Инструкция по установке личного сертификата.

Оглавление

Введение.

В результате обращения заявителем в Региональный центр регистрации УФК по г. Москве за получением квалифицированного сертификата ключа проверки электронной подписи (далее - КСКП) должны быть получены КСКП на бумажном носителе и КСКП на электронном носителе (флешке). Для работы с электронной подписью необходимо установить полученный КСКП.

Подготовка к установке.

Перед установкой личного сертификата необходимо убедиться в следующем:

1. Вы получили в Удостоверяющем центре личный сертификат электронной подписи и знаете, где он находится.

2. При генерации ключа, запроса на изготовление квалифицированного ключа электронной подписи (далее - файл запроса) и заявления на получение квалифицированного ключа электронной подписи в Удостоверяющем центре Федерального казначейства (далее - заявление), **Вы сгенерировали ключ и знаете, где он находится**.

3. На рабочем месте установлены корневые сертификаты. ГУЦ и УЦ ФК в соответствии с инструкцией на сайте УФК по г. Москве. Инструкция расположена на сайте Управления в разделе ГИС/Удостоверяющий центр/Инструкции пользователя/Инструкция по установке корневых сертификатов ГУЦ и УЦ ФК.

4. На рабочем месте установлен драйвер для ключевого носителя. Ключевой носитель – отчуждаемый (съемный) носитель (дискета, флешка, токен), содержащий ключ электронной подписи. Полный список типов ключевых носителей, поддерживаемых при генерации ключа электронной подписи, расположен на сайте УФК по г. Москве в разделе ГИС/Удостоверяющий центр/Нормативные документы/Типы ключевых носителей, поддерживаемые при генерации КЭП.

5. Ключевой носитель подключен к рабочему месту. Если в качестве ключевого носителя используется флешка или дискета, то они должны отображаться как съемный диск в «Моем компьютере». Если в качестве ключевого носителя используется токен, то в токене должна постоянно гореть лампочка.

6. На рабочем месте установлена программа КриптоПро CSP. В программу КриптоПро CSP введена действующая лицензия. Ваш ключевой носитель должен быть указан в списке установленных считывателей. Для проверки необходимо запустить КриптоПро CSP (Пуск/Все программы/КРИПТО-ПРО/КриптоПроCSP), открыть вкладку «Оборудование», нажать кнопку «Настроить считыватели…», откроется окно «Управление считывателями» (Рис. 1 «Окно «Управление считывателями»).

