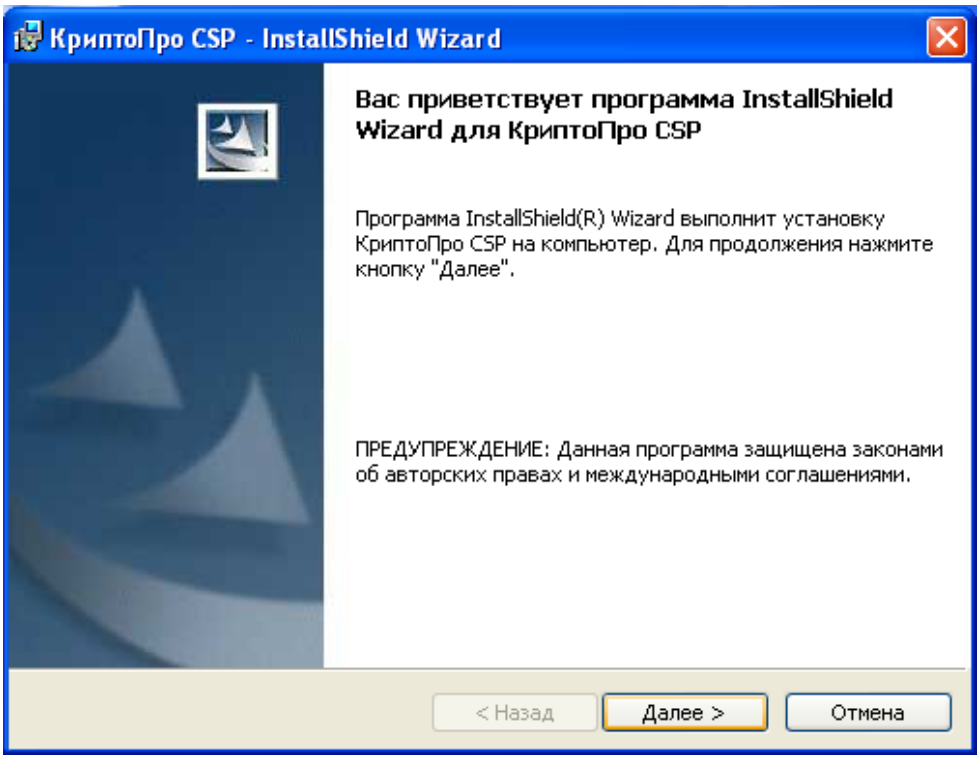
Нажимаем **Далее**. Для корректной установки криптопровайдера рутокен не должен быть подсоединён к компьютеру. Если это так, то отсоедините его и ,для продолжения установки, нажмите кнопку **Установить** (Рисунок 2).

Рисунок 2.



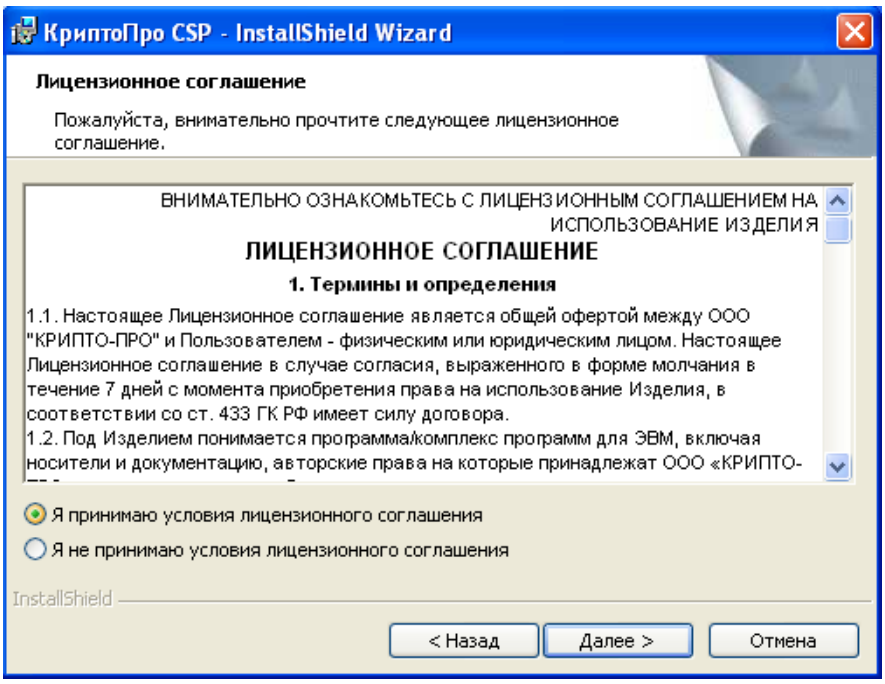
Следуйте инструкциям мастера установки нажимая **Далее** (Рисунок 3).

Рисунок 3.



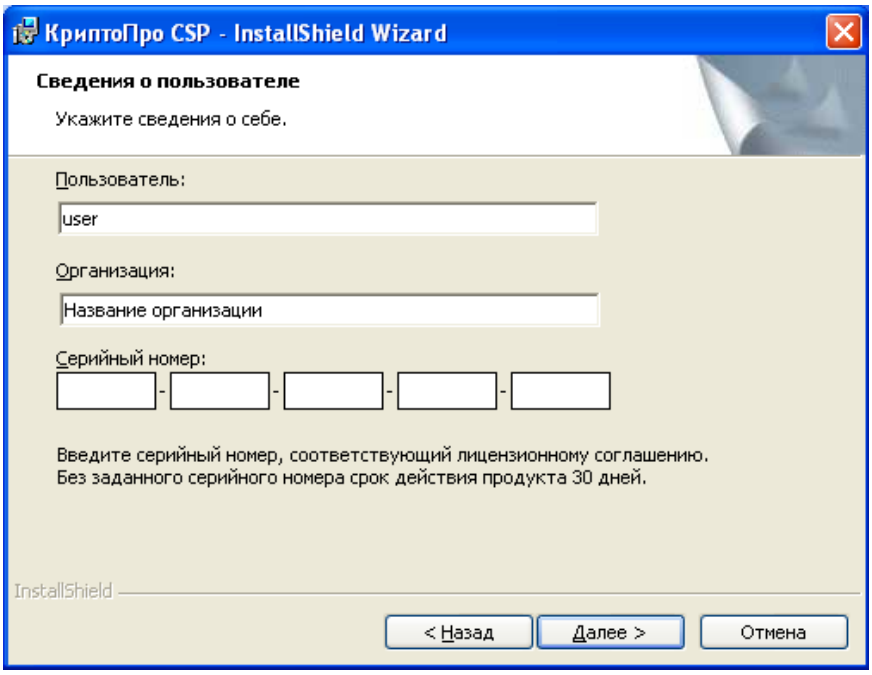
После прочтения лицензионного соглашения нужно отметить пункт **Я принимаю условия лицензионного соглашения** и нажать **Далее** (Рисунок 4).

Рисунок 4.



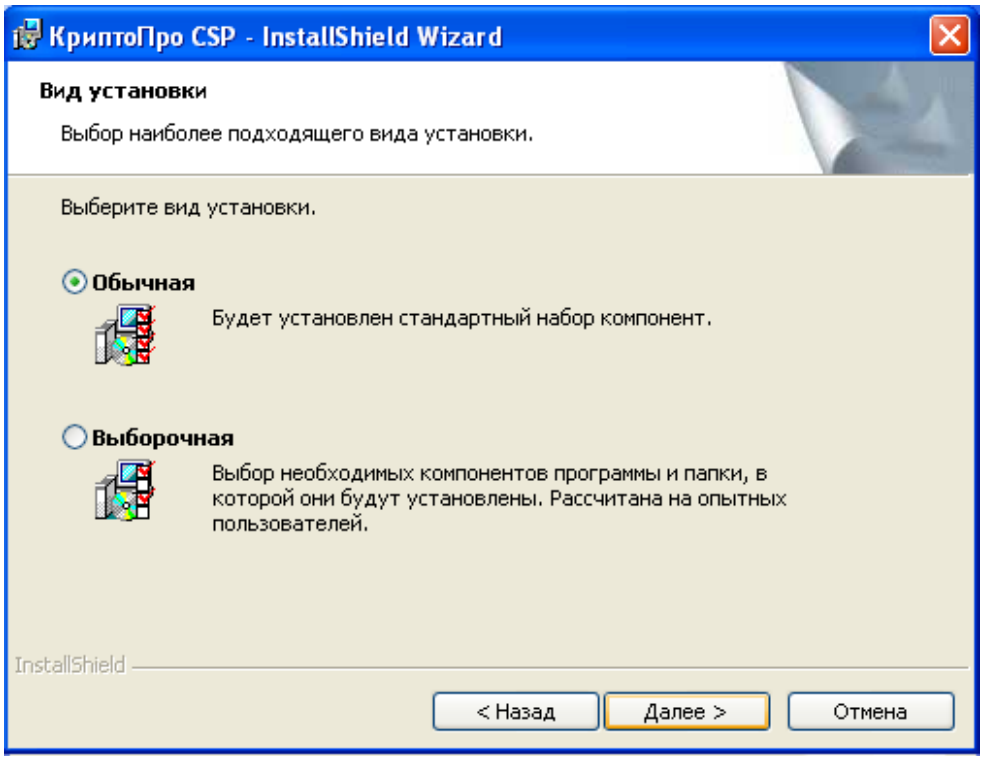
Далее необходимо ввести ваши лицензионные данные. Заполните все поля в соответствии с вашим именем пользователя и данными полученными с лицензией на криптопровайдер (Рисунок 5). После того как все поля заполнены, нажимаем кнопку **Далее.**

Рисунок 5.



В следующем окне выбираем обычную установку и нажимаем **Далее** (Рисунок 6).

Рисунок 6.



Программа готова к установке. Нажимаем кнопку **Установить** и затем **Готово** (Рисунок 7,8).

Рисунок 7.

