ИНСТРУКЦИЯ
по
экспорту сертификата в файл
формата **DER (.cer).**

ВНИМАНИЕ!!!

А. Убедитесь, что у вас на компьютере установлено КриптоПро.

Б. Убедитесь, что КриптоПро настроено верно.

В. При использовании в качестве ключевых носителей **eToken** или **Rutoken** установлено соответствующие драйвера и модули поддержки для КриптоПро.

Г. Убедитесь, что ключевые контейнеры и сертификаты корректно просматриваются через КриптоПро.

Порядок выгрузки:

1. Запустите КриптоПро CSP. Для этого перейдите в «Панель Управления» и запустите КриптоПро двойным щелчком левой кнопки мыши по иконке «КриптоПро CSP» 

(рис.1). Обладателям КриптоПро версии 3.6 запуск программы также можно выполнить запуск через меню «Пуск» => «Программы» => «Крипто-Про» => «КриптоПро **CSP»** (рис.2).

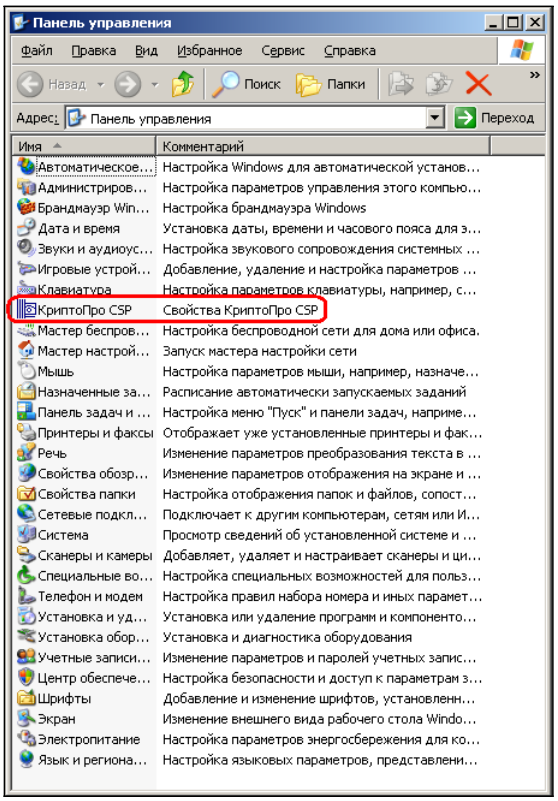

Рис.1

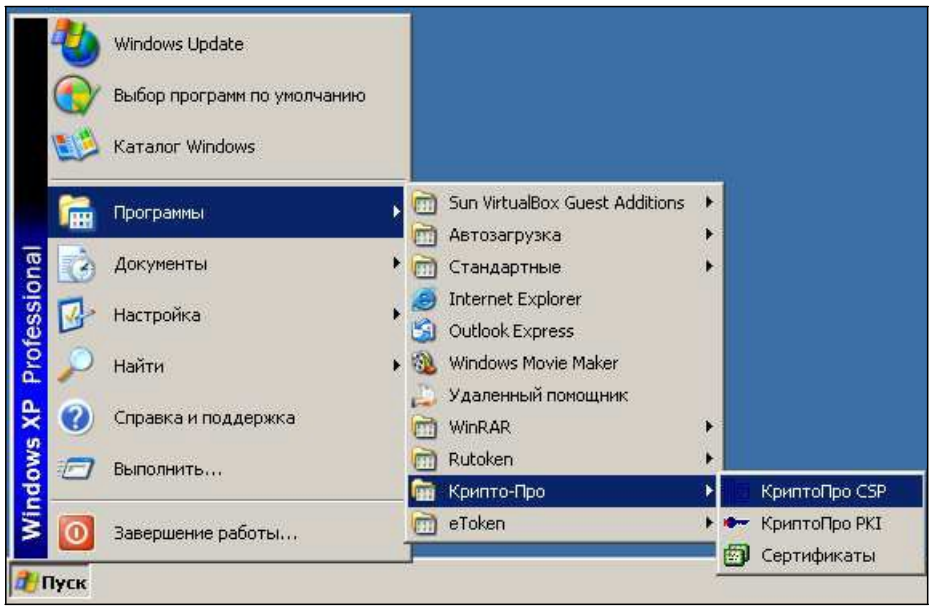

Рис.2

2. В КриптоПро перейдите на вкладку «Сервис» и нажмите кнопку «Просмотреть сертификаты в контейнере**…**» (рис.3).

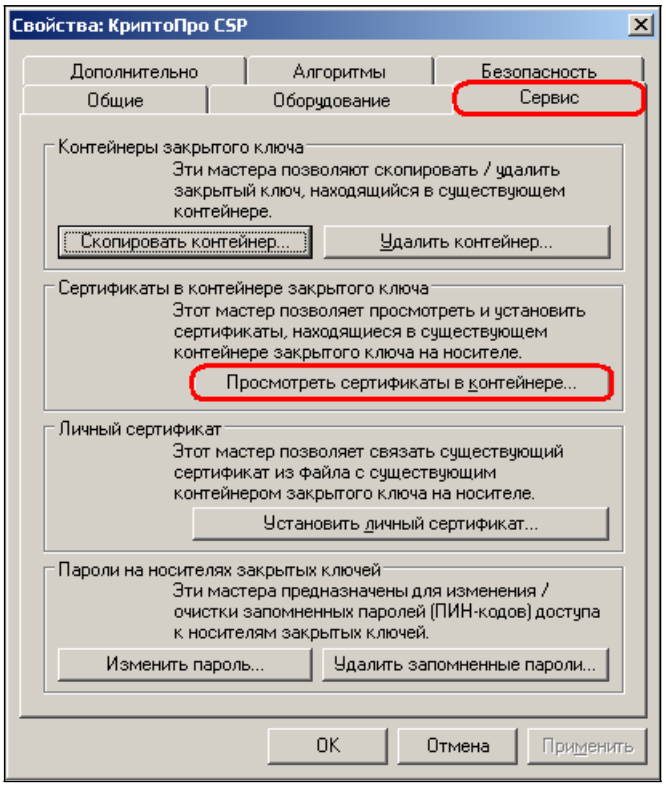

Рис.3

3. В открывшемся окне нажмите кнопку «Обзор» напротив поля «Имя ключевого контейнера» (рис.4).

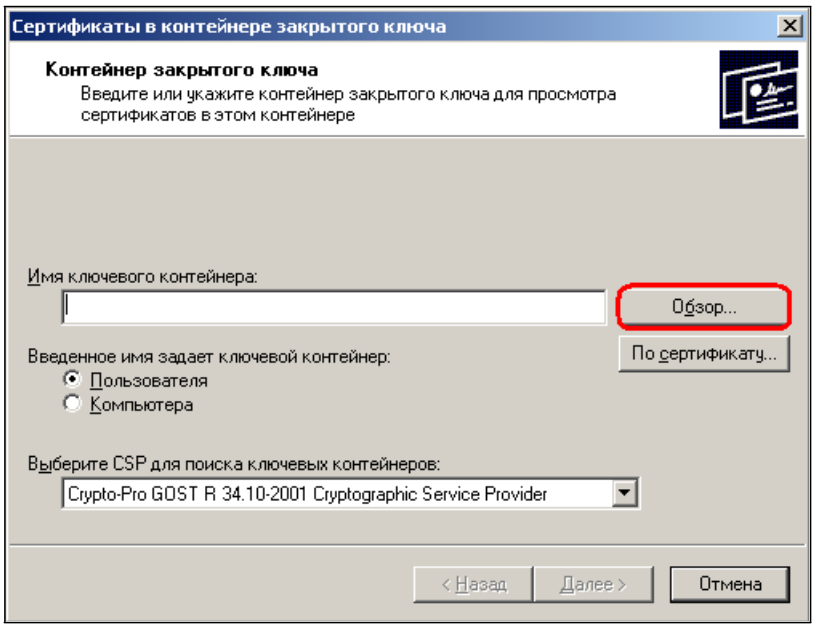

Рис.4

4. В указанном списке выберите имя ключевого контейнера на вашем носителе и нажмите кнопку «ОК» (рис.5).

