

30	
4.	ПРИ ВХОДЕ В ЛИЧНЫЙ КАБИНЕТ СООБЩЕНИЕ «НЕВАЛИДНЫЙ СЕРТИФИКАТ»
30	
5.	ПРИ ПРОВЕРКЕ ПОДПИСИ – «КРАСНАЯ ОШИБКА»
31	
6.	ПРИ УСТАНОВКЕ АКТИВЕХ-КОМПОНЕНТА ПОДПИСИ ВОЗНИКАЕТ ОШИБКА «НЕ УДАЛОСЬ ЗАРЕГИСТРИРОВАТЬ МОДУЛЬ...»
31	
7	ПРИЛОЖЕНИЯ
32	
1.	КАК ОПРЕДЕЛИТЬ ВЕРСИЮ WINDOWS
32	
2.	КАК ОПРЕДЕЛИТЬ ВЕРСИЮ БРАУЗЕРА
36	
3.	КАК СДЕЛАТЬ СКРИНШОТ
37	

1 Общие сведения

В Едином федеральном реестре сведений о фактах деятельности юридических лиц (далее - ЕФРСФДЮЛ)¹ вход в личный кабинет юридического лица (далее - ЮЛ) осуществляется с использованием сертификата ключа проверки электронной подписи.

Размещаемые в ЕФРСФДЮЛ сообщения, созданные в личном кабинете ЮЛ, должны быть подписаны электронной подписью (далее – ЭП).

Включая Единый федеральный реестр сведений о банкротстве, являющийся его неотъемлемой частью.

Таким образом обеспечивается неотрекаемость опубликованных сведений и их целостность (если данные были изменены после подписи, ЭП позволит доказать факт искажения информации).

2 Что нужно установить для подписи сведений, вносимых в ЕФРСФДЮЛ, электронной подписью

На персональном компьютере пользователя должно быть установлено и настроено:

1.

Специальное программное обеспечение - средство электронной подписи - шифровальные (криптографические) средства, используемые для авторизации в Системе и создания ЭП сообщений.

Пользователь также должен иметь актуальный сертификат ключа проверки электронной подписи в виде электронного документа, выданный авторизованным удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи уполномоченному для работы в Системе.

Инструкции по установке сертификата предоставляются удостоверяющим центром.

2.

Криптопровайдер – программное обеспечение, которое осуществляет вычисление ЭП (КриптоПро, VipNet CSP, Signal-COM CSP).

Инструкции по установке криптопровайдера предоставляются удостоверяющим центром.

3.

ActiveX-компонент для подписи сообщений и карточек ЭП. Он необходим, чтобы из браузера Internet Explorer или Mozilla Firefox можно было обратиться к криптопровайдеру. Инсталлятор ActiveX-компонента можно скачать здесь - http://www.fedresurs.ru/Helps/cspcomsetup_v2.msi.

3 Порядок установки ПО, необходимого для создания ЭП

Важно! Для установки программного обеспечения, пользователь должен обладать правами локального администратора на компьютере.

1. Установка криптопровайдера и сертификата ключа подписи

Возможные варианты действий:

1. Криптопровайдер был ранее установлен на компьютер пользователя, сертификат ключа проверки ЭП также был ранее получен и установлен, срок его действия не истек. В этом случае, необходимо выяснить, есть ли выдавший сертификат удостоверяющий центр в перечне УЦ, размещенном на сайте ЕФРСФДЮЛ (<http://www.fedresurs.ru/Help>). Если УЦ там есть, то необходимо уточнить непосредственно в службе поддержки УЦ, допустимо ли использование данного сертификата в ЕФРСФДЮЛ. В случае положительного ответа на этот вопрос, можно переходить к разделу 2 данной инструкции.

2. Один из криптопровайдеров КриптоПро, VipNet CSP, Signal-COM CSP был ранее установлен, но впоследствии удален или срок действия сертификата ключа проверки ЭП пользователя истек.
 - a. Рекомендуется обратиться в удостоверяющий центр, в котором ранее были получены криптопровайдер и сертификат, для получения нового сертификата ключа проверки электронной подписи и необходимого для вычисления ЭП криптопровайдера.
 - b. Установить и настроить криптопровайдер согласно инструкциям, полученным в удостоверяющем центре.
3. На компьютере не был установлен криптопровайдер.
 - a. Необходимо получить криптопровайдер и сертификат ключа проверки ЭП в одном из УЦ, указанных в списке на <http://fedresurs.ru/Help>.
 - b. При установке и настройке криптопровайдера необходимо следовать инструкциям, предоставленным УЦ.

