ИНСТРУКЦИЯ
по установке личного сертификата

ВНИМАНИЕ!

А. Убедитесь, что у Вас на компьютере установлен КриптоПро CSP. Рекомендуем использовать сертифицированную версию ПО - КриптоПро CSP 3.6 R2 (версия продукта 3.6.6497).

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

В. Убедитесь, что настройки оборудования (считывателей и ключевых носителей) в КриптоПро CSP произведены правильно.

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

Д. Рекомендуется до установки Вашего личного сертификата установить соответствующие ему сертификаты нашего удостоверяющего центра. Чаще всего это корневые Сертификаты Удостоверяющего Центра, однако иногда требуются и сертификаты для взаимодоверия (кросс-сертификаты). Подробнее см. ИНСТРУКЦИЮ по УСТАНОВКЕ корневых сертификатов**.**

Порядок установки личного сертификата:

1. Запустите КриптоПро CSP. Для этого перейдите в «Панель Управления» («Пуск» => «Настройка» => «Панель управления») и запустите КриптоПро двойным щелчком левой кнопки мыши по иконке «КриптоПро CSP» (рис.1).

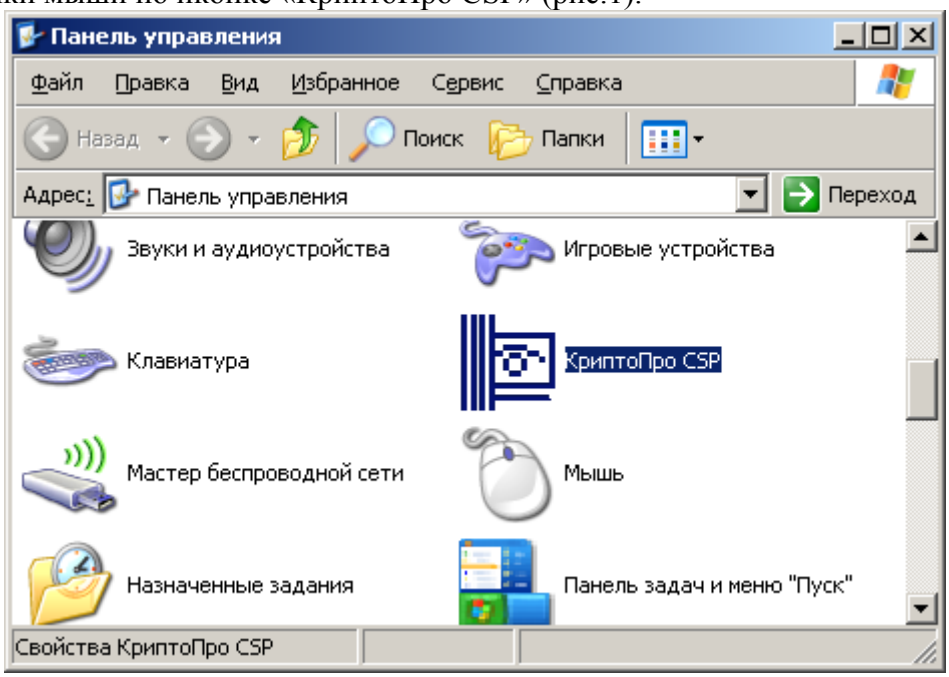

Рис.1

Для обладателей КриптоПро 3.6 запуск программы можно выполнить через меню «Пуск» => «Программы» => «Крипто-Про» => «КриптоПро CSP» (рис.2).