ВНИМАНИЕ!

А. Имя ключевого контейнера может быть произвольным. Скорее всего – это будет уникальный буквенно-цифровой идентификатор.

Б. На каждом носителе могут присутствовать несколько контейнеров. Определить, какой из них содержит необходимый нам сертификат, возможно исключительно методом перебора и просмотра содержимого (сертификата).

В.
Если в качестве ключевого носителя используется дискета – тогда в поле «Считыватель» необходимо искать контейнеры, расположенные на считывателе «Дисковод А» (Как правило. Но могут быть и другие буквы для дисковода).

Если в качестве ключевого носителя используется ***eToken*** - тогда в поле «Считыватель» необходимо искать контейнеры, расположенные на считывателях **«AKS ifdh 0»** или **«AKS ifdh 1».**

Если в качестве ключевого носителя используется ***Rutoken*** - тогда в поле «Считыватель» необходимо искать контейнеры, расположенные на считывателях **«Active Co. ruToken 0», «Active Co. ruToken 1»** или **«Active Co. ruToken 2»**.

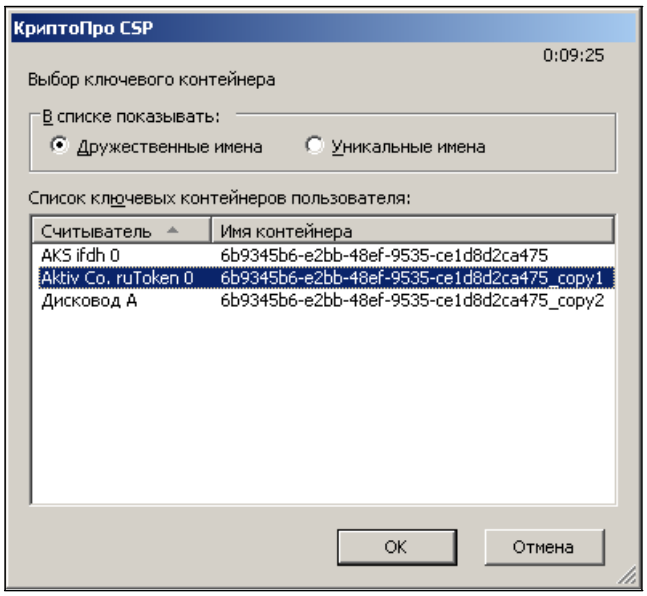

Рис.5

5. После этого вы будете возвращены в предыдущее окно, только в поле «Имя ключевого контейнера» будет присутствовать имя выбранного вами контейнера (рис.6). Нажмите кнопку «Далее».