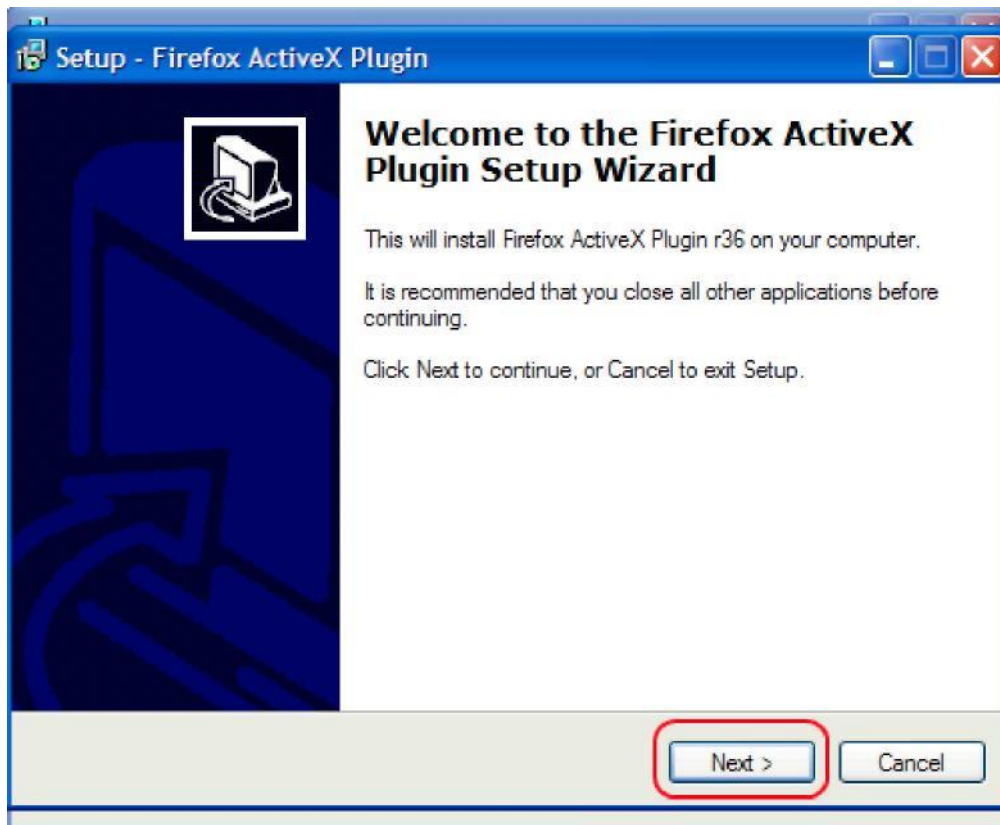
2. Установка ActiveX-компонента подписи

ActiveX-компонент подписи необходим для вызова криптопровайдера из браузера. Компонент подписи может работать в браузере Internet Explorer (поддерживаются только 32х разрядные версии браузеров), а также в браузере Mozilla FireFox.

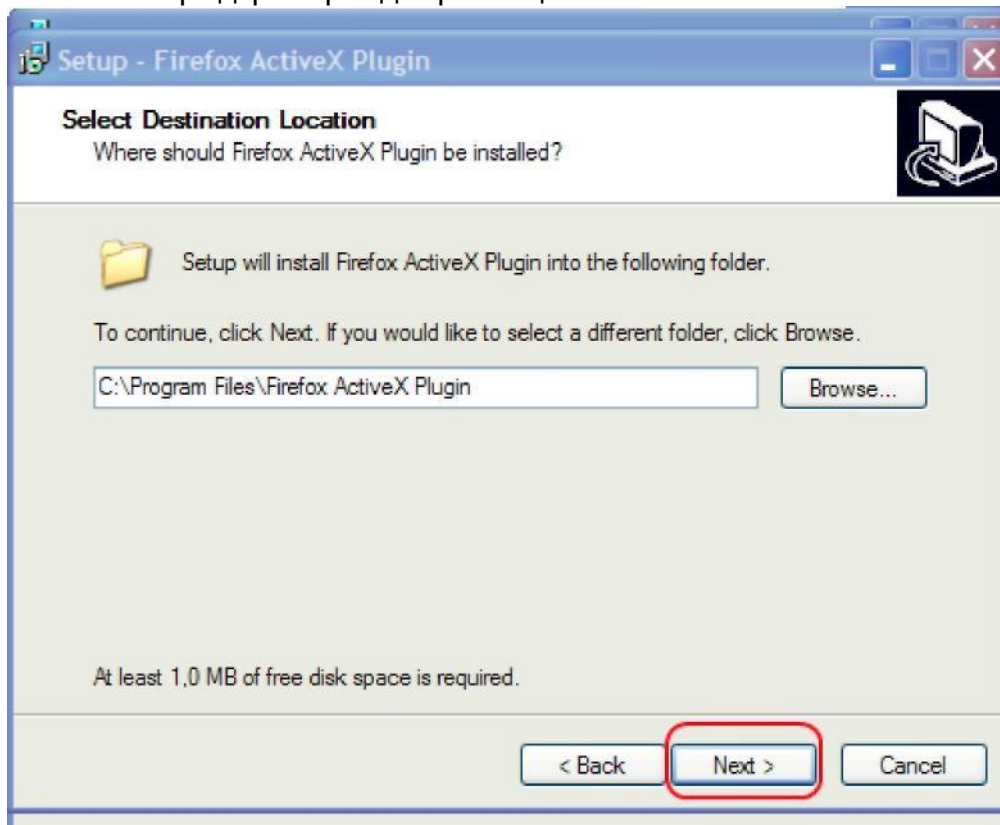
В ЕФРСФДЮЛ рекомендуется использовать браузеры Internet Explorer версии 8 и выше (поддерживаются только 32х разрядные версии браузеров) и Mozilla FireFox версии 8 и выше.