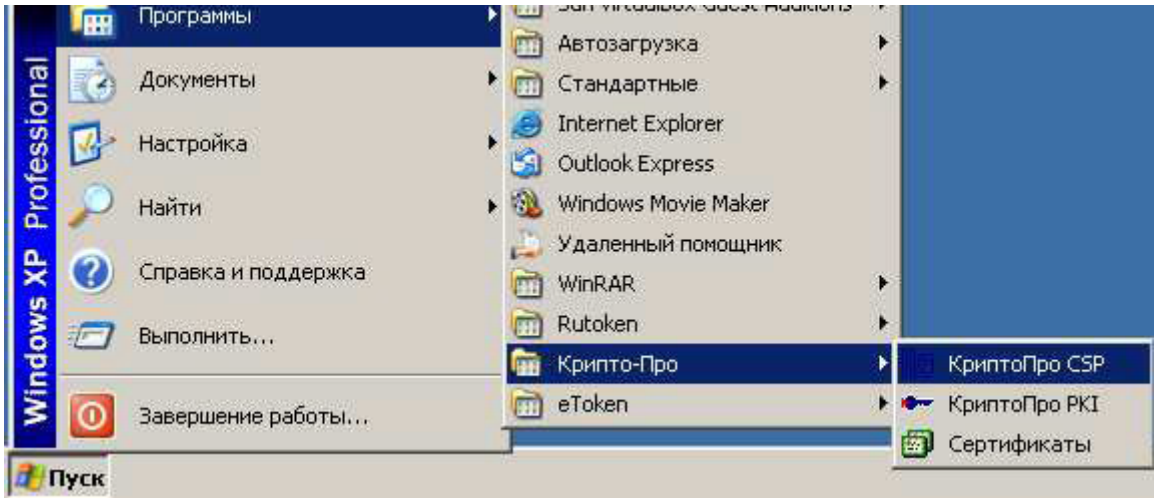

Рис.2

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

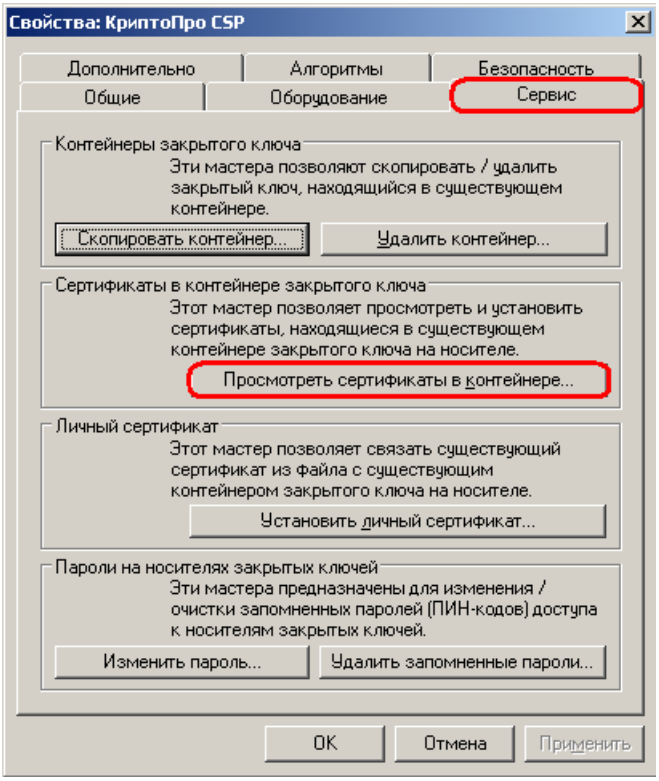

Рис.3

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

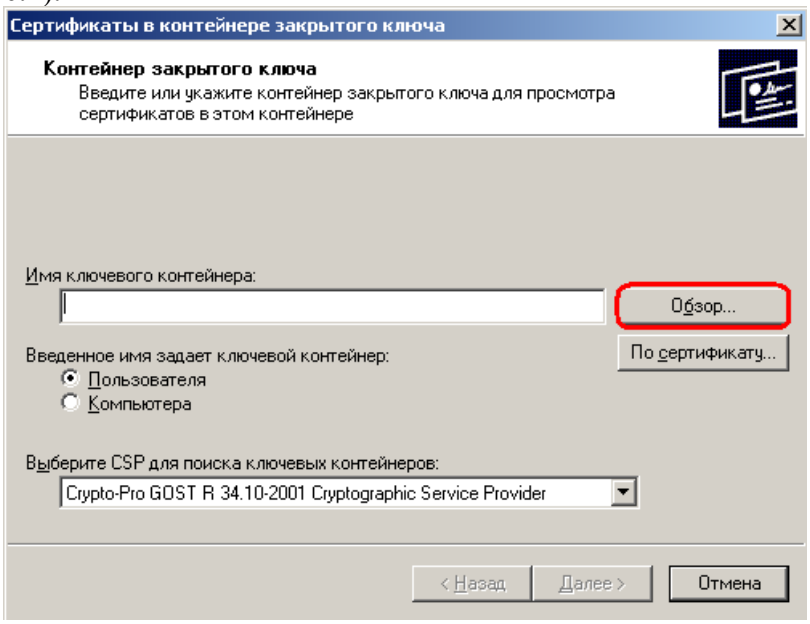

Рис.4

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

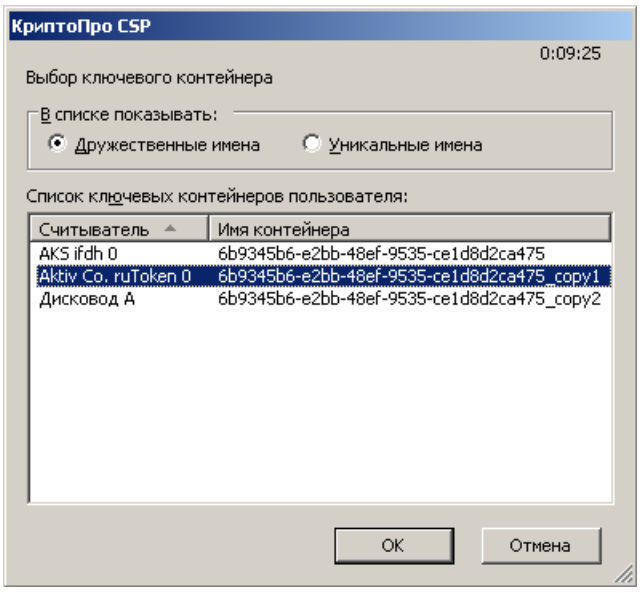

Рис.5

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».

---

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