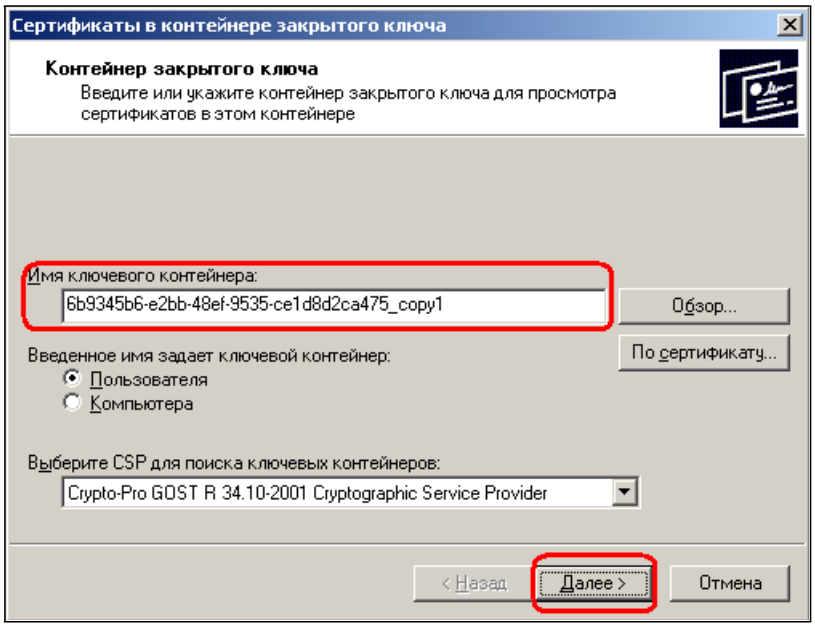

Рис.6

6. После этого откроется окно, с данными о владельце сертификата (рис.7). Убедитесь, что сертификат в выбранном контейнере является искомым (проверьте ФИО владельца и срок действия сертификата) и нажмите кнопку «Свойства».

В противном случае нажмите кнопку «Назад» и повторите п.п. 3-5 перебирая по очереди все контейнеры до нахождения требуемого сертификата.

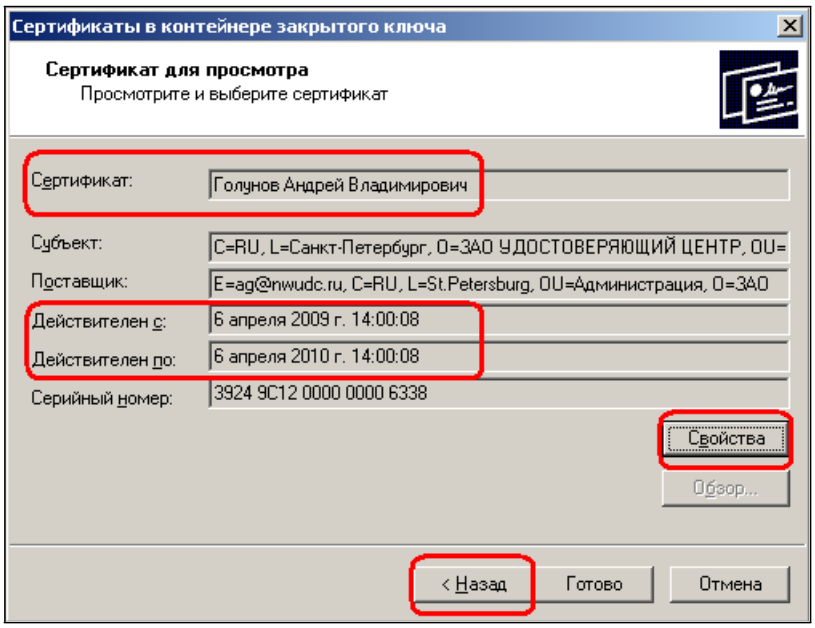

Рис.7

7. В открывшемся окне проверьте:
1) что значок сертификата не имеет на своем изображении желтых треугольников с восклицательным знаком внутри; красных кругов с белым крестиком;
2) назначение сертификата;
3) наличие закрытого ключа, соответствующего данному сертификату.
и перейдите на вкладку «Путь сертификации» (рис.8).