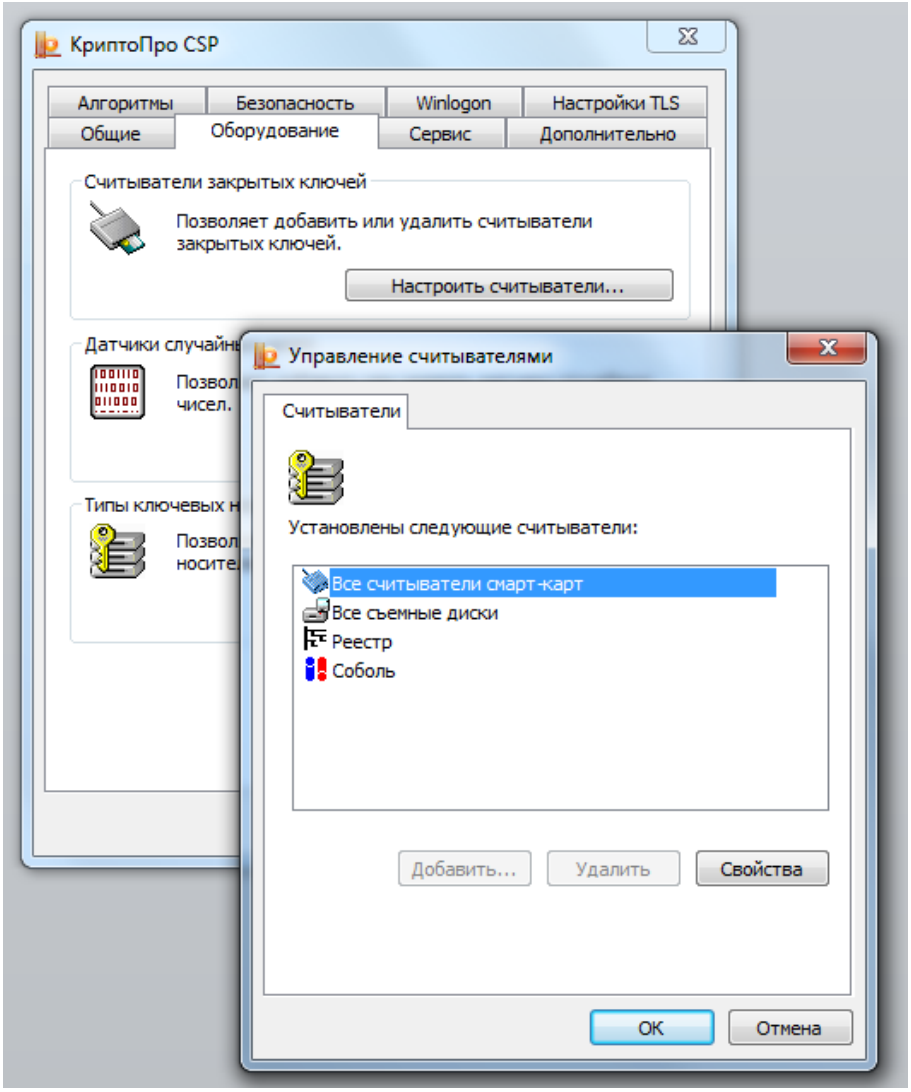

Рис. 1 «Окно «Управление считывателями».

Если ключевым носителем является Рутокен или Etoken, в списке должны присутствовать «Все считыватели смарт-карт». Если ключевым носителем является флешка или дискета, в списке должны присутствовать «Все съемные диски». В случае отсутствия в этом списке Вашего ключевого носителя, его необходимо добавить. Кнопка «Добавить» может быть недоступна, если у Вас отсутствуют права администратора.

Установка сертификата.

Для установки сертификата необходимо запустить КриптоПро CSP(Пуск/Все программы/КРИПТО-ПРО/КриптоПро CSP)(Рис. 2 «Пуск»), открыть вкладку «Сервис» (Рис. 3 «Вкладка «Сервис»), нажать кнопку «Установить личный сертификат…», откроется окно «Мастер установки личного сертификата» (Рис. 4 «Мастер установки личного сертификата»).

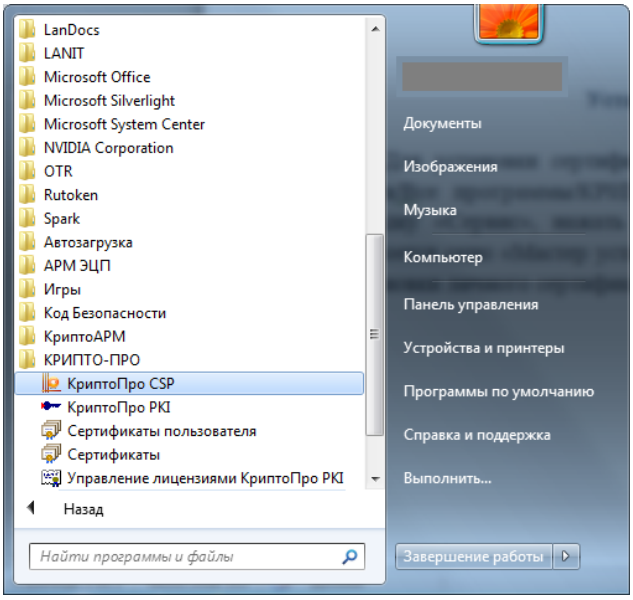

Рис. 2 «Пуск».