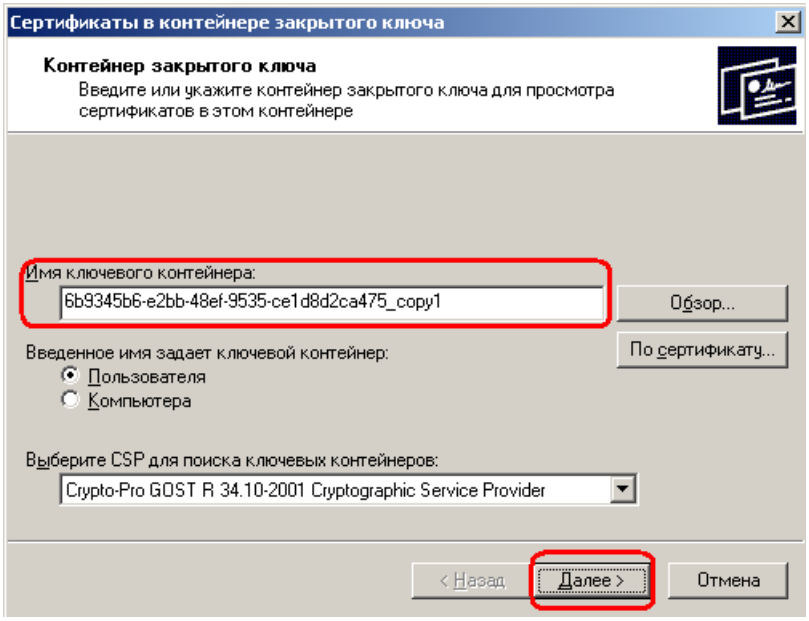

Рис.6

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» (рис.7).

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

Если уставлена версия КриптоПро CSP 3.6 R2 (версия продукта 3.6.6497) или выше, то в открывшемся окне можно нажать на кнопку «Установить», после чего утвердительно ответить на уведомление о замене сертификата (если оно появится). В противном случае в окне «Сертификат для просмотра» необходимо нажать кнопку «Свойства».