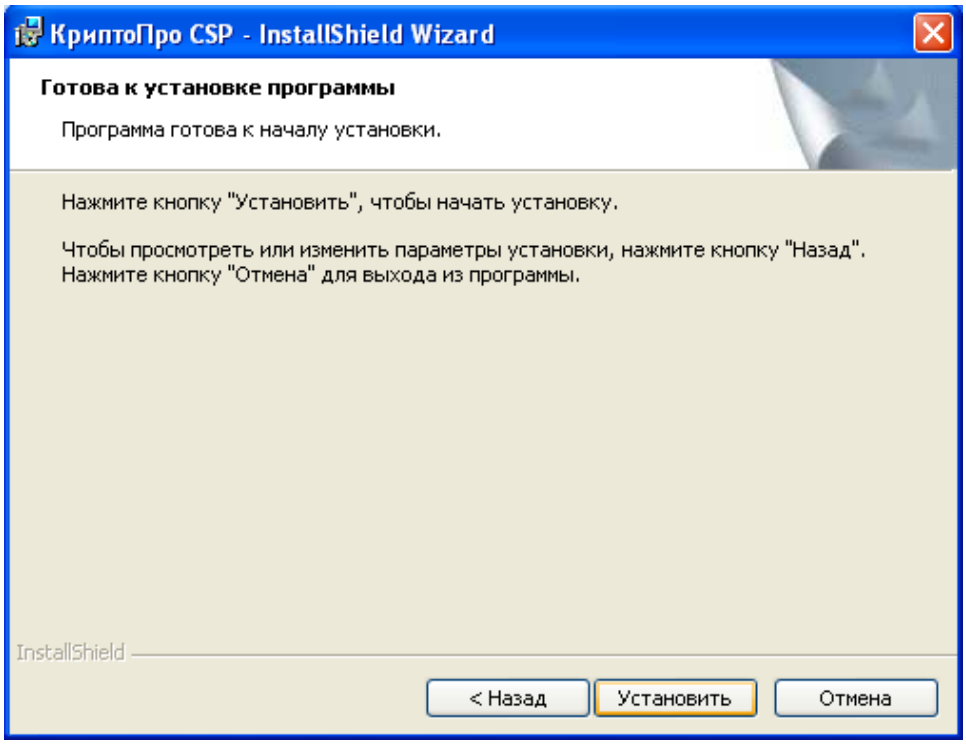
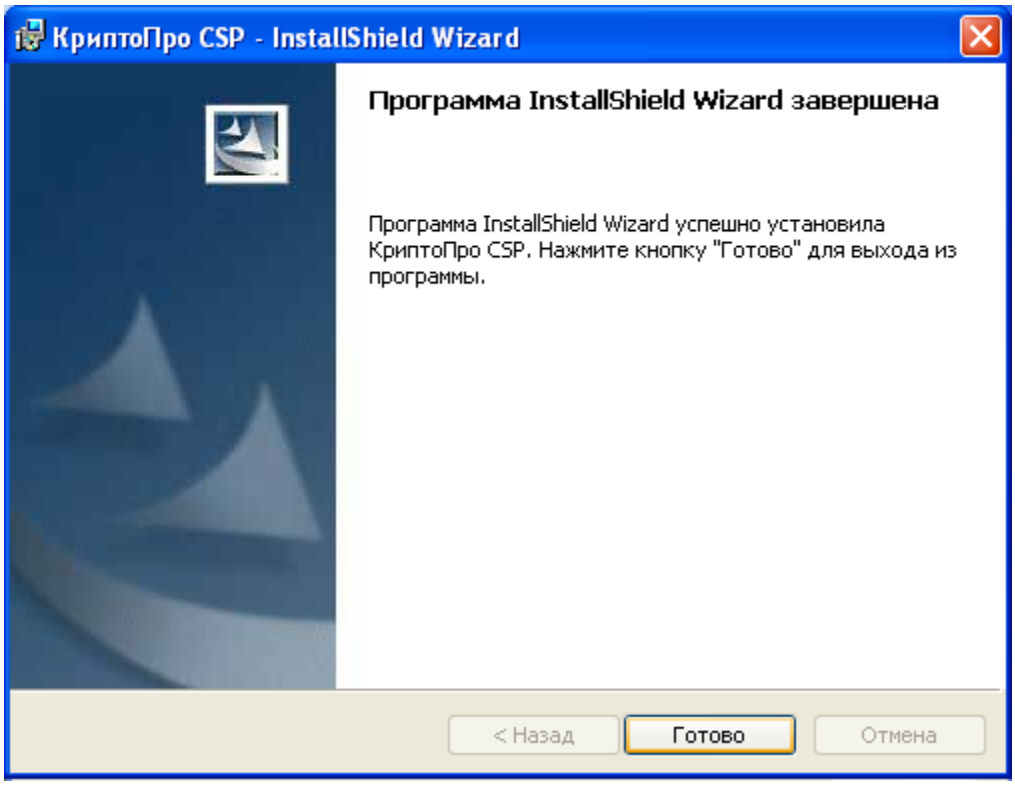
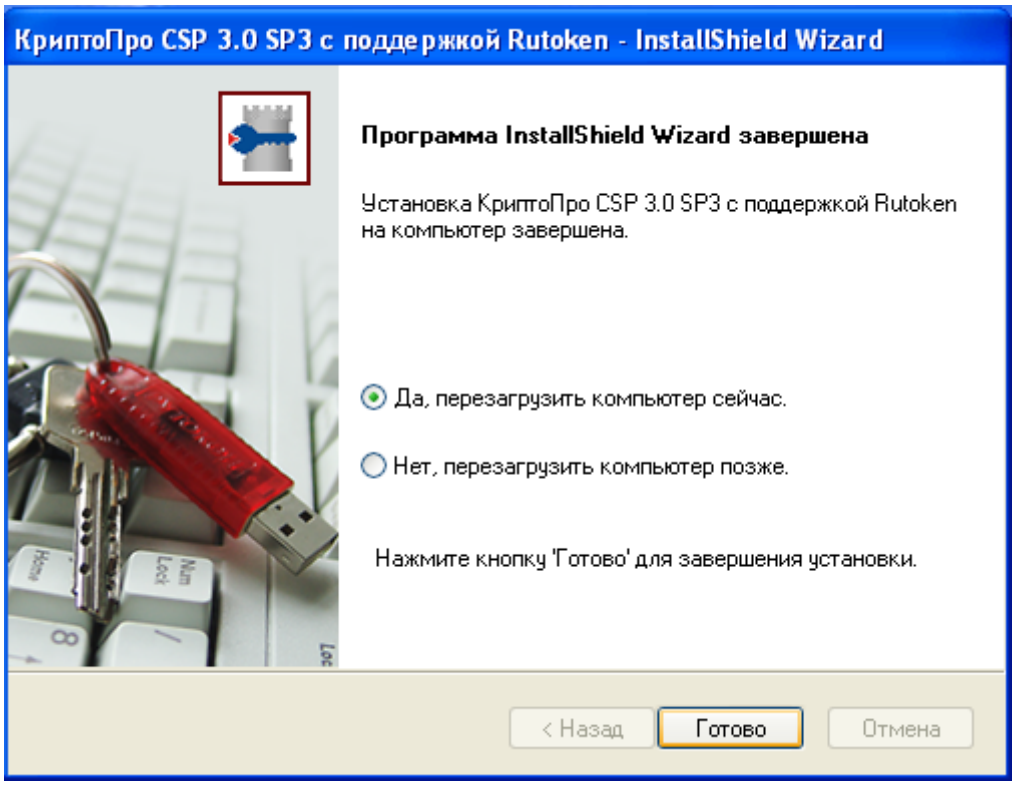


Рисунок 8.



Для окончания установки необходимо перезагрузить компьютер. Выберите пункт **Да, перезагрузить компьютер сейчас** и нажмите **Готово** (Рисунок 9).

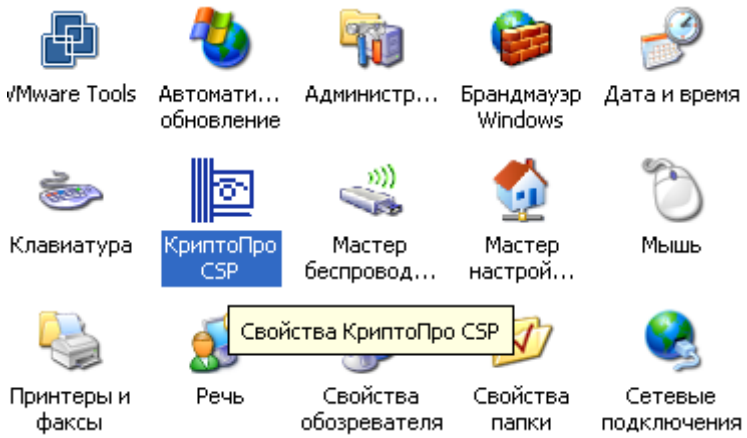
Рисунок 9.



2.2 Настройка криптопровайдера

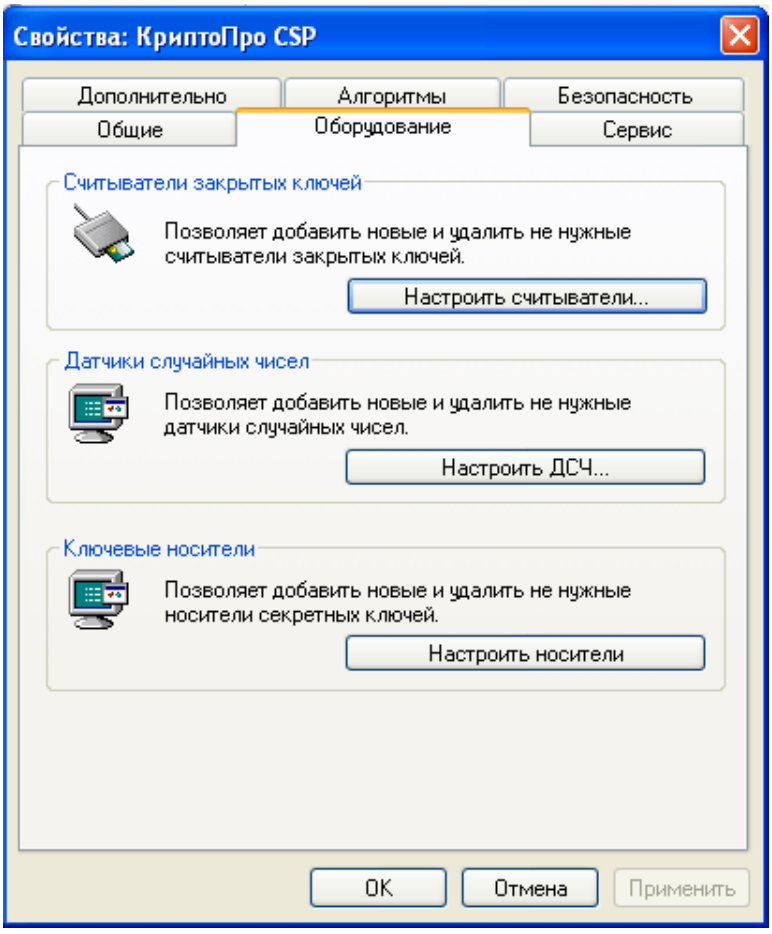
После перезагрузки необходимо в криптопровайдер добавить считыватель реестр. Для этого откроем **Пуск → Панель управления→КриптоПроCSP** (Рисунок 10).

Рисунок 10.



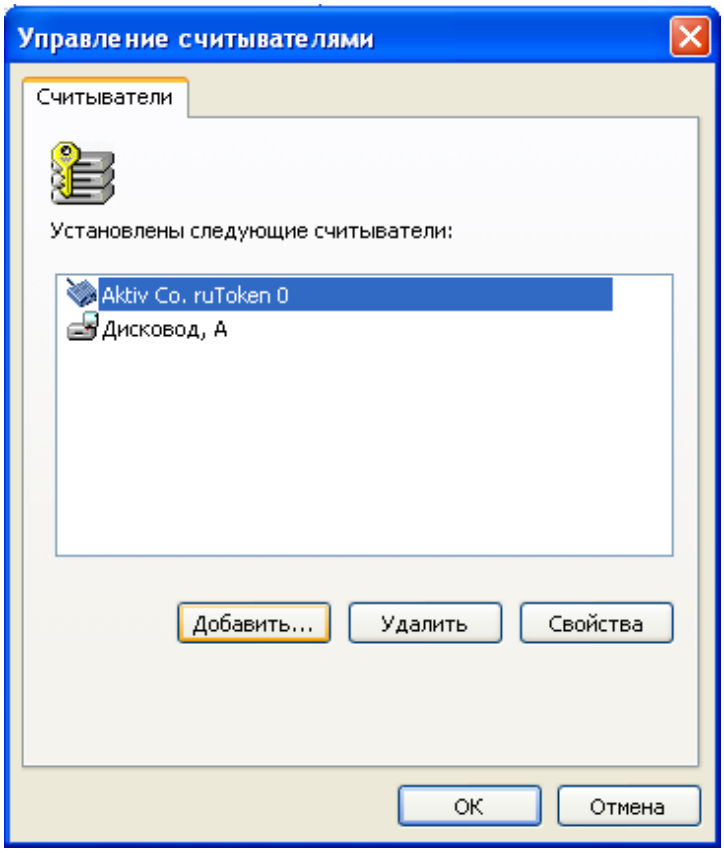
В открывшемся окне выберем вкладку **Оборудование** и нажмём на кнопку **Настроить считыватели…** (Рисунок 11).