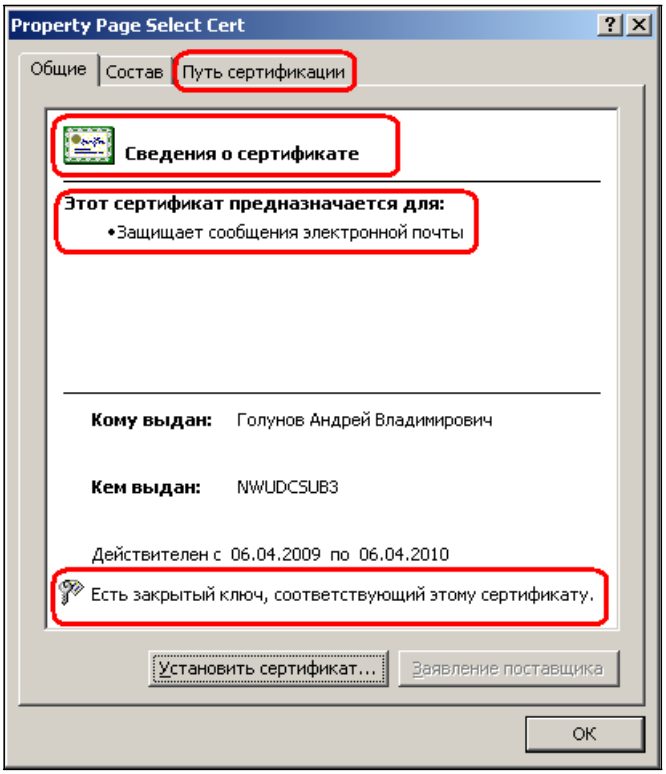

Рис.8

8. На вкладке «Путь сертификации» проверьте, что цепочка сертификатов выстраивается верно. А также статус сертификата (Должен быть: «Этот сертификат действителен»). Затем следует перейти на вкладку «Состав».

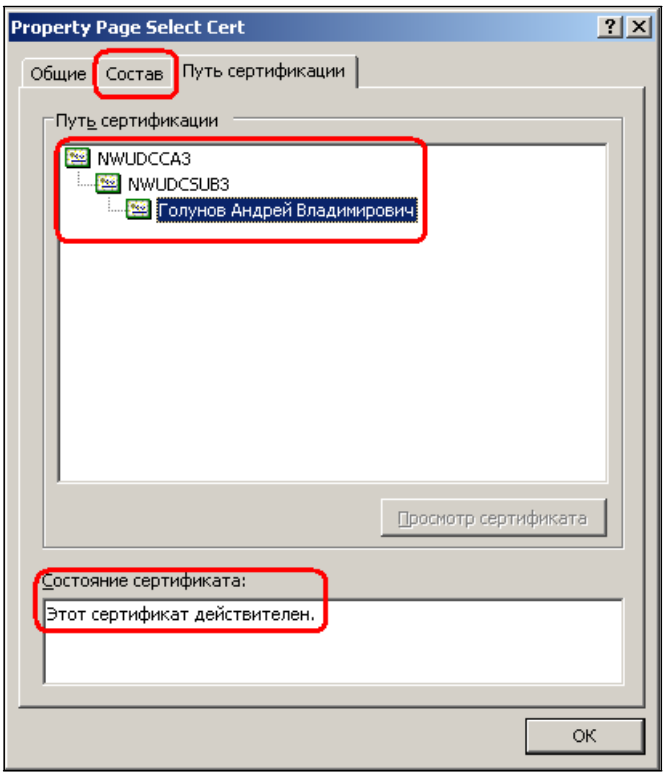

Рис.9

Если цепочка сертификатов не выстраивается (в цепочке присутствует только 1 ваш сертификат с желтым треугольником и восклицательным знаком внутри), возможно у вас не установлены корневые сертификаты нашего удостоверяющего центра.

Если какие-либо сертификаты не действительны или повреждены (кранный круг с белым крестиком внутри) следует переустановить корневые сертификаты. Также настоятельно рекомендуется проверить компьютер на наличие вирусов.

9. На вкладке «Состав» нажмите кнопку «Копировать в файл» (рис.10).