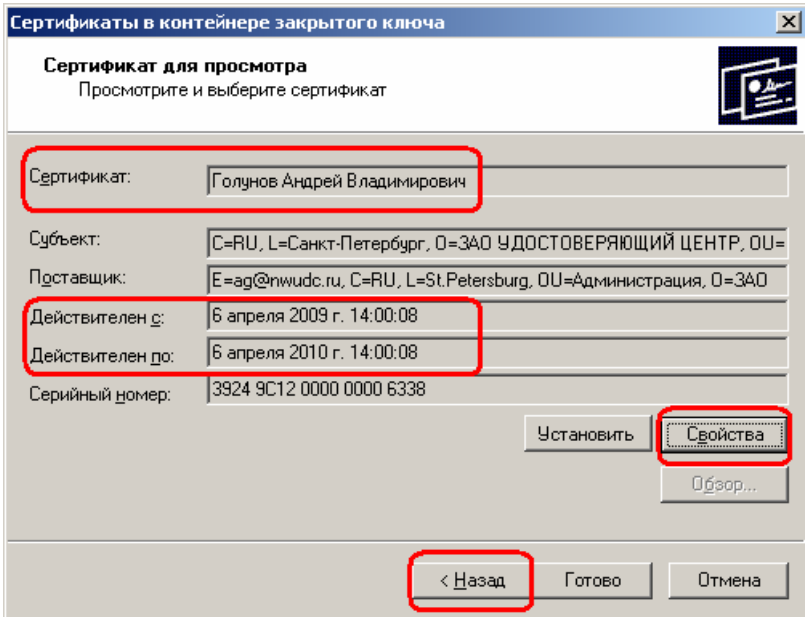

Рис.7

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).

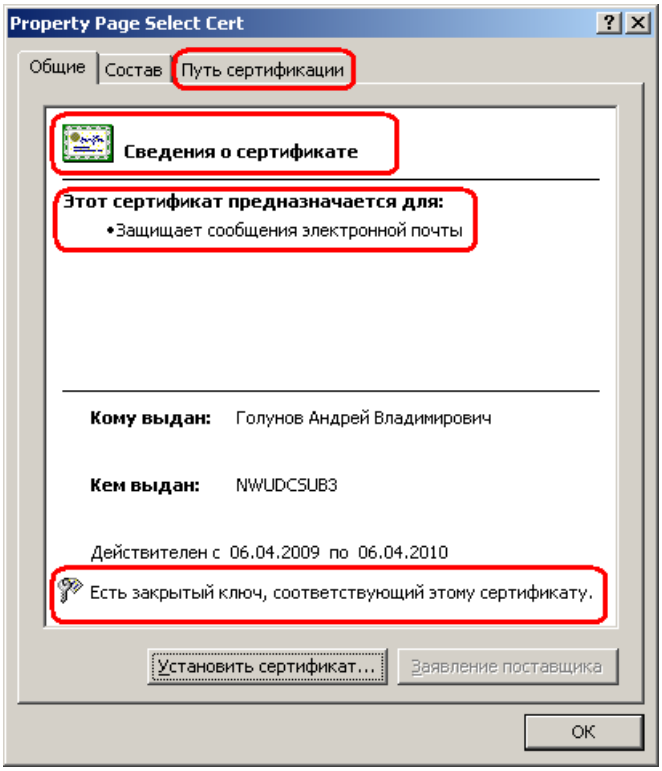

Рис.8

8. На вкладке «Путь сертификации» проверьте:

А. что цепочка сертификатов выстраивается верно (должно быть несколько сертификатов, как правило - 3, но не менее 2-х);

Б. что статус сертификата принимает значение «Этот сертификат действителен».

ВНИМАНИЕ!

А. Если цепочка сертификатов не выстраивается (в цепочке присутствует только один Ваш сертификат с желтым треугольником и восклицательным знаком внутри), возможно у Вас не установлены корневые сертификаты нашего удостоверяющего центра (см. инструкцию по установке сертификатов корневых центров сертификации).

Б. Если какие-либо сертификаты недействительны или повреждены (на значке сертификата присутствует красный круг с белым крестиком внутри) следует переустановить корневые сертификаты. Также настоятельно рекомендуется проверить компьютер на наличие вирусов.