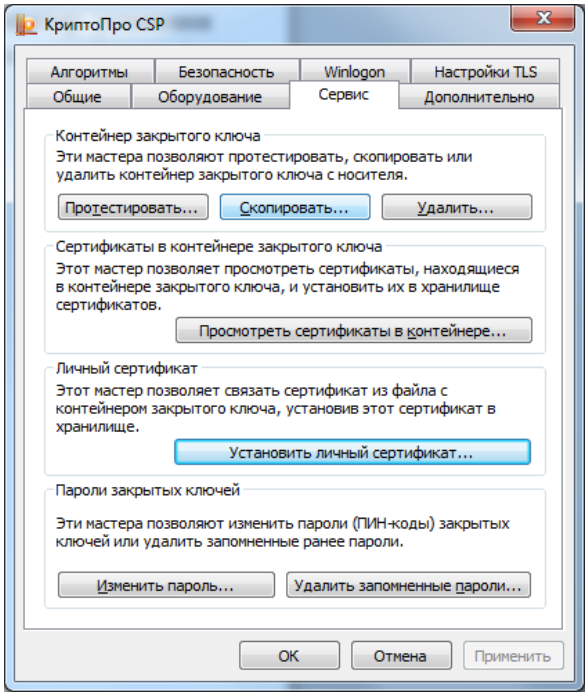

Рис. 3 «Вкладка «Сервис».

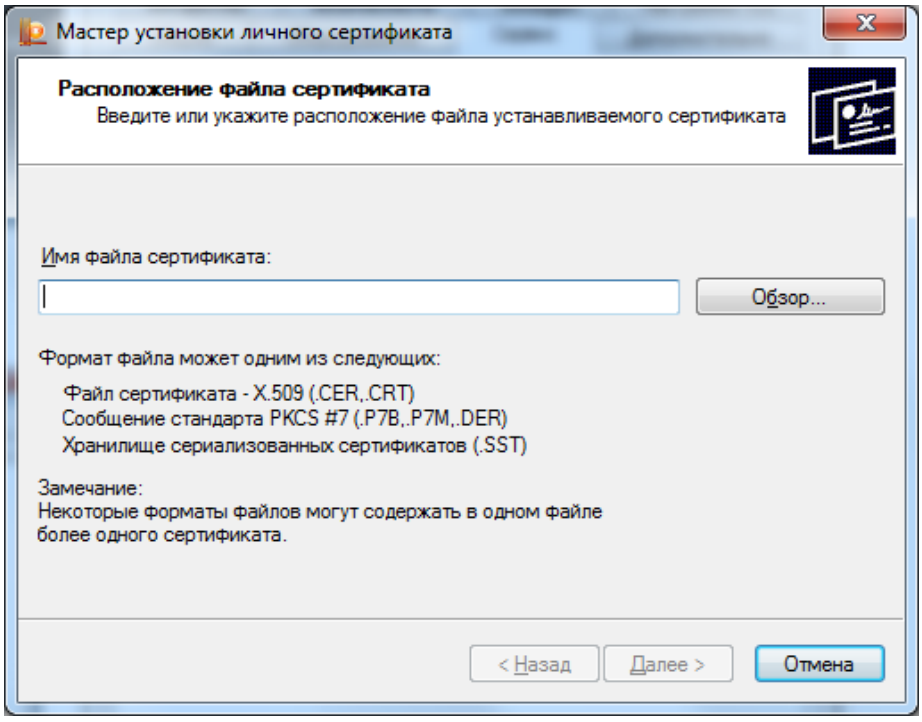

Рис. 4 «Мастер установки личного сертификата».

В данном окне необходимо нажать кнопку «Обзор…» и выбрать сертификат, полученный в Удостоверяющем центре (Рис. 5 «Выбор сертификата»). После Выбора сертификата нажать кнопку «Далее».