Порядок установки:

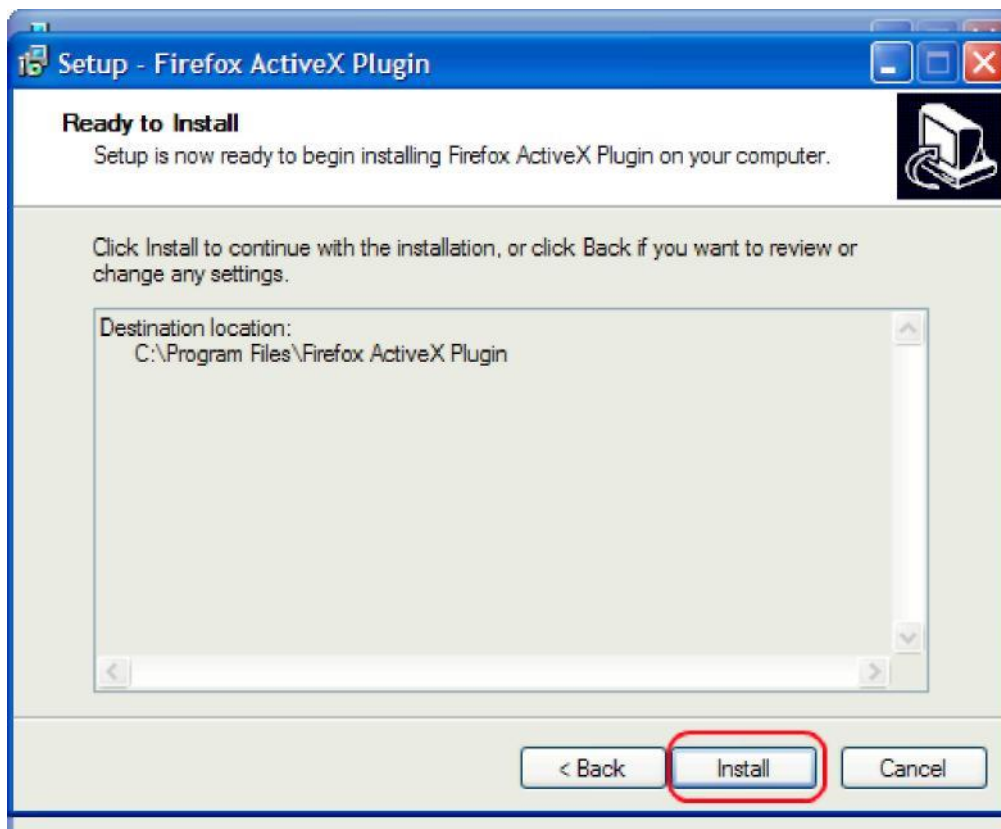
1. Скачать со страницы «Помощь» сайта ЕФРСФДЮЛ (<http://www.fedresurs.ru/help>) инсталлятор ActiveX-компонента подписи (http://www.fedresurs.ru/helps/cspcomsetup_v2.msi).
2. Запустить инсталлятор cspcomsetup.msi.
3. Сразу же после начала инсталляции откроется дополнительное окно инсталлятора плагина для FireFox, позволяющего запускать ActiveX-компонент в этом браузере. В открывшемся окне необходимо нажать на кнопку «Next»:



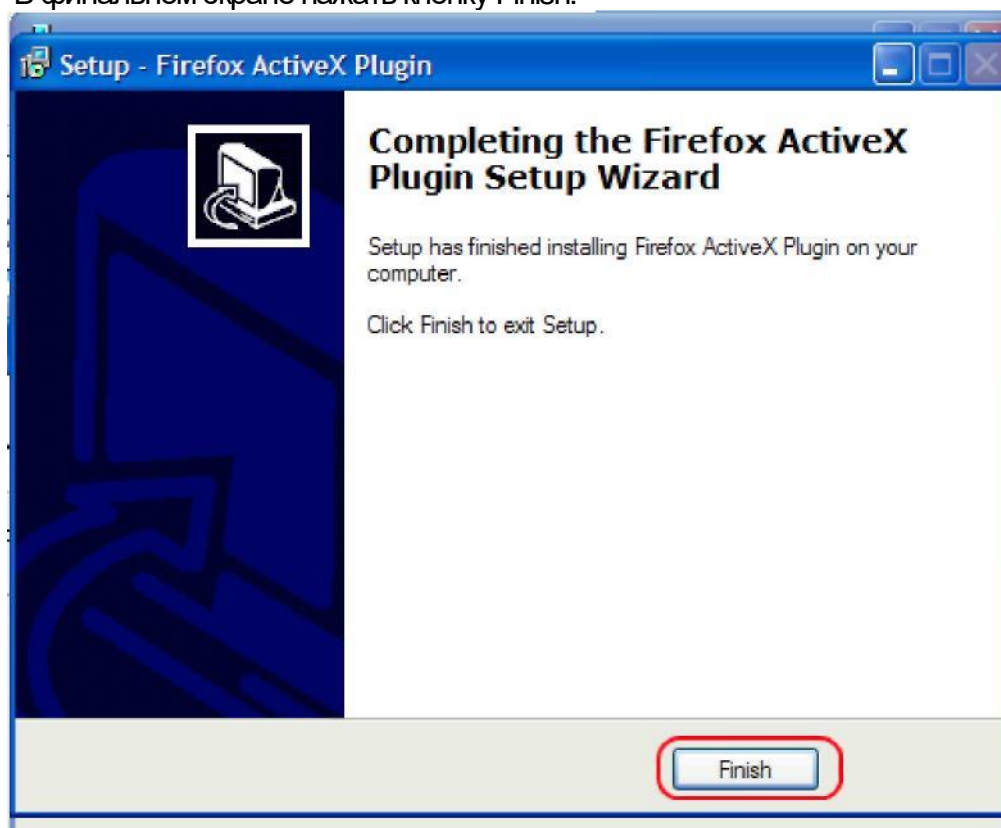
4. В окне выбора директории для размещения плагина – тоже:



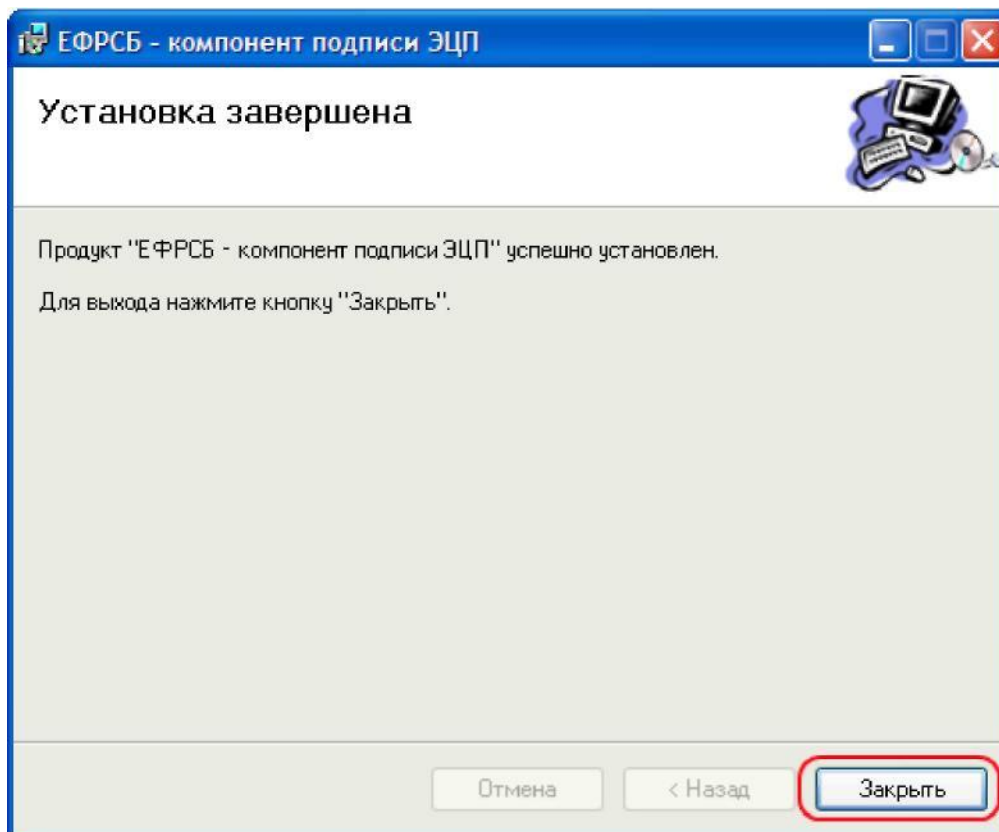
5. В окне подтверждения инсталляции нажать «Install»:



6. В финальном экране нажать кнопку Finish:



7. В последнем экране инсталляции компонента подписи необходимо нажать «Закреть»:



4 Настройка ПО для возможности подписи

1. *Добавление сертификата в локальное хранилище Windows*

Чтобы ActiveX-компонент подписи мог обращаться к криптопровайдеру, **сертификат ключа подписи и корневой сертификат удостоверяющего центра** должны быть добавлены в хранилище сертификатов Windows. В настоящем разделе будет показано, как это сделать для криптопровайдеров КриптоПро, VipNet, Signal-COM.

Примечание: предполагается, что криптопровайдер установлен. Если нет, необходимо его установить согласно инструкциям в разделе 31.