---

9. Затем перейдите обратно на вкладку «Общие» и нажмите кнопку «Установить сертификат…» (рис.9).

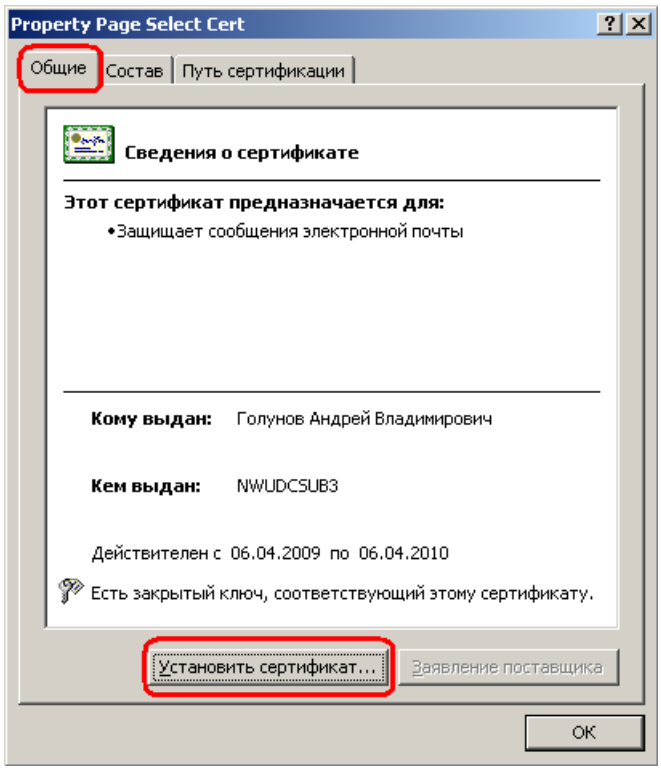

Рис.9

10. В окне Мастера импорта сертификатов нажмите кнопку «Далее» (рис.10).

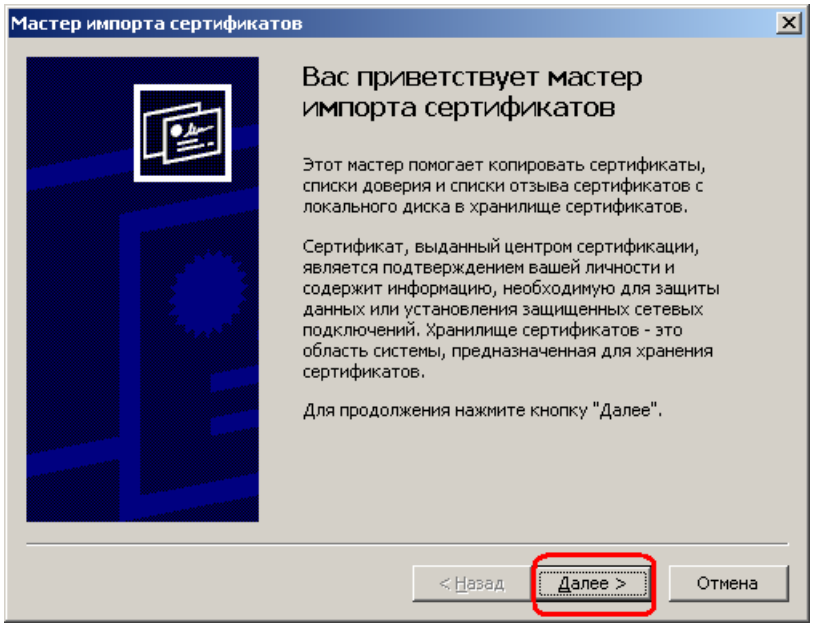

Рис.10

11. В следующем окне выберите пункт «Поместить все сертификаты в следующее хранилище» и нажмите кнопку «Обзор» (рис.11).