Рисунок 11.



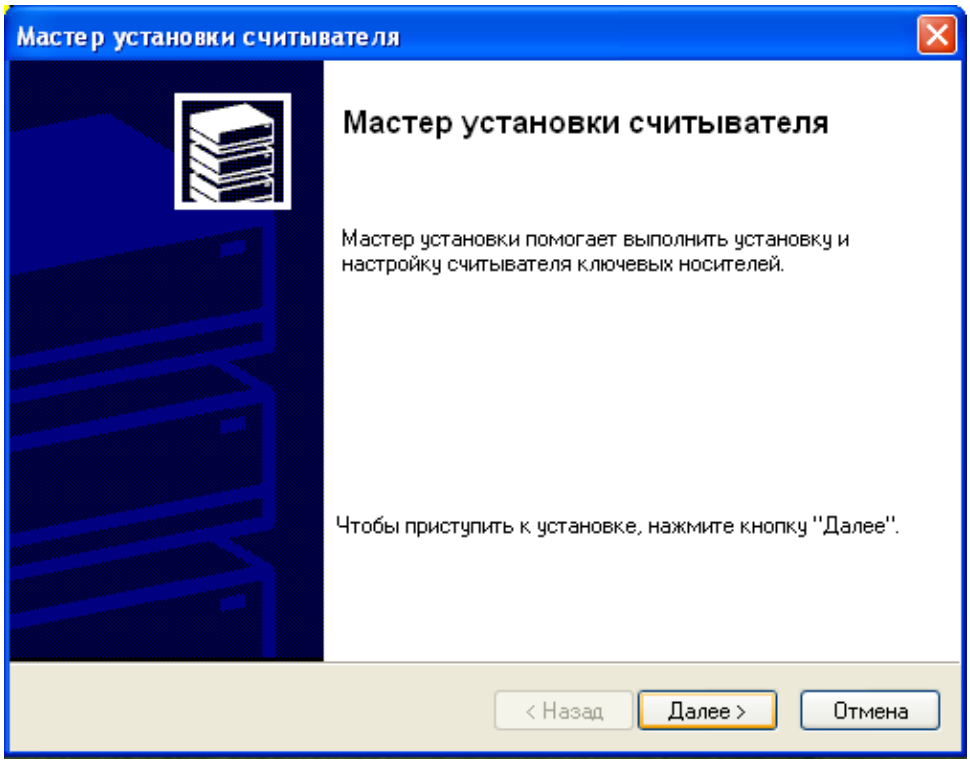
В следующем окне нажмём кнопку **Добавить…** (Рисунок 12).

Рисунок 12.



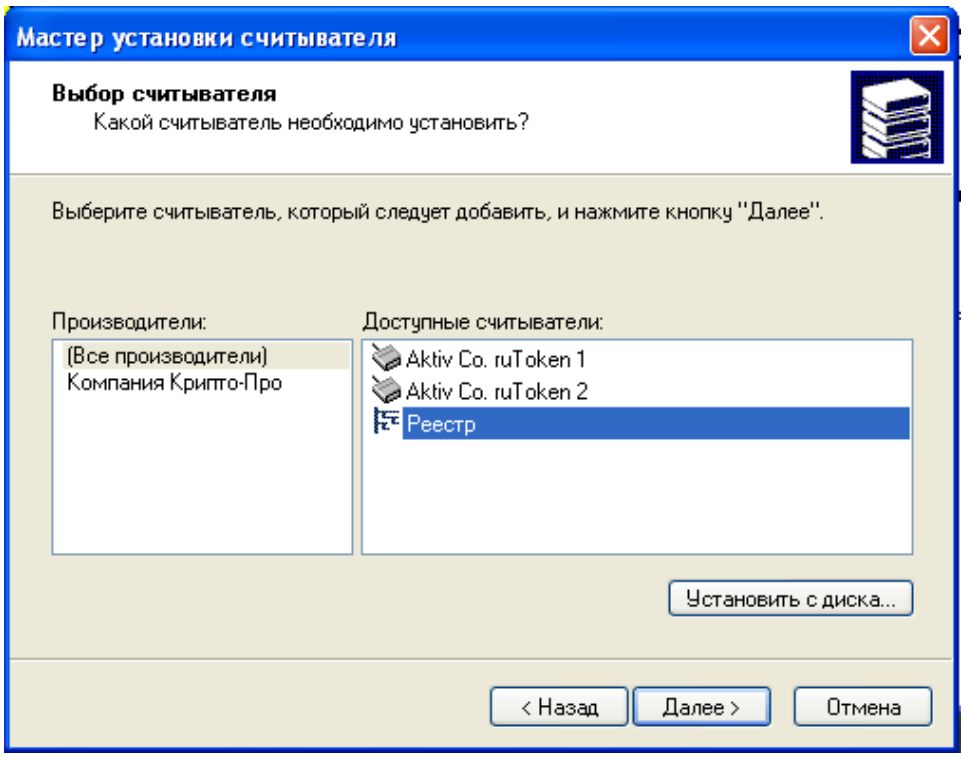
Далее увидим окно мастера установки и нажмём **Далее** (Рисунок 13).

Рисунок 13.



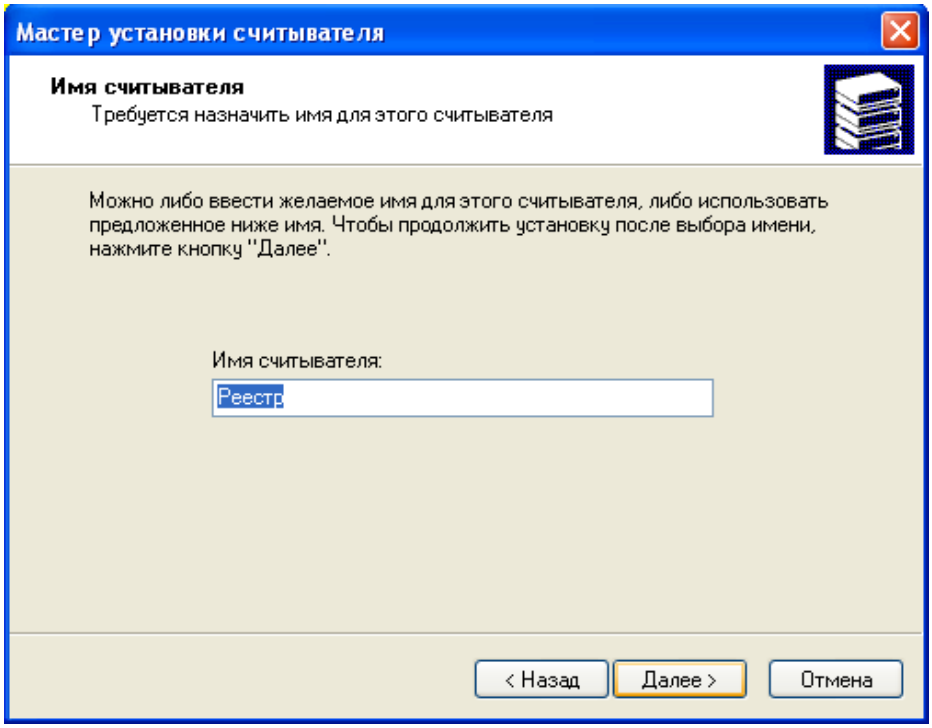
В следующем окне нам предоставлен выбор считывателей. Выбираем считыватель **Реестр** и нажимаем **Далее** (Рисунок 14).

Рисунок 14.



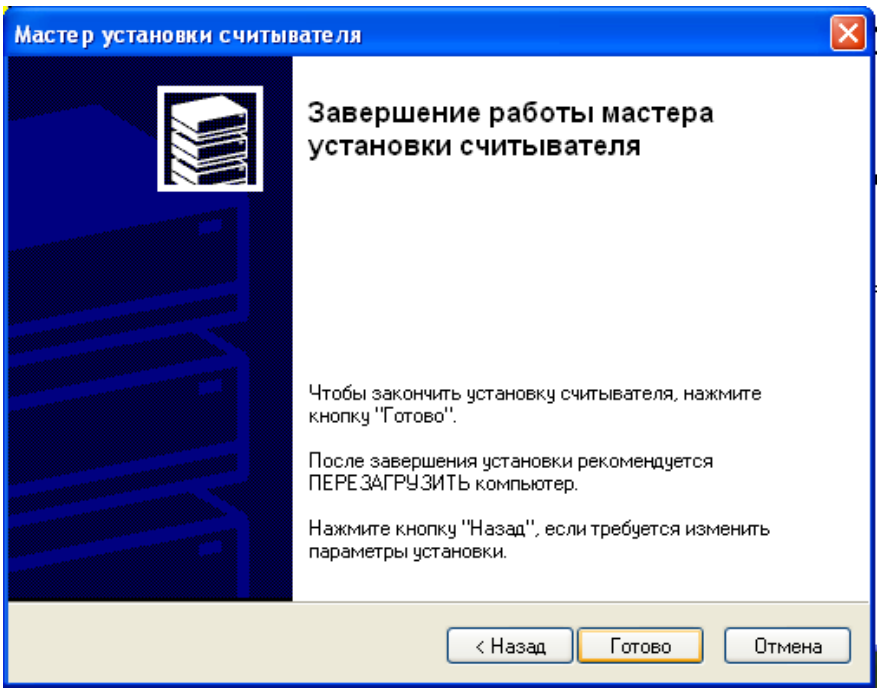
Мастер установки спросит как назвать данный считыватель. Можно оставить предлагаемый вариант и нажать **Далее** (Рисунок 15).

Рисунок 15.



Завершаем установку считывателя нажатием кнопки **Готово** в следующем окне (Рисунок 16).

Рисунок 16.



Теперь мы видим, что в окне считывателей появился новый считыватель **Реестр.** Закрываем окна нажатием на кнопку **ОК** (Рисунок 17,18).

Рисунок 17.