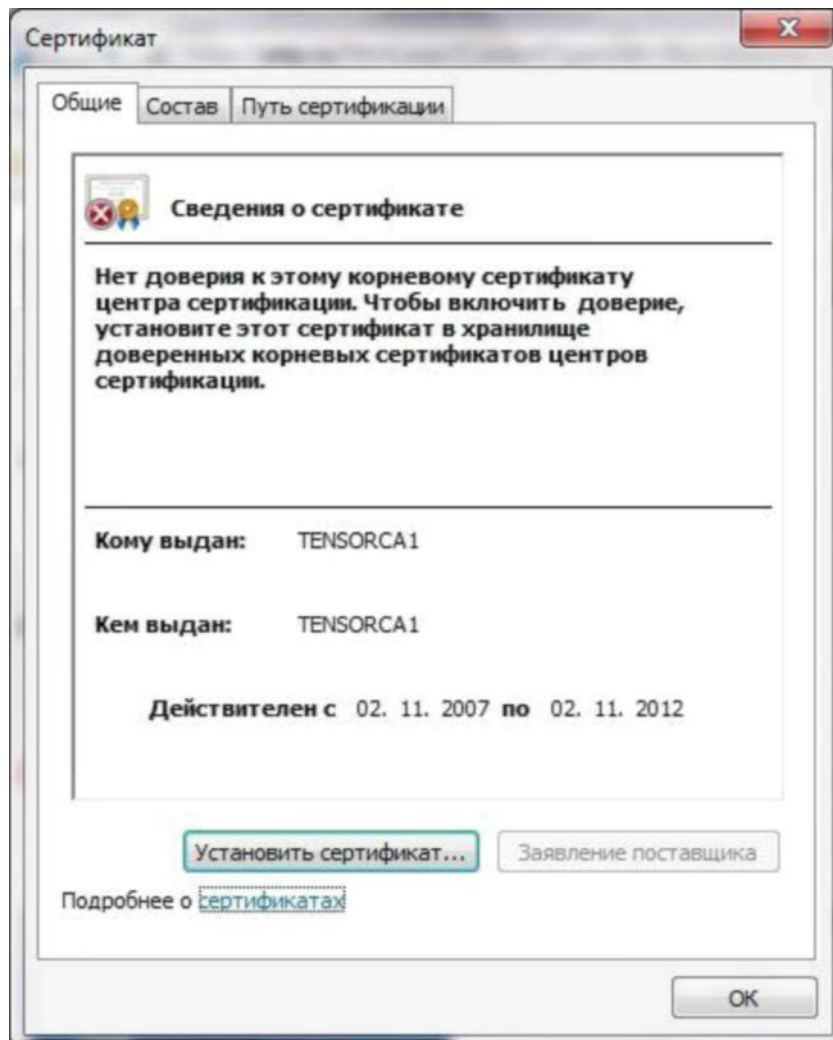
4.1.1 Установка корневого сертификата

Если Вы получали ЭП в одном из УЦ через Ассоциацию электронных торговых площадок, корневой сертификат можно скачать с сайта <http://aetp.ru/>, раздел «Электронная подпись» – «Удостоверяющие центры». Если Вы получали ЭП не через Ассоциацию, обратитесь за корневым сертификатом в Ваш удостоверяющий центр (УЦ).

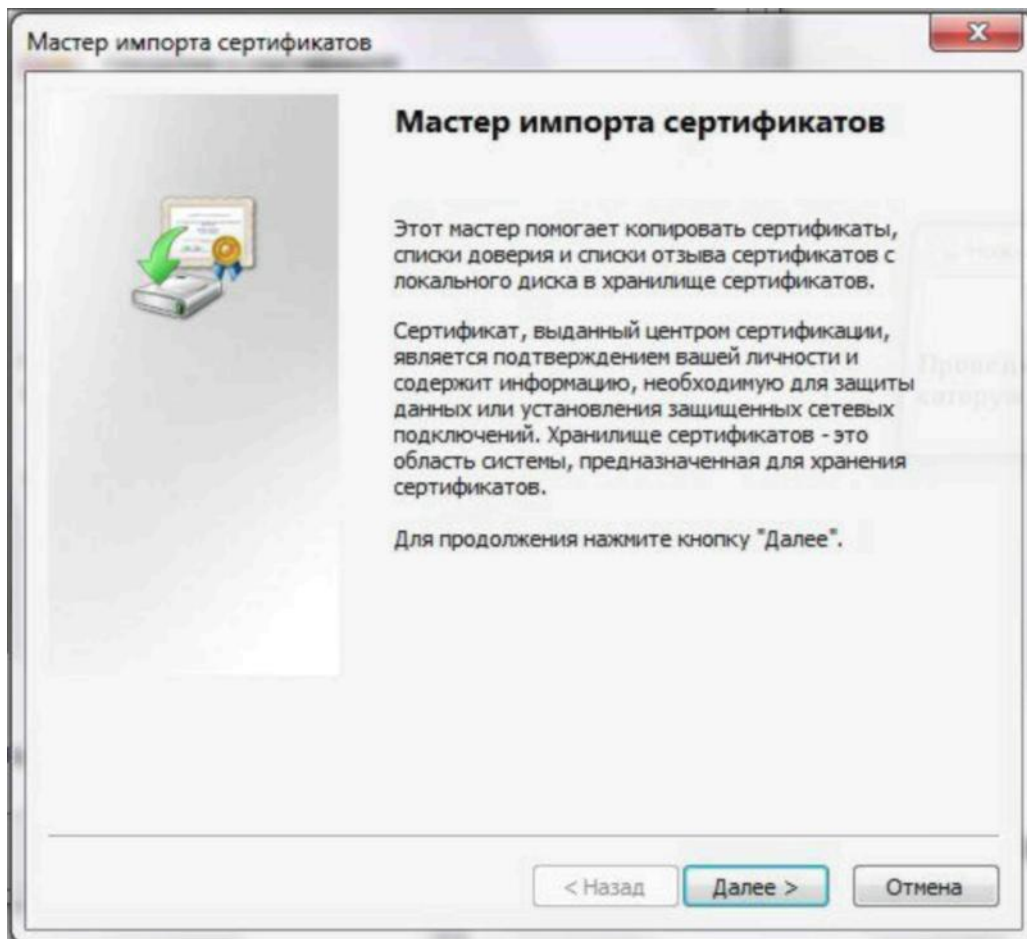
Если Вы получали ЭП в УЦ e-Notary, корневой сертификат можно скачать с сайта <http://www.e-notary.ru/>, раздел – «Корневые сертификаты аккредитованного УЦ e-Notary».