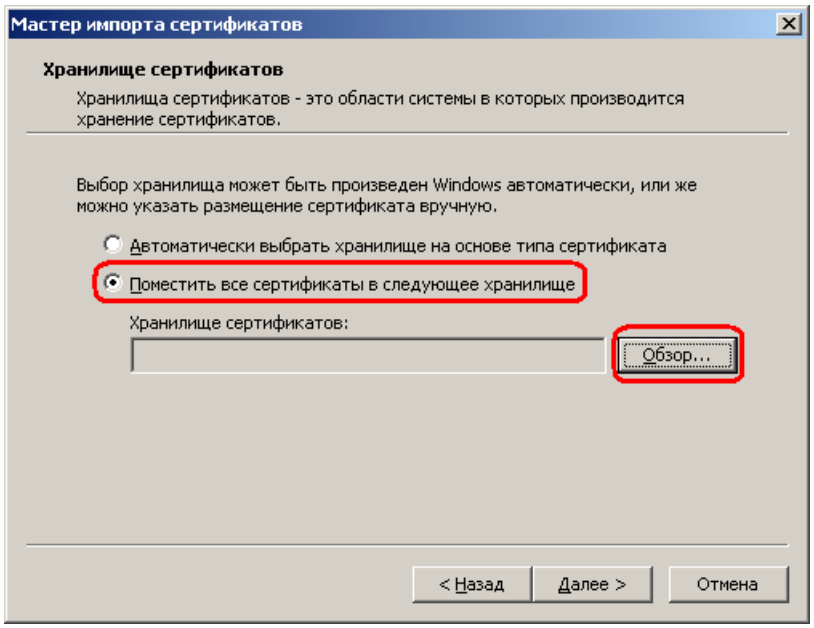

Рис.11

12. Выберите хранилище «Личные» и нажмите кнопку «ОК» (рис.12).

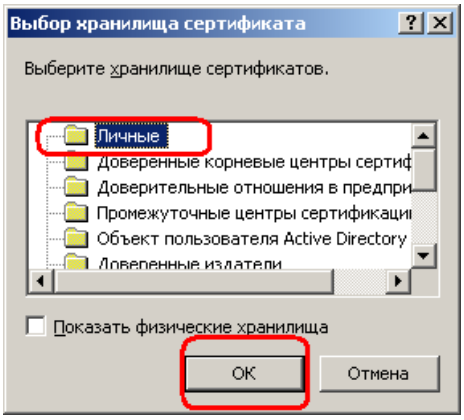

Рис.12

13. После этого Вы будете автоматически перемещены в предыдущее окно, только в поле «Хранилище сертификатов» будет указано «Личные» (рис.13). Нажмите кнопку «Далее».

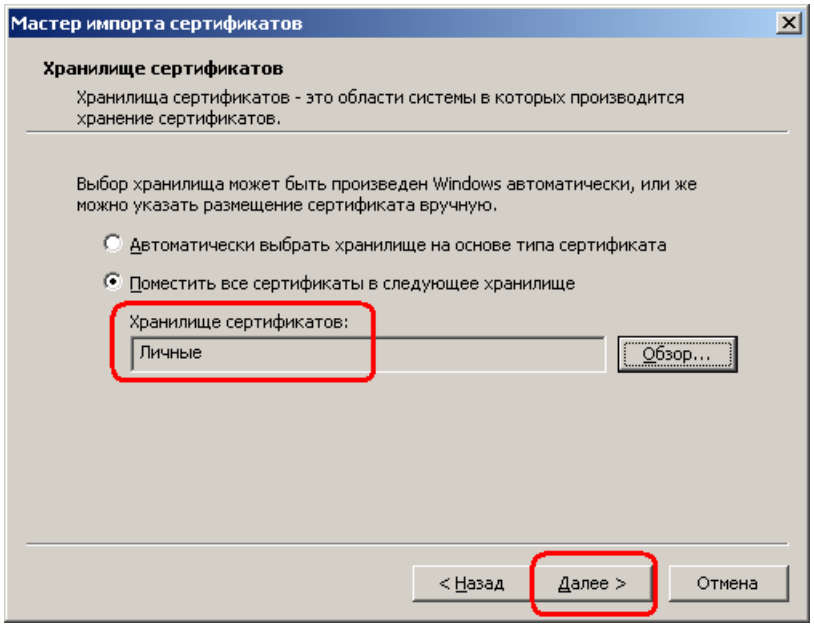

Рис.13

14. В окне «Завершение работы мастера импорта сертификатов» нажмите кнопку «Готово» (рис.14).