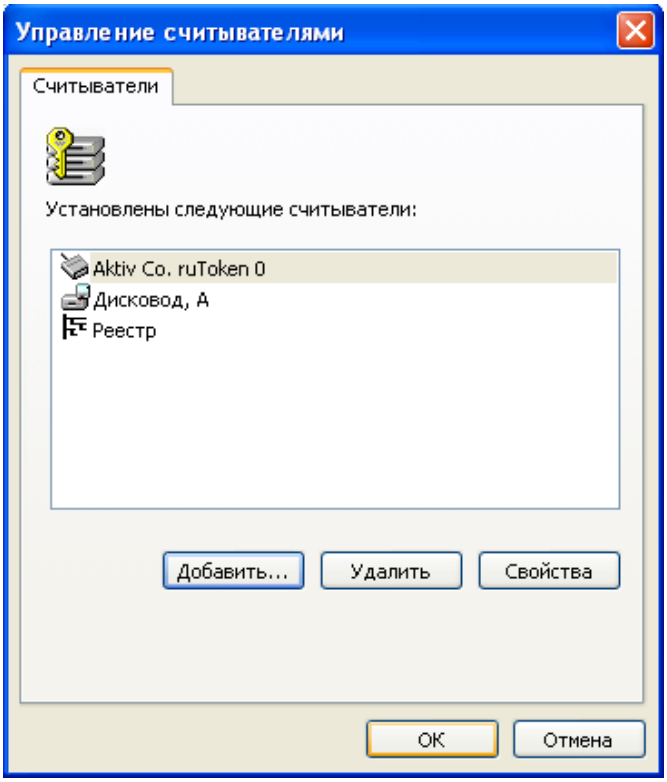
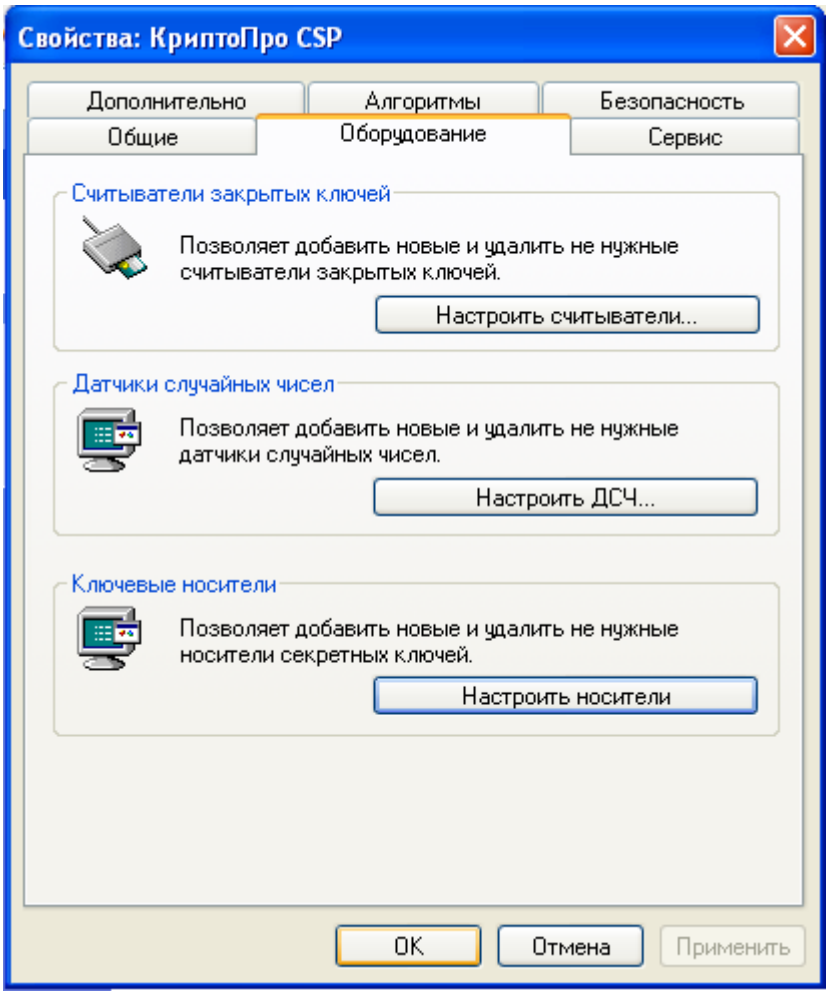


Рисунок 18.



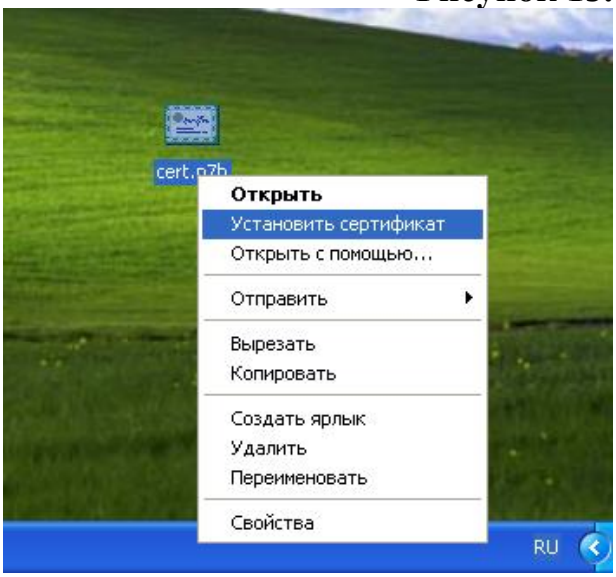
Криптопровайдер успешно установлен и готов к работе.

3. Установка цепочки сертификатов центра сертификации и личного сертификата

3.1 Установка цепочки сертификатов

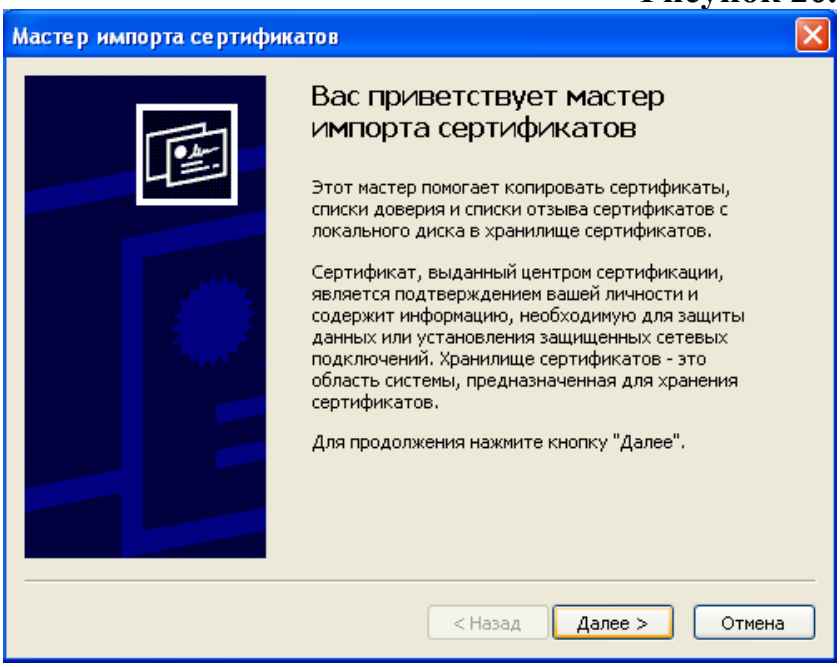
Для установки цепочки сертификатов центра сертификации необходимо нажать правой кнопкой мыши на файле цепочки. В появившемся меню выбрать пункт **Установить сертификат** (Рисунок 19).

Рисунок 19.



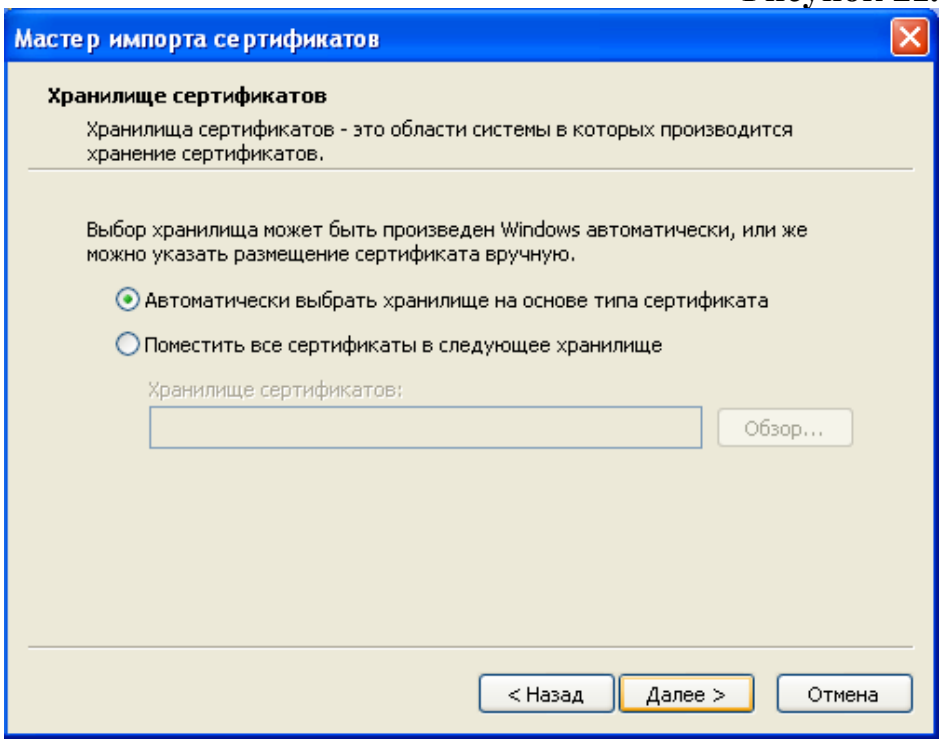
Далее следуем инструкциям мастера установки и нажимаем **Далее** (Рисунок 20).

Рисунок 20.



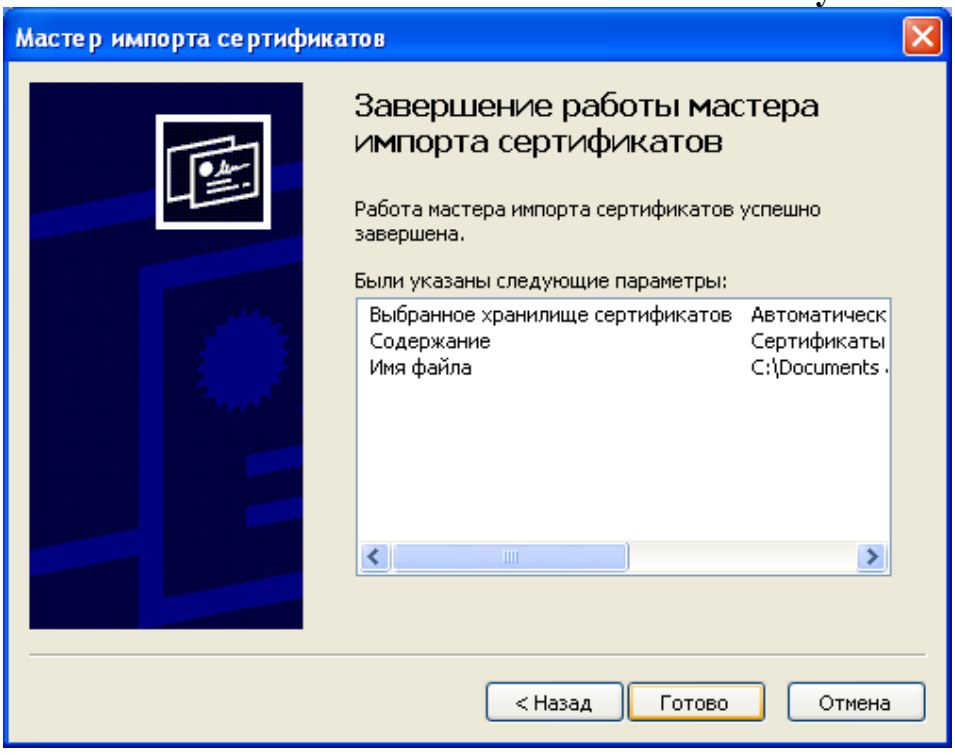
Мастер установки попросить указать хранилище для установки сертификата. Выбираем **Поместить все сертификаты в следующее хранилище**, нажимаем **Обзор** и выбираем **Доверенные корневые центры сертификации.** Нажимаем **OK** и кнопку **Далее** (Рисунок 21).

Рисунок 21.