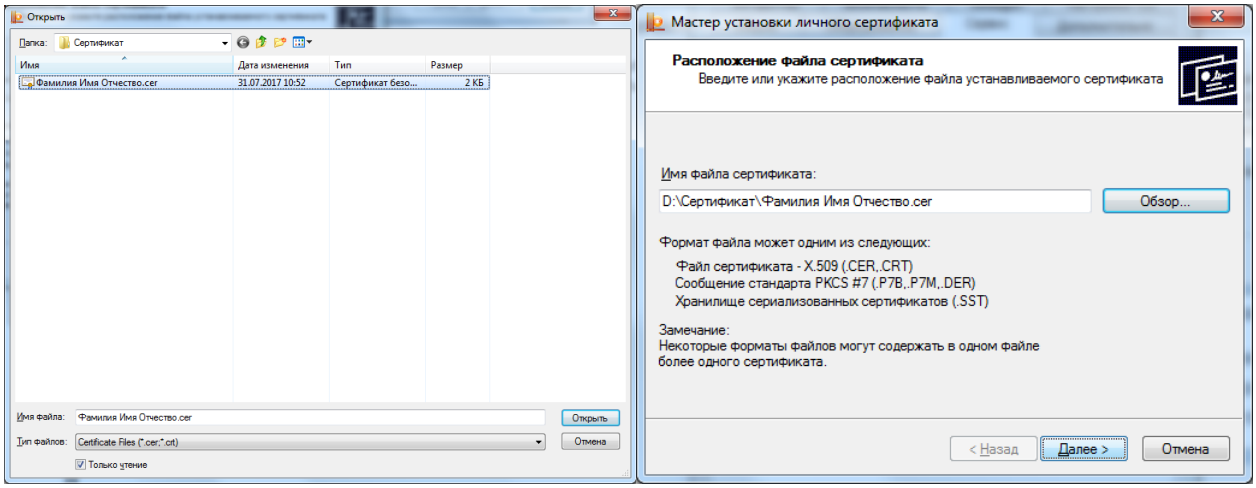

Рис. 5 «Выбор сертификата».

В следующем окне будут отображены сведения о сертификате. Если сведения соответствуют сертификату на бумажном носителе, необходимо нажать кнопку «Далее». (Рис. 6 «Сведения о сертификате»).

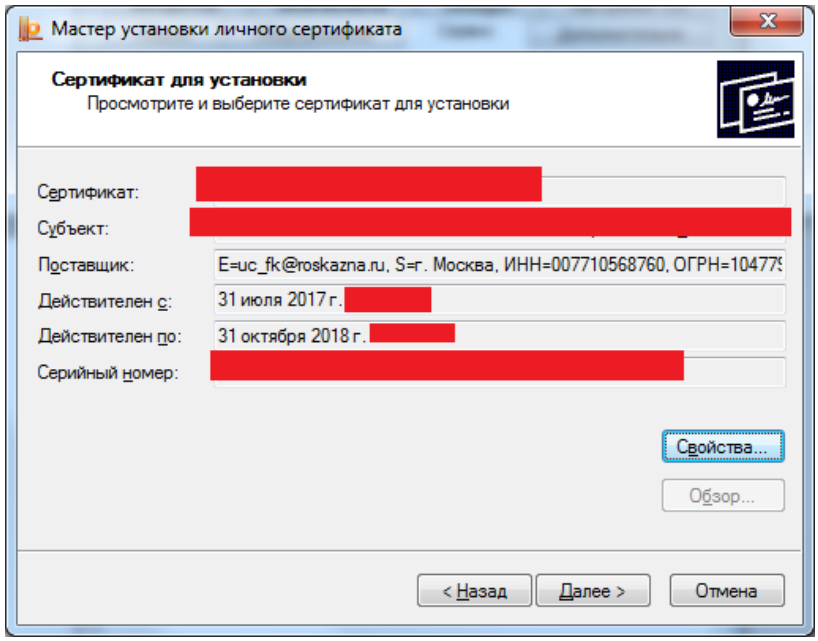

Рис. 6 «Сведения о сертификате».