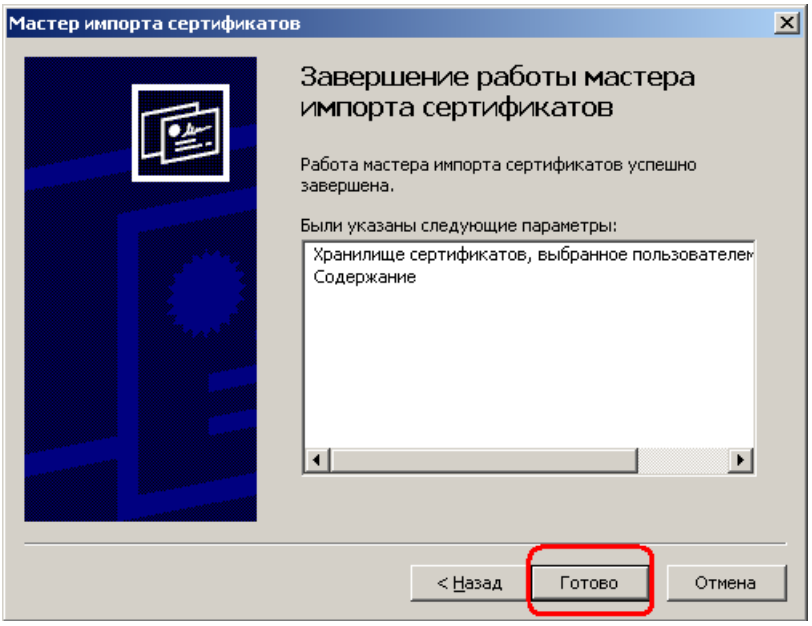

Рис.14

15. Начнется процесс установки сертификата. При необходимости введите PIN-код.

16. При успешной установке сертификата появится сообщение «Импорт успешно выполнен» (рис.15). Нажмите кнопку «ОК».

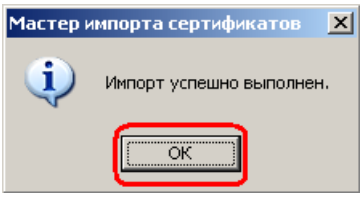

Рис.15

17. На этом установка личного сертификата завершена.

После успешного прописывания сертификата в хранилище ***иногда*** возникает сообщение с просьбой записать сертификат на носитель. Данное сообщение принадлежит eToken PKI Client (драйверу для eToken), а не КриптоПРО. При появлении данного сообщения необходимо отказаться от записи сертификата на eToken:

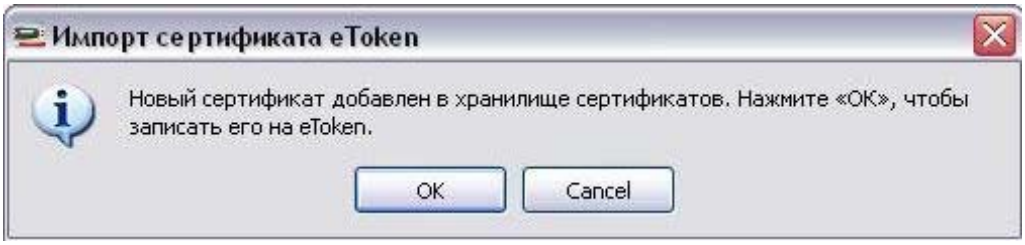

Рис.16

Для отключения в будущем данного сообщения необходимо выполнить следующее:
Войти в меню "Пуск" => "Выполнить" => msconfig => "ОК" => закладка "Автозагрузка" => отключить (снять галку) у PKIMonitor => "ОК" => перезагрузить ПК.
После перезагрузки появится окно с предупреждением о внесенных изменениях, в котором нужно поставить галку «Не выводить данное сообщение» и нажать "ОК".
В дальнейшем при установке сертификата это сообщение выдаваться уже не будет.