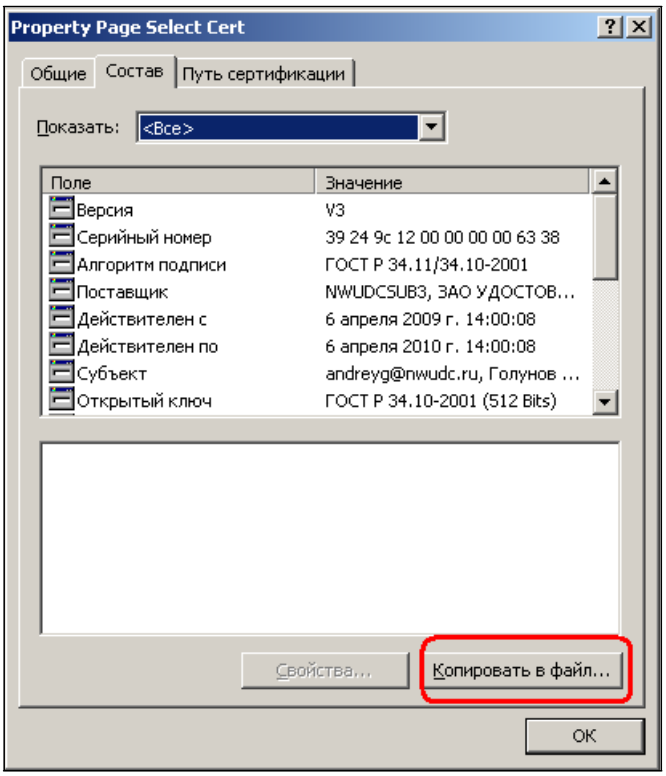

Рис.10

10. В окне мастера экспорта сертификатов нажмите кнопку «Далее» (рис.11).

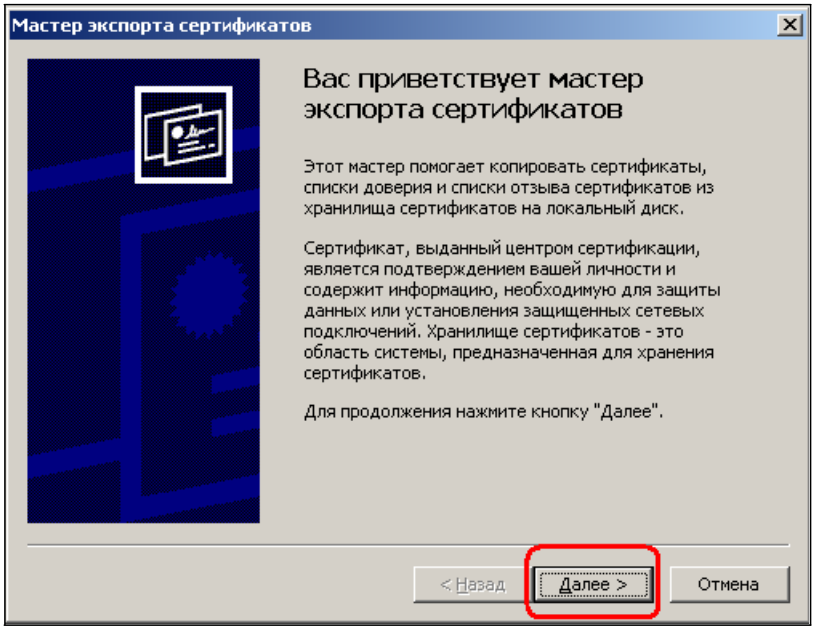

Рис.11

11. Выберите пункт «Нет, не экспортировать закрытый ключ» и нажмите кнопку «Далее» (рис.12).