В окне «Контейнер закрытого ключа» необходимо выбрать закрытый ключ, соответствующий сертификату.

ВАЖНО!

Закрытый ключ генерируется заявителем в программе «АРМ генерации ключей» на этапе создания файла запроса и заявления. В случае утери закрытого ключа, его восстановление невозможно, и для работы с электронной подписью необходимо подавать документы на изготовление нового сертификата, вместе с Заявлением на изменение статуса сертификата, с просьбой о прекращении действия сертификата, ключ от которого был утерян.

ВАЖНО!

Пароль и пин-код устанавливаются заявителем в программе «АРМ генерации ключей» на этапе создания файла запроса и заявления. В случае утери пин-кода или пароля, его восстановление невозможно, и для работы с электронной подписью необходимо подавать документы на изготовление нового сертификата, вместе с Заявлением на изменение статуса сертификата, с просьбой о прекращении действия сертификата, пароль или пин-код от которого был утерян.

ВАЖНО!

Если в качестве ключевого носителя используется флешка, то закрытый ключ на ней выглядит как папка, название которой заканчивается на «.000» (возможны варианты «.001», «.002» и т.д.). Закрытый ключ будет работать, только если он находится в корневой директории флешки (там, где его создала «АРМ генерации ключей»). Перемещение закрытого ключа как обычной папки в Windows запрещено.

ВАЖНО!

Если при установке сертификата Вы обнаружили отсутствие закрытого ключа, важно понимать, что НЕВОЗМОЖНО создать заявление и файл запроса, не создав закрытый ключ. Если по каким-либо причинам закрытый ключ не записался на ключевой носитель, он мог остаться в Реестре компьютера, на котором генерировались заявление и файл запроса. С помощью кнопки «Скопировать…» на вкладке «Сервис» в программе КриптоПро CSP необходимо скопировать закрытый ключ из реестра на ключевой носитель. После копирования ключа необходимо удалить его из реестра (кнопка «Удалить…» на вкладке «Сервис»)

Выбрать закрытый ключ можно двумя способами: автоматически или вручную. Для выбора закрытого ключа автоматически необходимо поставить галочку перед словами «Найти контейнер автоматически» (Рис. 7 «Автоматический поиск ключа»)

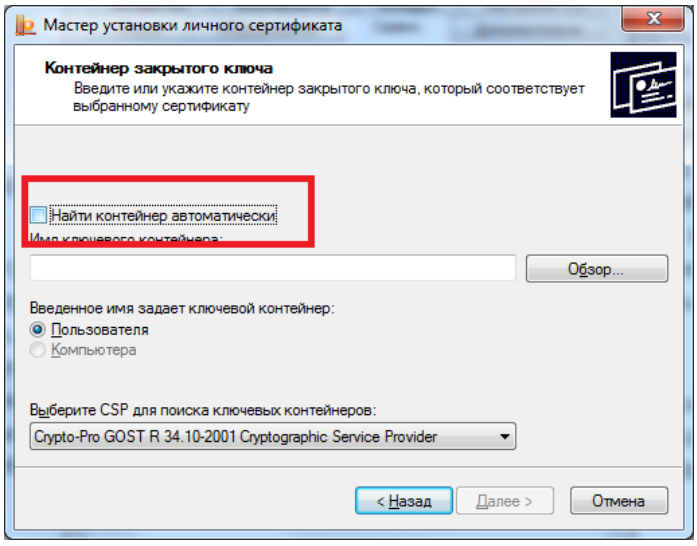

Рис. 7 «Автоматический поиск ключа».

Для выбора закрытого ключа вручную, необходимо нажать кнопку «Обзор…», и в открывшемся окне «Выбор ключевого контейнера» выбрать закрытый ключ, соответствующий сертификату (Рис. 8 «Выбор ключа вручную»).