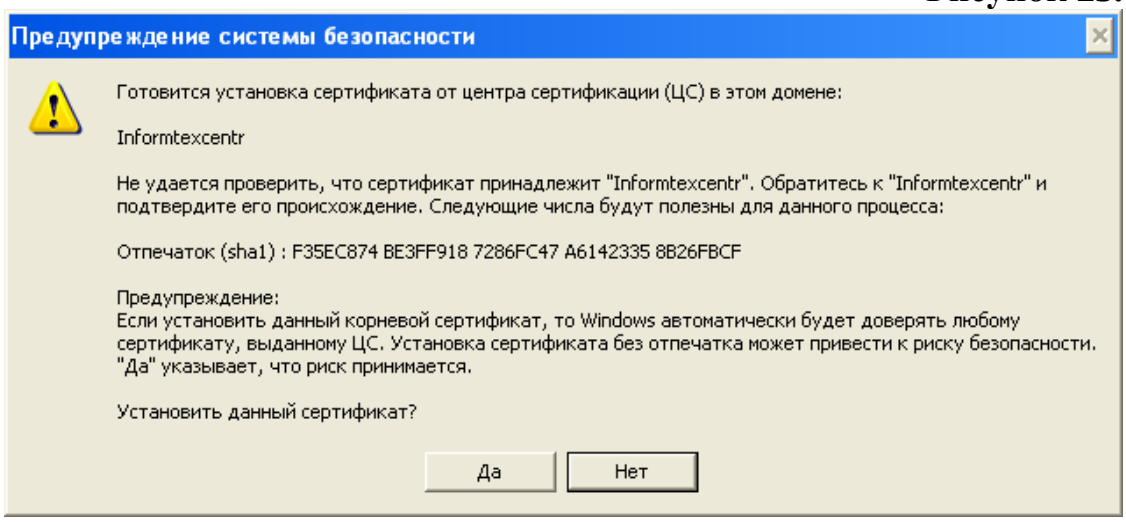
В окне завершения работы мастера нажимаем Готово (Рисунок 22).

Рисунок 22.



Система безопасности выдаст следующее предупреждение (Рисунок 23). На вопрос «**Установить данный сертификат?»** отвечаем **Да.**

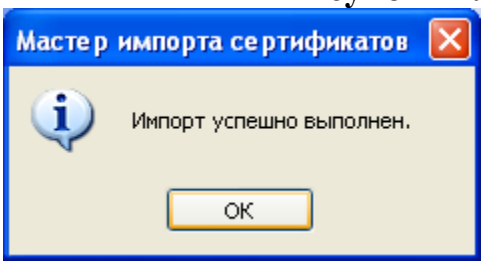
Рисунок 23.



И получаем сообщение об успешном окончании установки (Рисунок 24).

Нажимаем **Ок**.

Рисунок 24.

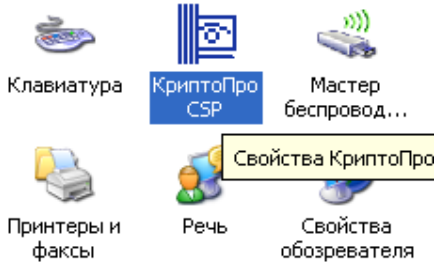


Сертификат центра сертификации и список отозванных сертификатов успешно установлены.

3.2 Установка личного сертификата

Для установки личного сертификата в систему откроем криптопровайдер. **Пуск →Панель управления→КриптоПроCSP** (Рисунок 25).

Рисунок 25.

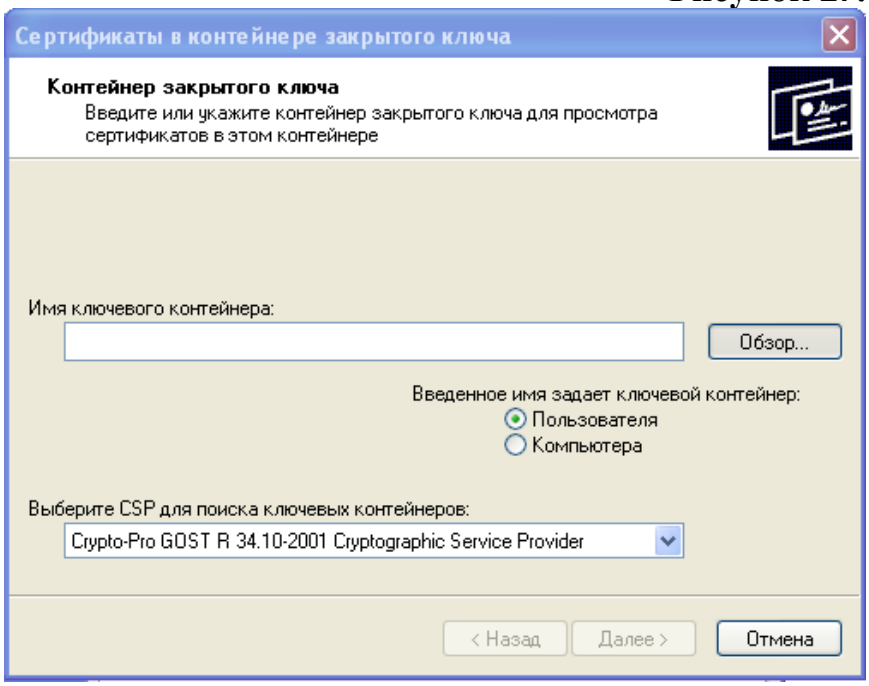


На вкладке **Сервис** нажмём на кнопку **Просмотреть сертификат в контейнере** (Рисунок 26).

Рисунок 26.

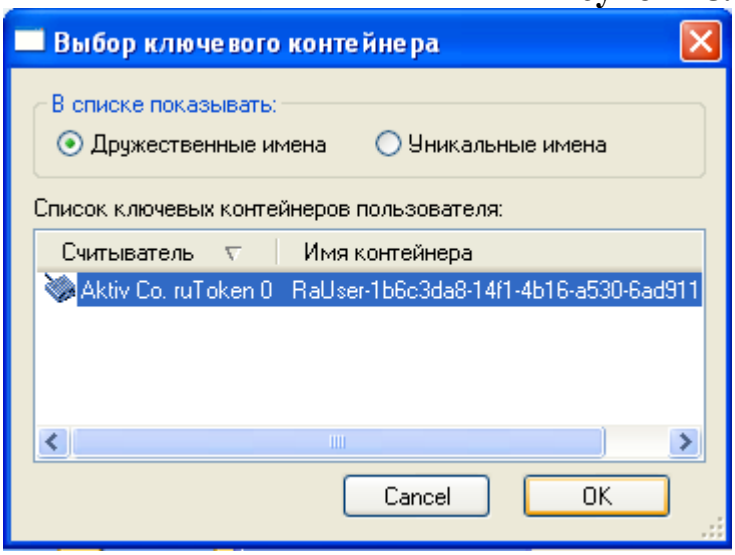
Вставим рутокен в компьютер и в открывшемся окне нажмём кнопку **Обзор** для выбора контейнера (Рисунок 27).

Рисунок 27.



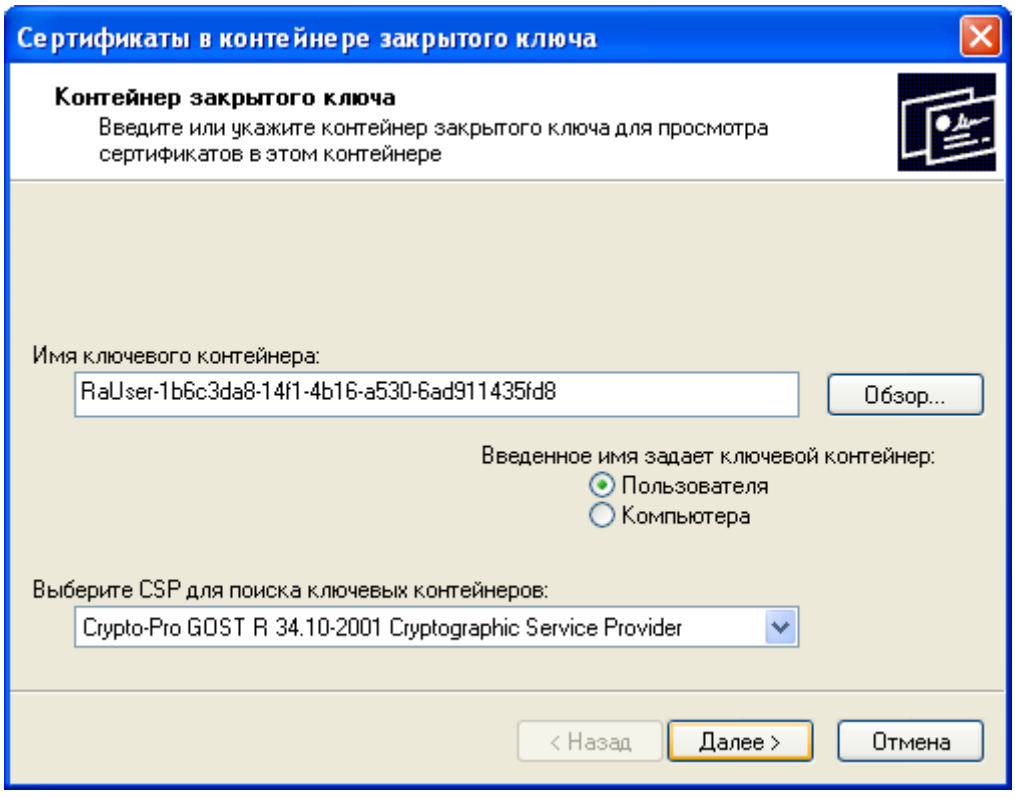
Выбираем наш рутокен и нажимаем **ОК** (Рисунок 28).

Рисунок 28.



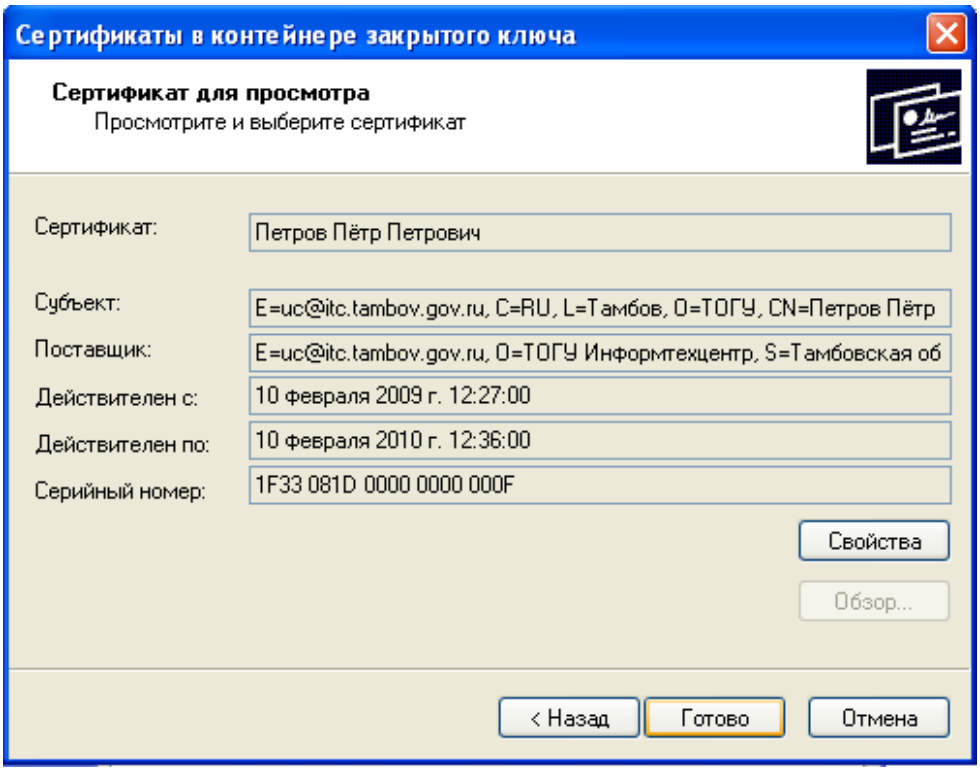
Теперь мы видим имя нашего рутокена в строке имени ключевого контейнера. Нажимаем **Далее** (Рисунок 29).