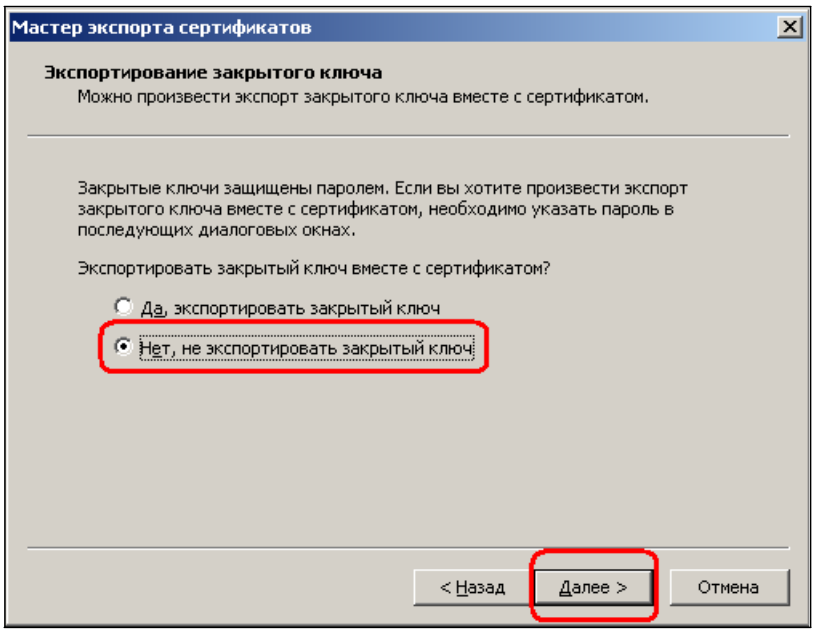

Рис.12

12. Выберите необходимый формат файла (как правило, требуется сертификат в формате DER(.cer)) и нажмите кнопку «Далее» (рис.13).

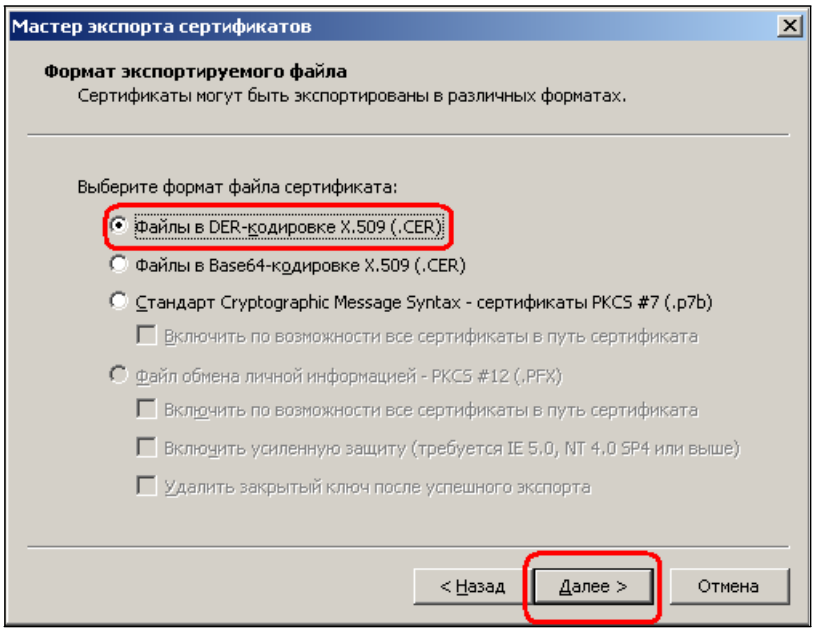

Рис.13

13. Укажите имя файла, в который вы хотите сохранить сертификат. По умолчанию сертификат будет сохранен в директории **«C:\Documents and Settings**\<Имя пользователя>**»**. Если вы хотите сохранить файл в другое место, следует нажать кнопку «Обзор» и выбрать другое размещение. Затем нажмите кнопку «Далее» (рис.14).