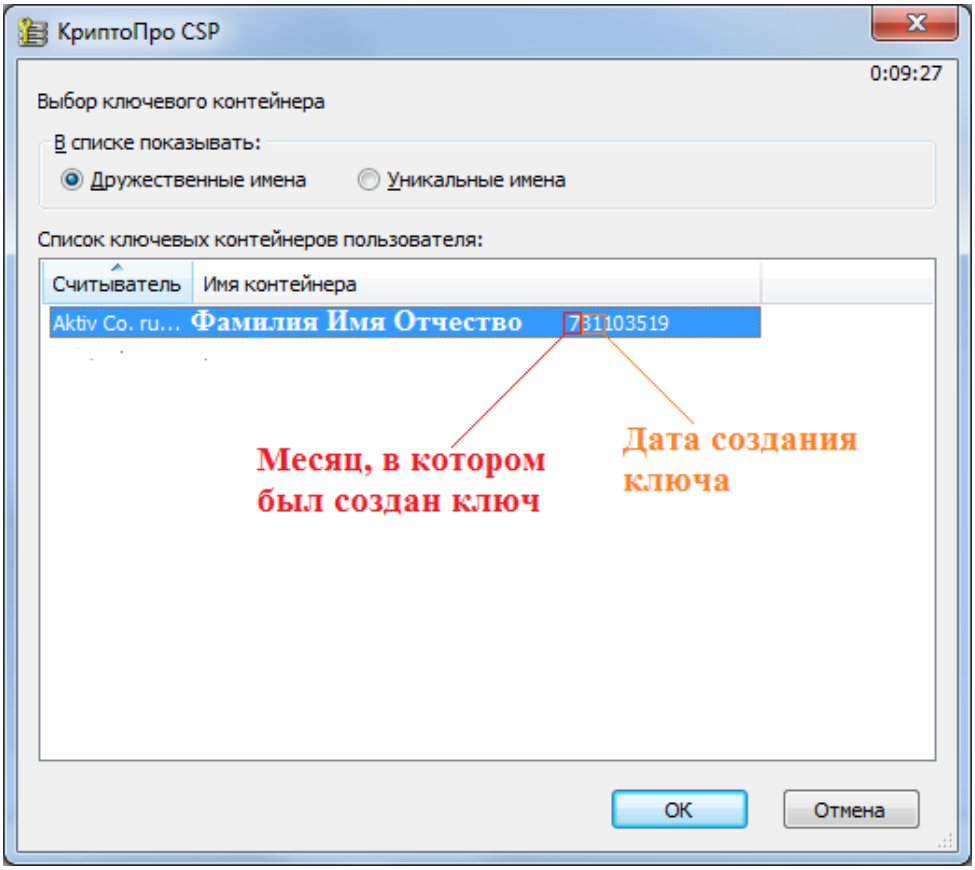

Рис. 8 «Выбор ключа вручную».

После выбора сертификата необходимо нажать кнопку «Далее». Появится окно выбора хранилища сертификатов. Если хранилище «Личное» автоматически не выбрано, необходимо нажать кнопку «Обзор» и выбрать его вручную (Рис. 9 «Выбор хранилища»).

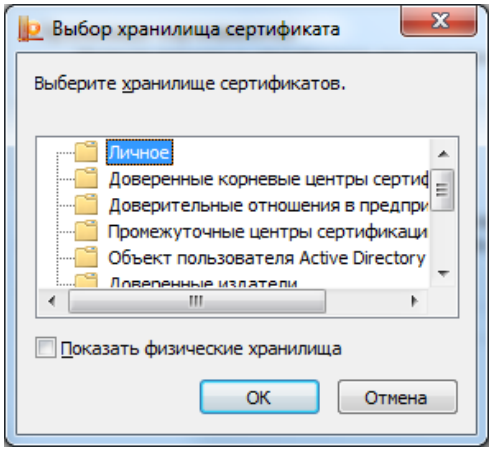

Рис. 9 «Выбор хранилища».