Рисунок 29.



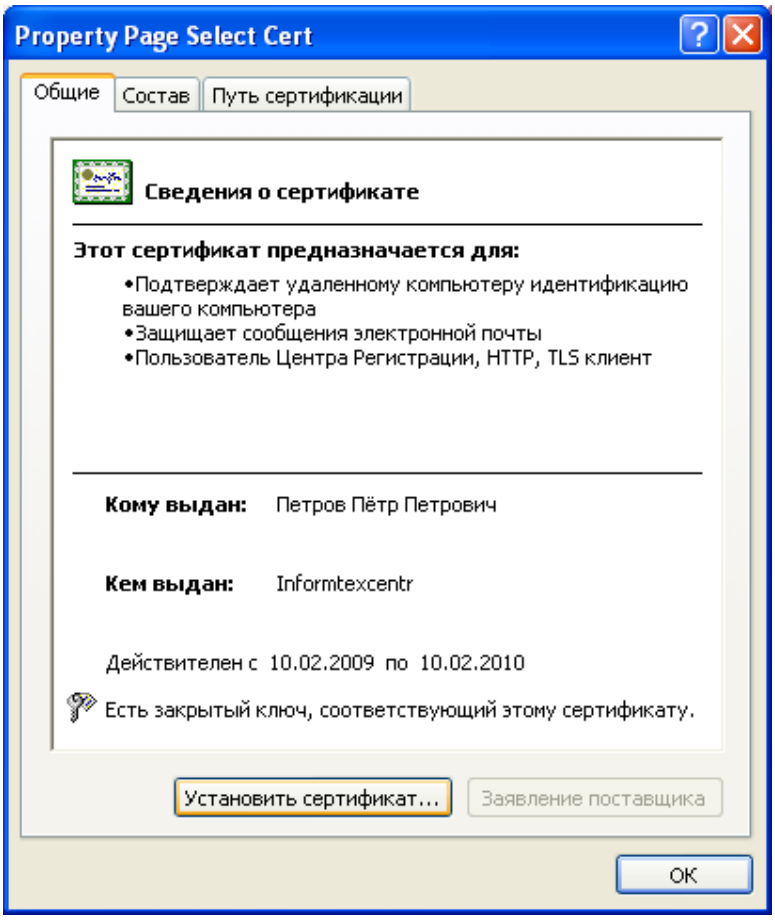
В следующем окне мы видим информацию о сертификате, который находится на данном ключевом носителе. Нажимаем кнопку **Свойства** (Рисунок 30).

Рисунок 30.



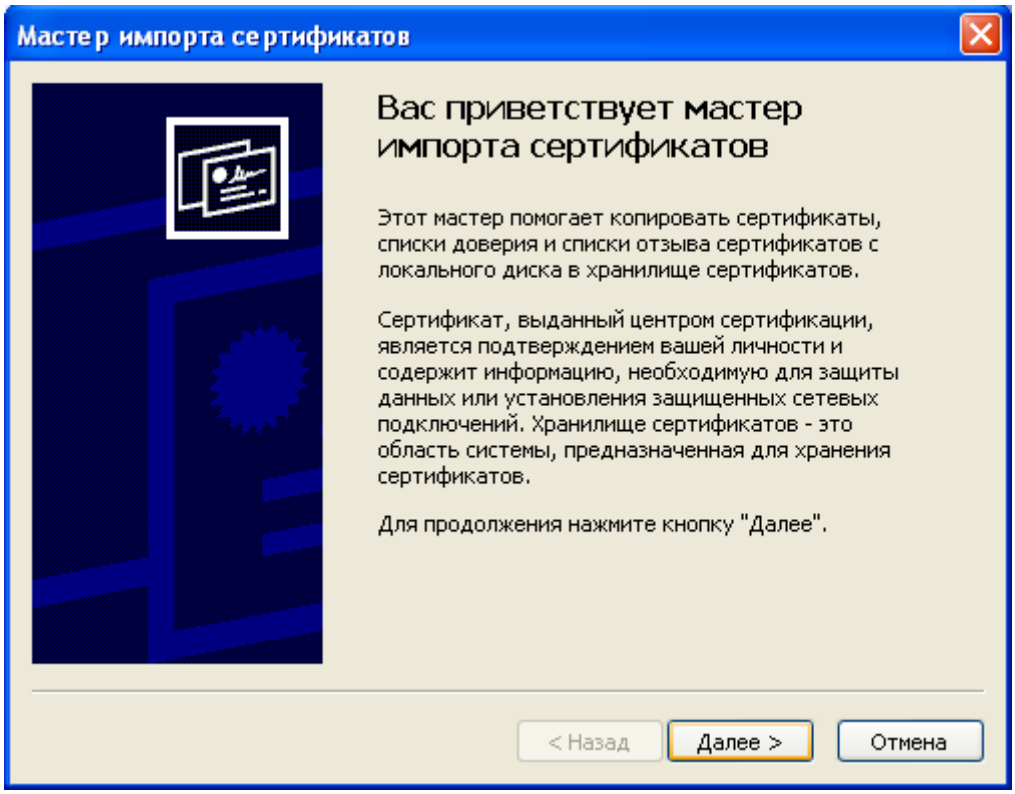
Открылось окно нашего личного сертификата. Нажимаем на кнопку **Установить сертификат** (Рисунок 31).

Рисунок 31.



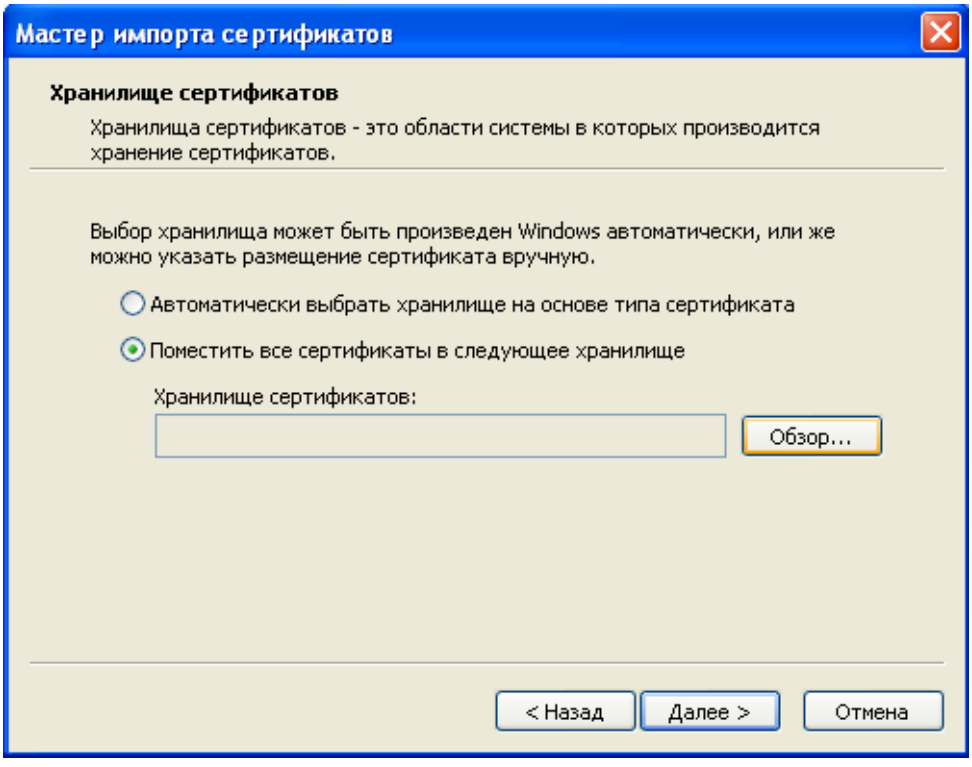
Откроется мастер установки сертификатов. Нажимаем **Далее** (Рисунок 32).

Рисунок 32.



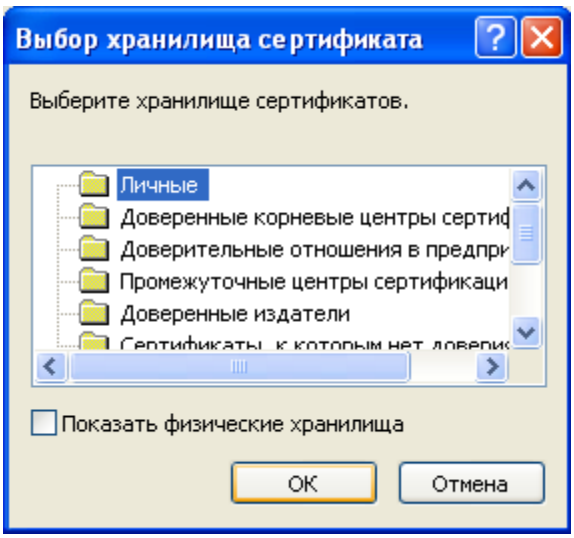
В окне выбора хранилища выбираем пункт **Поместить все сертификаты в следующее хранилище** и нажимаем кнопку **Обзор** (Рисунок 33).

Рисунок 33.



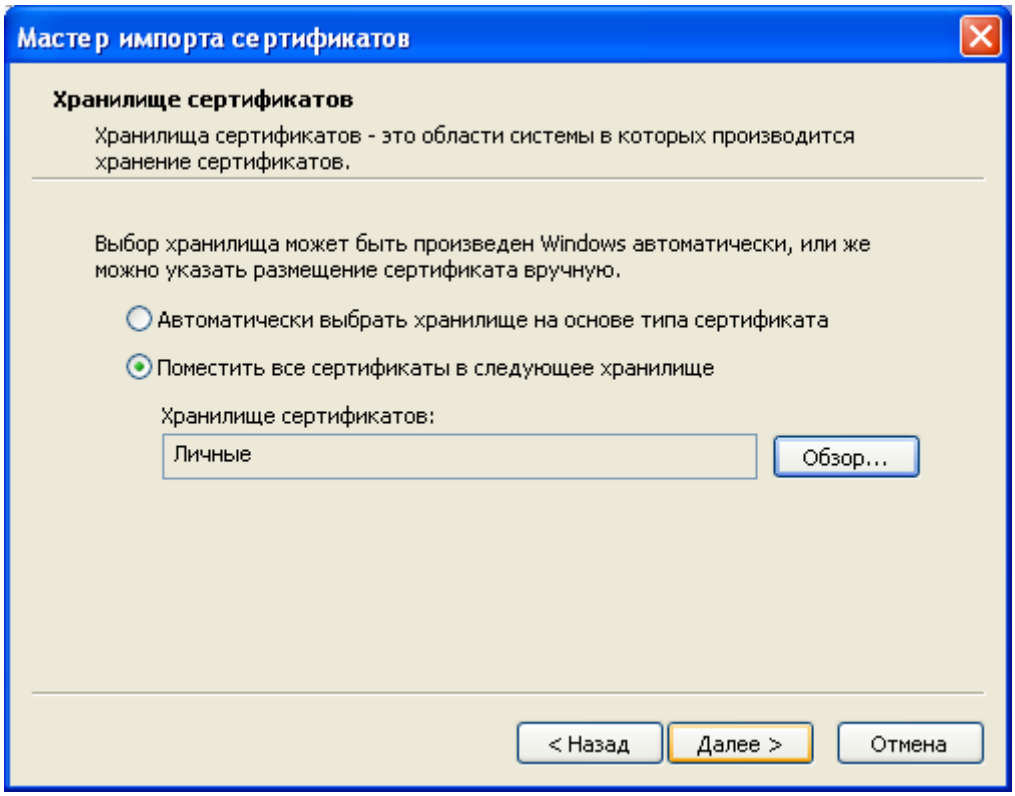
В открывшемся окне выбираем папку **Личные** и нажимаем **ОК** (Рисунок 34).