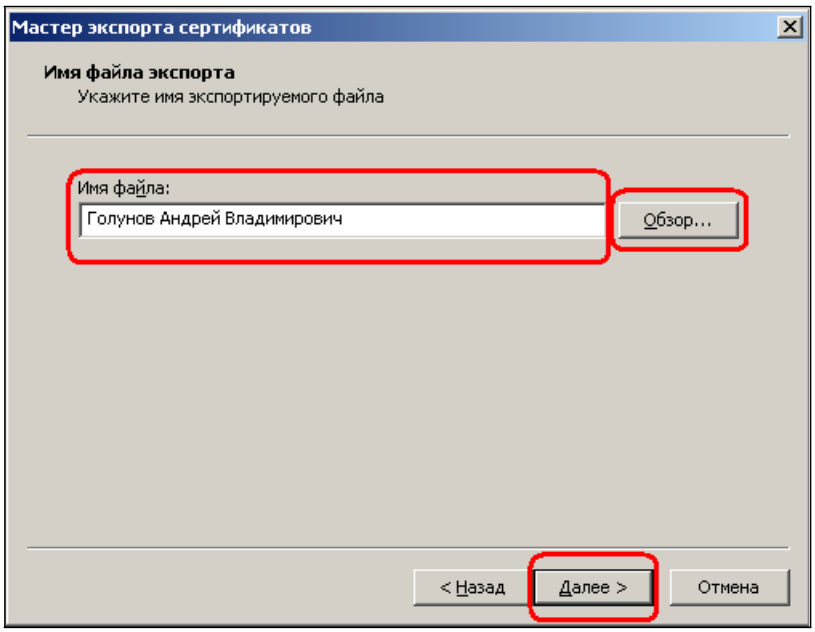

Рис.14

14. В следующем окне нажмите кнопку «Готово» (рис.15).

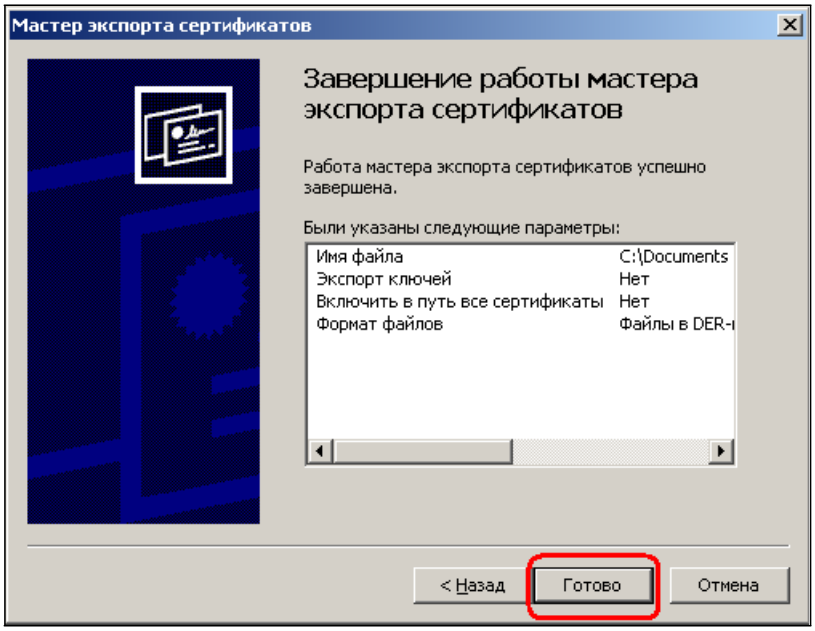

Рис.15

15. В результате появится сообщение об успешном экспорте сертификата (рис.16). Нажмите кнопку **«Ок».**

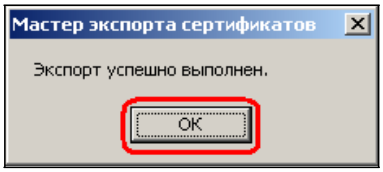

Рис.17

16. Поздравляем. На этом экспорт сертификата в файл закончен. Если вам не надо экспортировать другие сертификаты, можете закрыть все открытые окна КриптоПро.