Так же рекомендуется поставить галочку напротив слов «Установить сертификат (цепочку сертификатов) в контейнер». Установка сертификата в контейнер не является обязательным условием для работы с электронной подписью в системах, оператором которых является Федеральное казначейство (Рис. 10 «Установка сертификата в контейнер»). После выбора хранилища необходимо нажать кнопку «Далее».

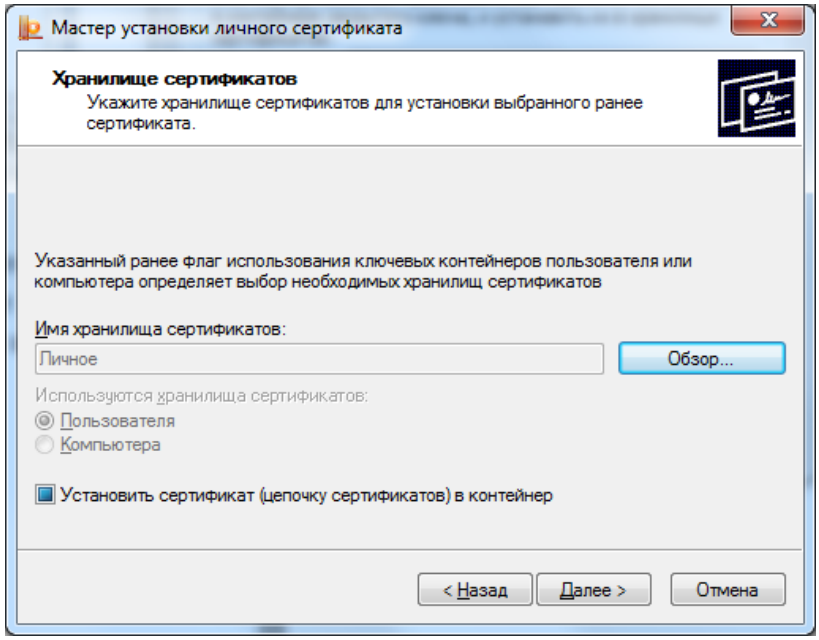

Рис. 10 «Установка сертификата в контейнер».

В окне «Завершение работы мастера установки личного сертификата» необходимо нажать кнопку «Готово» (Рис. 11 «Завершение работы мастера»).

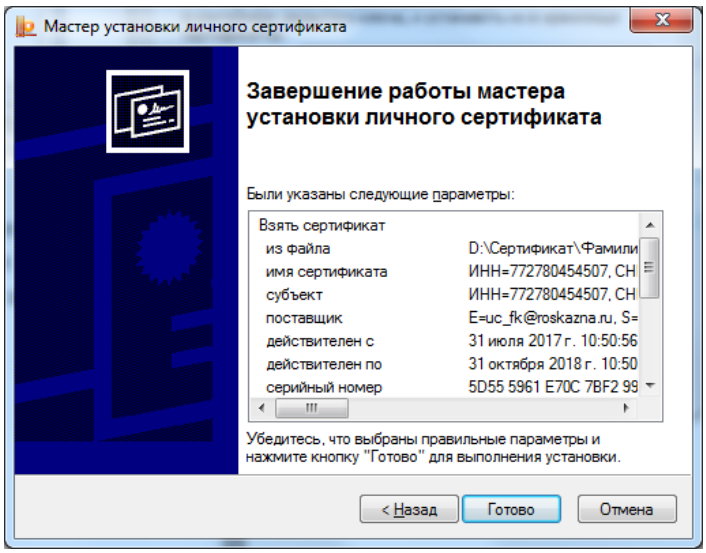

Рис. 11 «Завершение работы мастера».

Заключение.

Установка личного сертификата завершена. Срок действия сертификата равен одному году и трём месяцам с момента его издания Удостоверяющим центром. Плановая смена сертификата осуществляется не ранее двадцати календарных дней до окончания срока действия.