Рисунок 34.



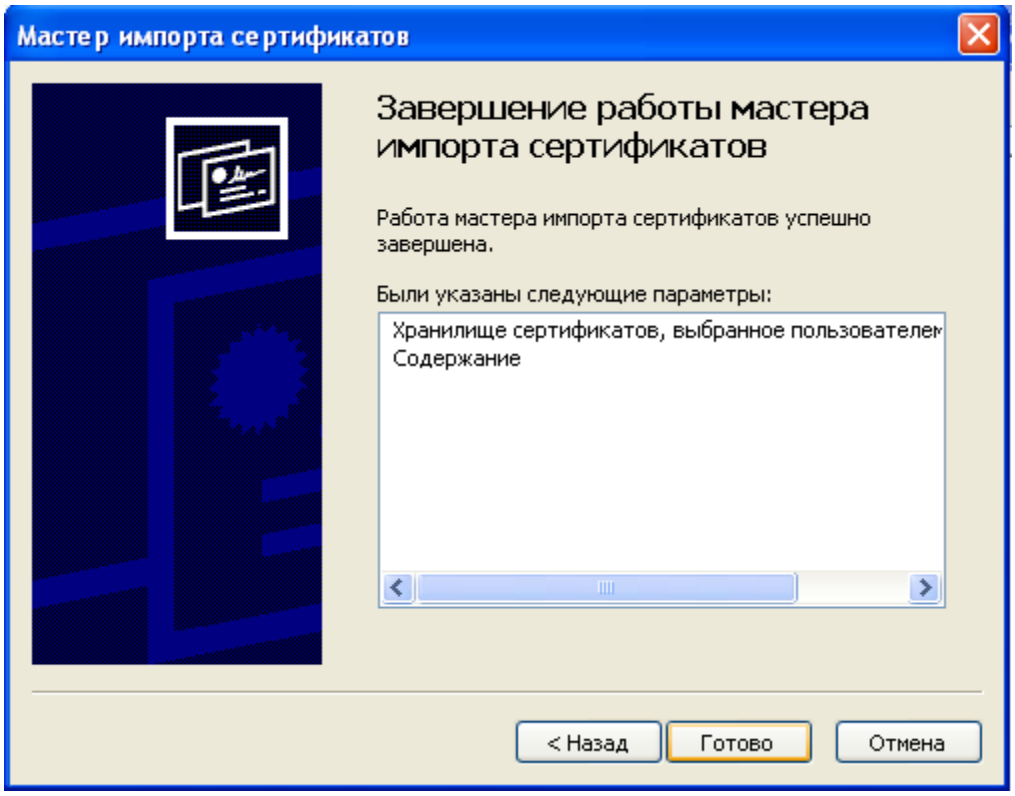
Хранилище выбрано. Нажимаем Далее (Рисунок 35).

Рисунок 35.



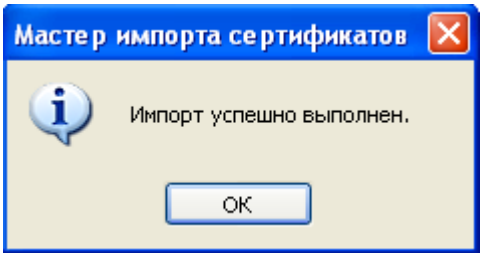
Завершаем работу мастера нажатием кнопки **Готово** (Рисунок 36).

Рисунок 36.



И видим сообщение об успешном импорте сертификата. Нажимаем **ОК** (Рисунок 37).

Рисунок 37.

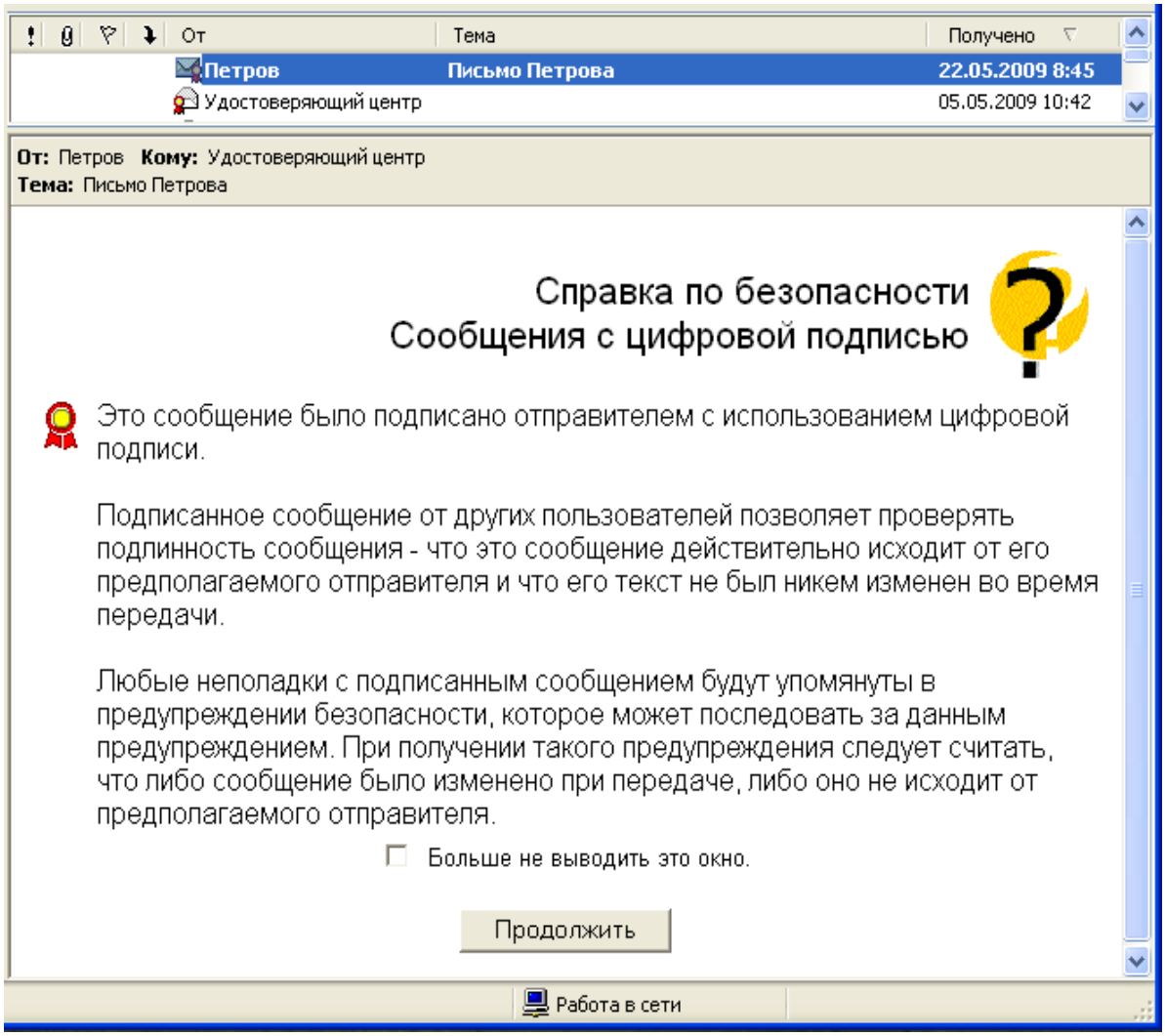


Ваш личный сертификат успешно установлен на компьютер.

4. Проверка достоверности сертификата при получении подписанного письма

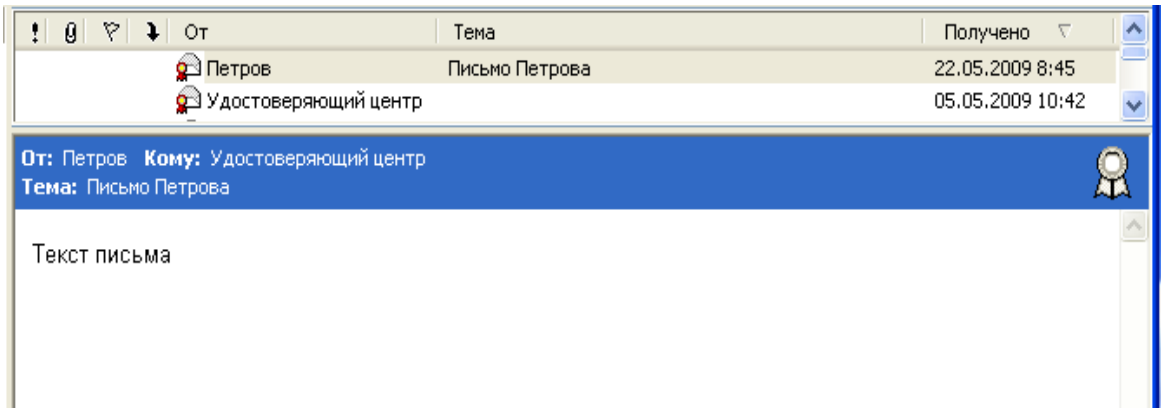
Получая электронное письмо, подписанное ЭЦП, (в данном случае от Петрова) в почтовой программе, открыв это письмо, мы видим следующее сообщение (Рисунок 38).

Рисунок 38.



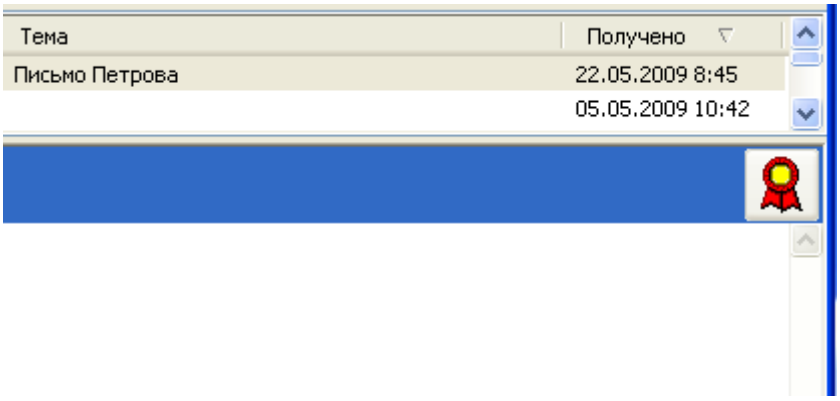
Для прочтения самого письма необходимо нажать на кнопку **Продолжить.** После чего мы сможем просмотреть содержимое письма (Рисунок 39).

Рисунок 39.



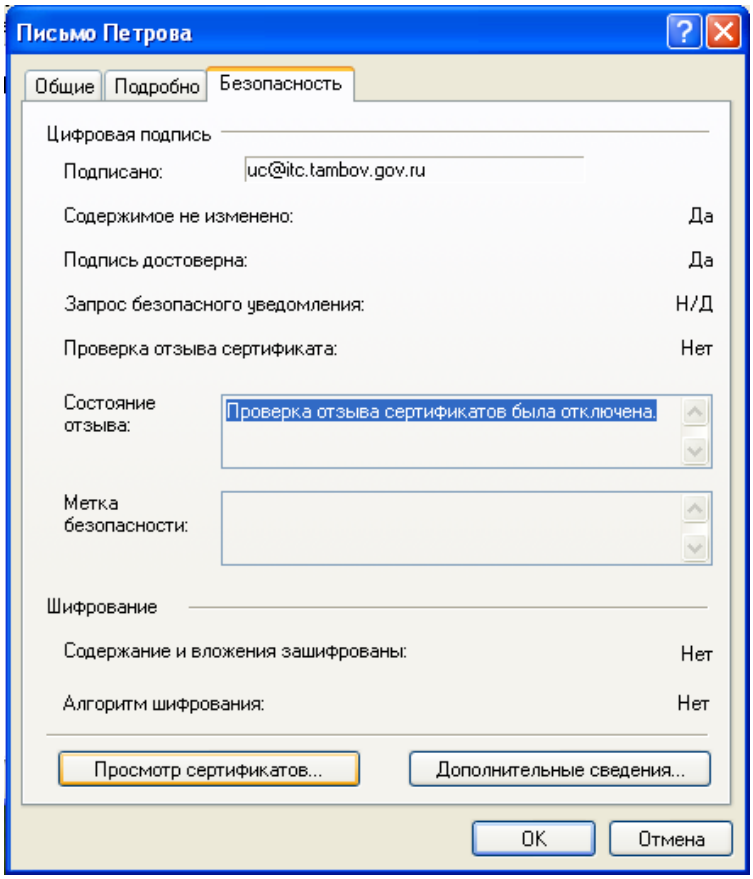
В правой части колонки, подсвеченной синим цветом, мы видим значок цифровой подписи, который становится цветным если навести на него курсор (Рисунок 40). Нажав на этот значок, мы можем просмотреть сертификат пользователя, который подписал это письмо, и проверить достоверность этого сертификата.

Рисунок 40.



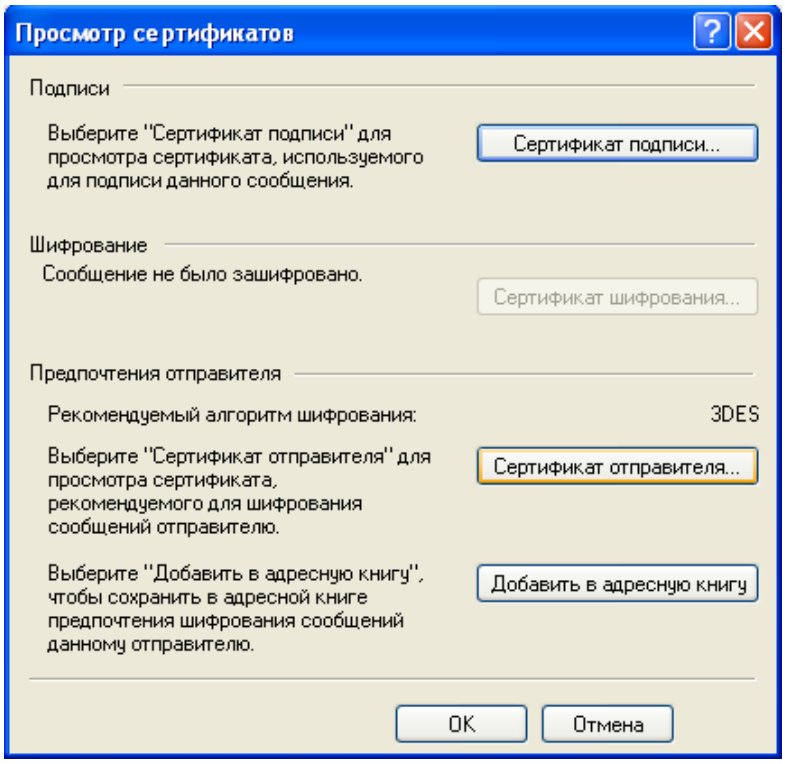
В открывшемся окне на вкладке **Безопасность** нужно нажать на кнопку **Просмотр сертификатов…** (Рисунок 41).

Рисунок 41.



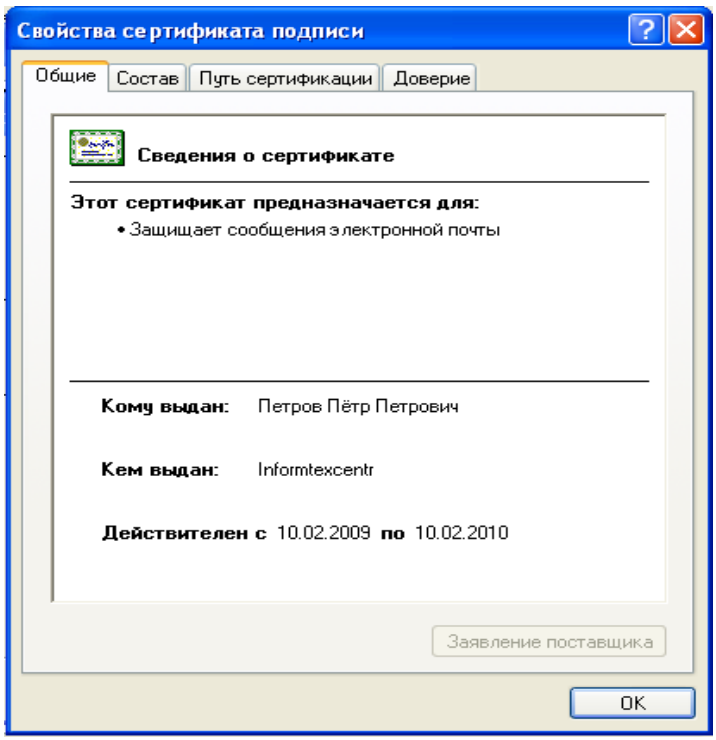
После чего мы можем просмотреть сертификат отправителя, нажав на кнопку **Сертификат отправителя** (Рисунок 42).

Рисунок 42.



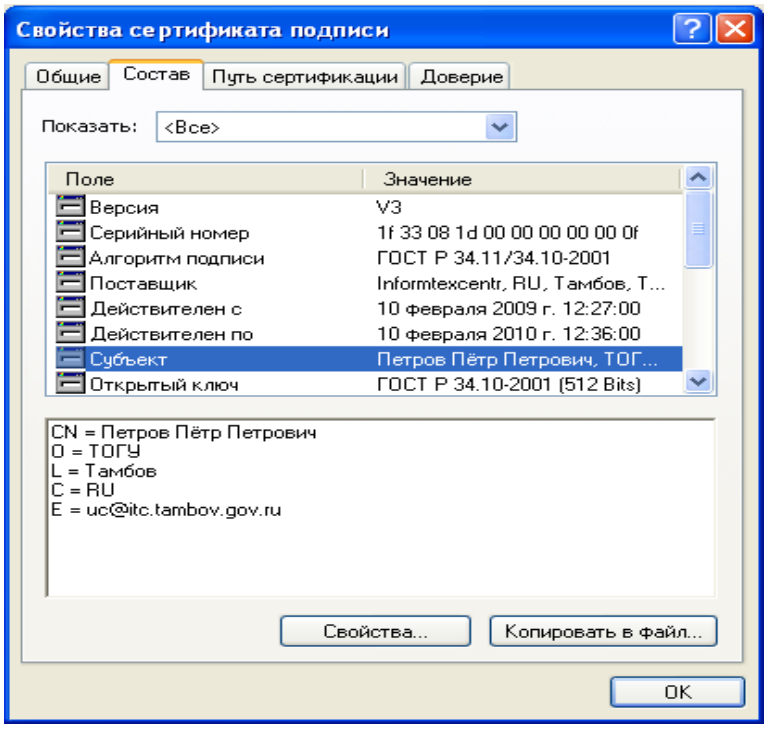
После чего откроется окно сертификата, в котором можно просмотреть информацию о самом сертификате и его владельце (Рисунок 43).

Рисунок 43.



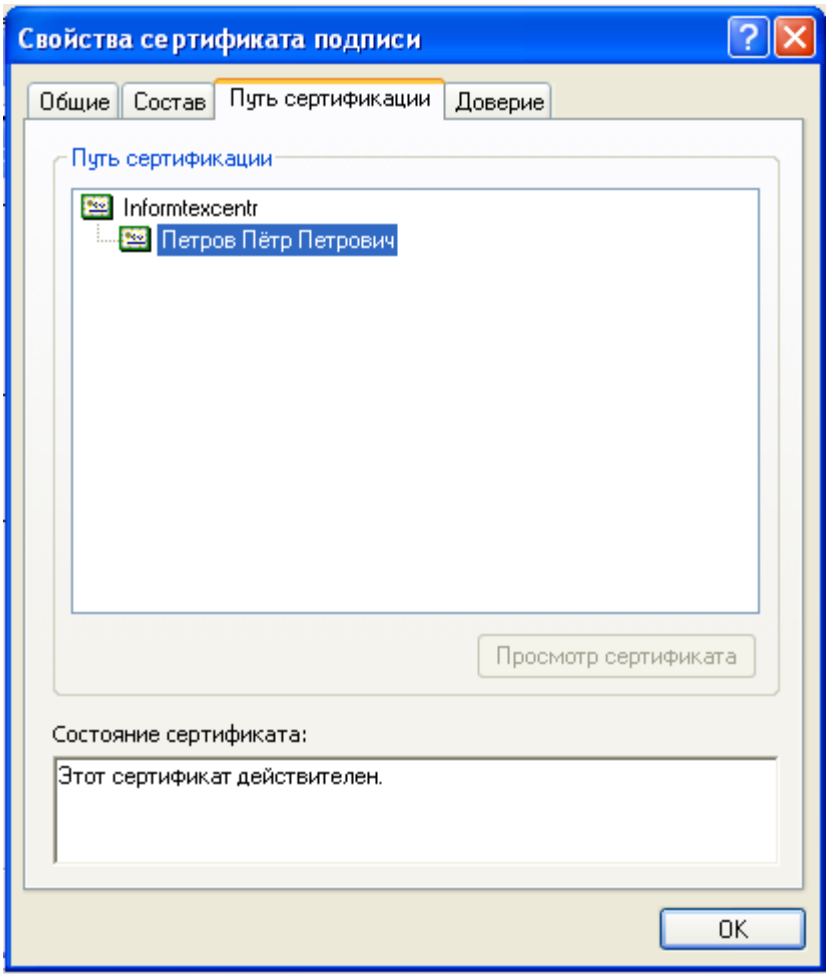
На вкладке **Состав** в пункте **Субъект** мы можем увидеть информацию о владельце сертификата (Рисунок 44). Здесь можно увидеть Ф.И.О. субъекта, организацию, отдел, город, регион и адрес электронной почты.

Рисунок 44.



На вкладке **Путь сертификата** можно просмотреть, действителен ли сертификат, и проследить путь сертификации до удостоверяющего центра, которым выдан данный сертификат (Рисунок 45).

Рисунок 45.



В графе **Состояние сертификата** мы видим, что сертификат действителен. Значит владелец сертификата на момент подписи имел право подписывать письмо своим личным сертификатом.