Откройте ссылку, сохраните файл сертификата на диске.

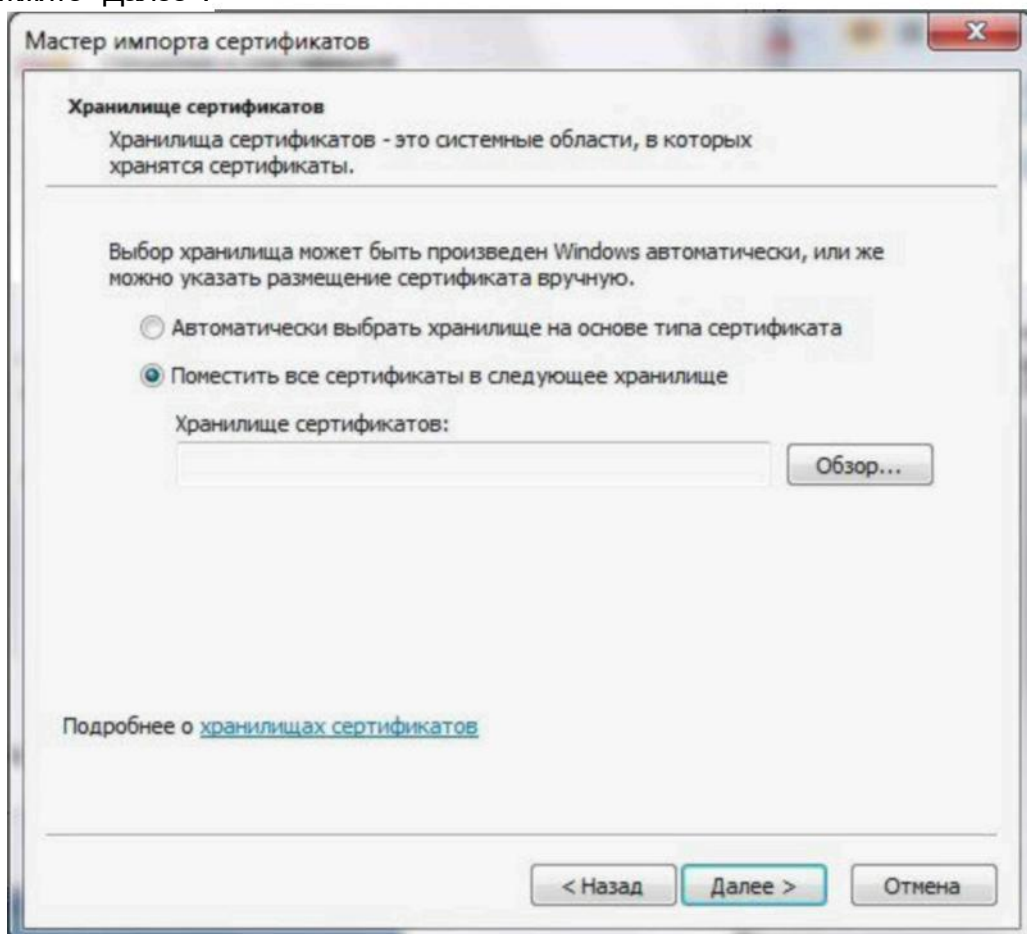
1. Откройте сертификат, нажмите «Установить»:



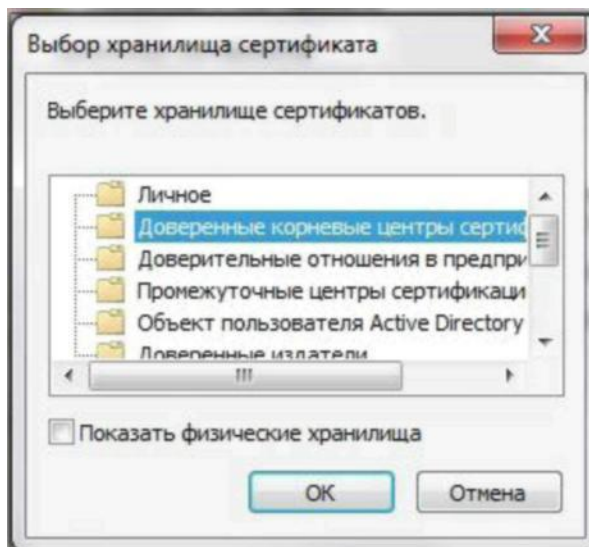
2. Откроется мастер импорта сертификатов:



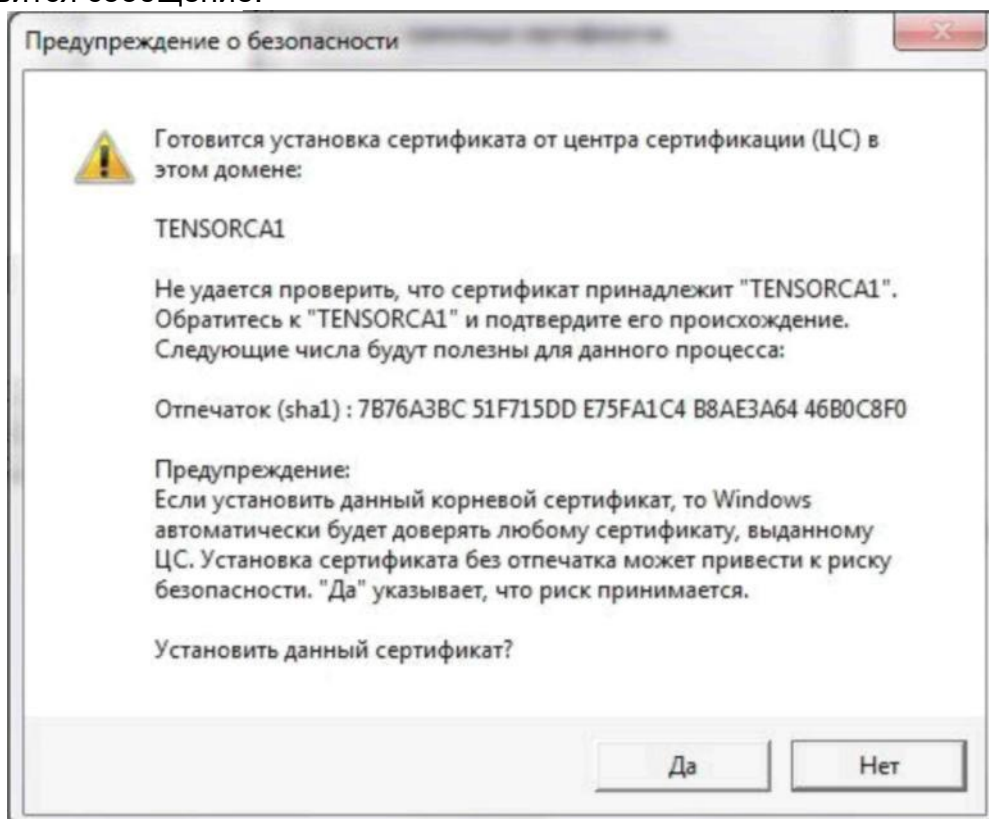
3. Нажмите «Далее»:



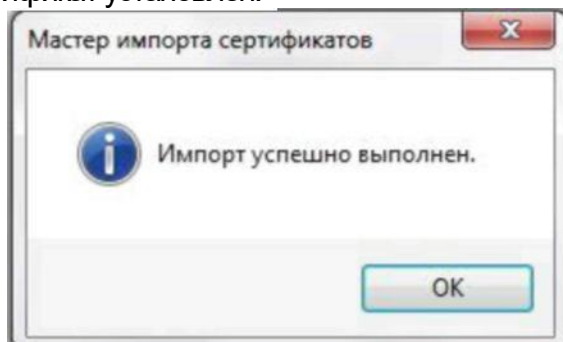
4. Выберите «Поместить сертификаты в следующее хранилище» и нажмите кнопку «Обзор»:



5. Выберите «Доверенные корневые центры сертификации», «OK», «Далее», «Готово». Появится сообщение:



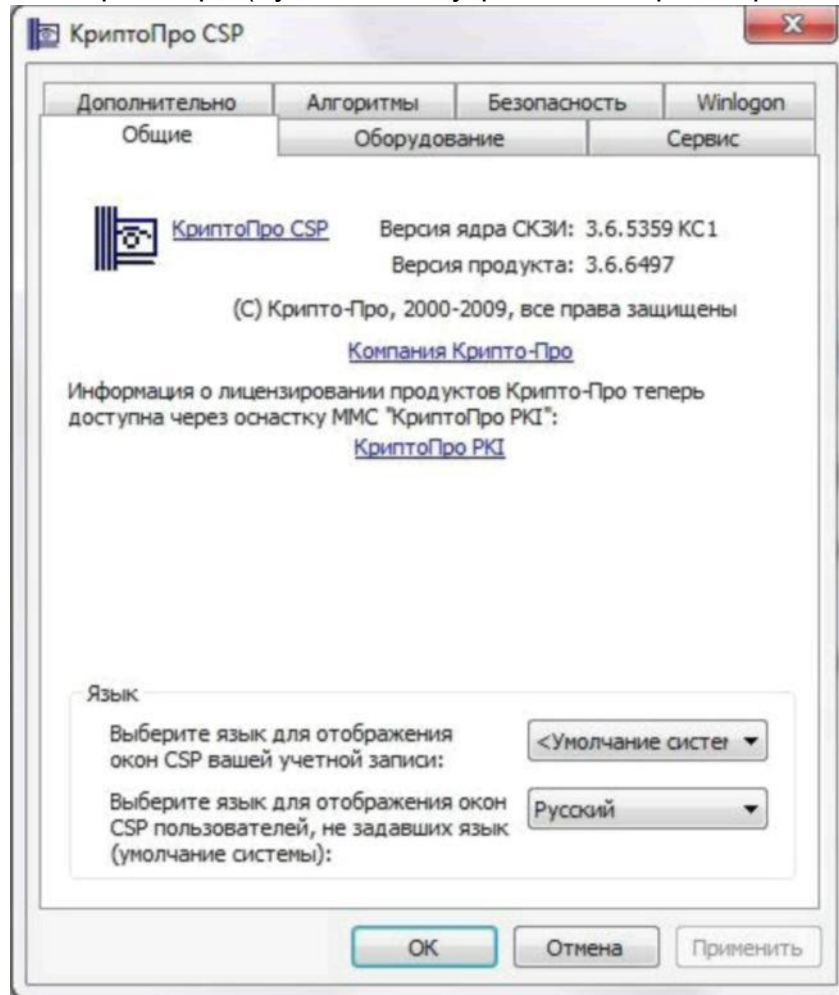
6. Нажмите «Да». Сертификат установлен:



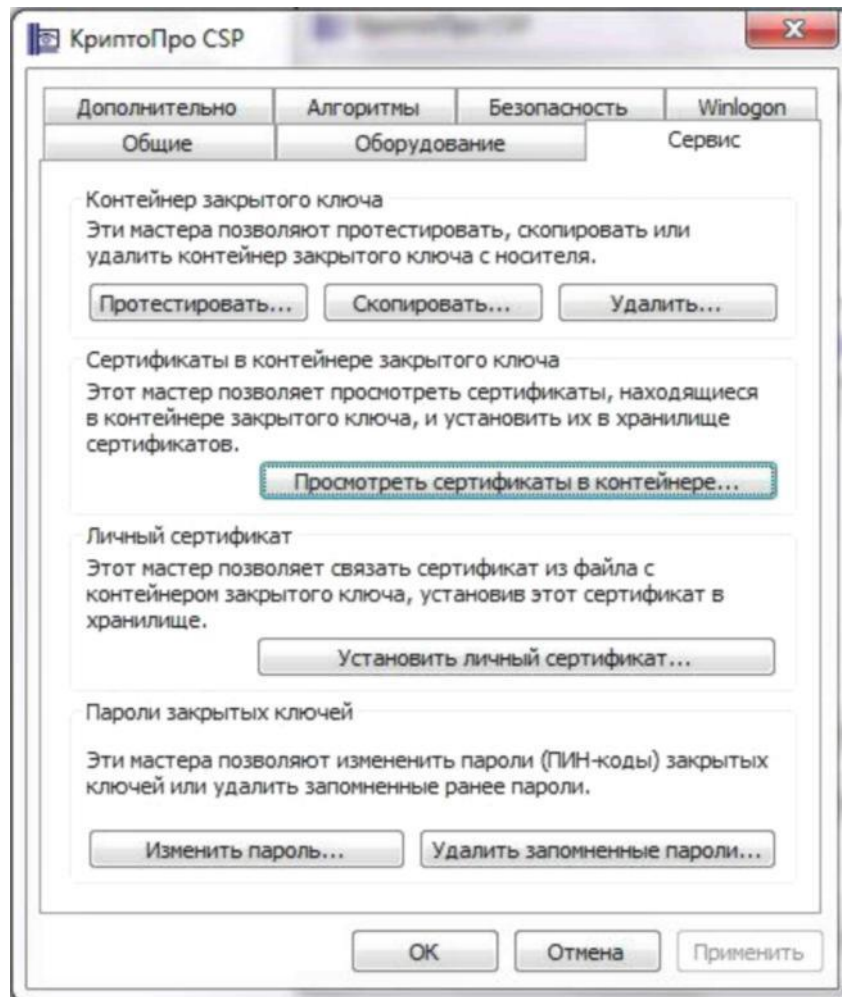
4.1.2 Установка личного сертификата при помощи КриптоПро

Если у Вас есть открытая часть сертификата (файл с расширением .cer), переходите сразу к пункту 11.

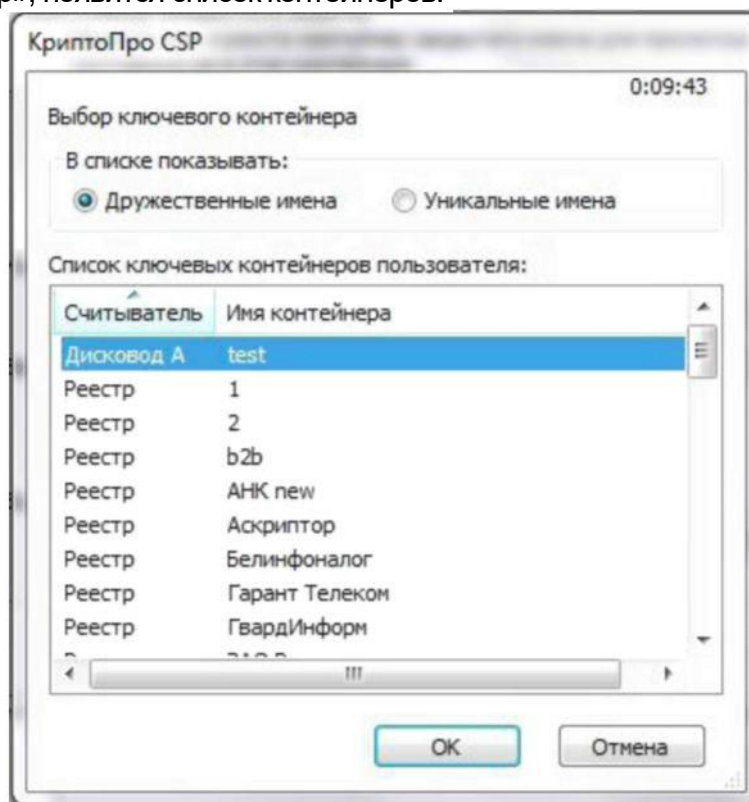
1. Откройте свойства КриптоПро. (Пуск – Панель управления – КриптоПро CSP).



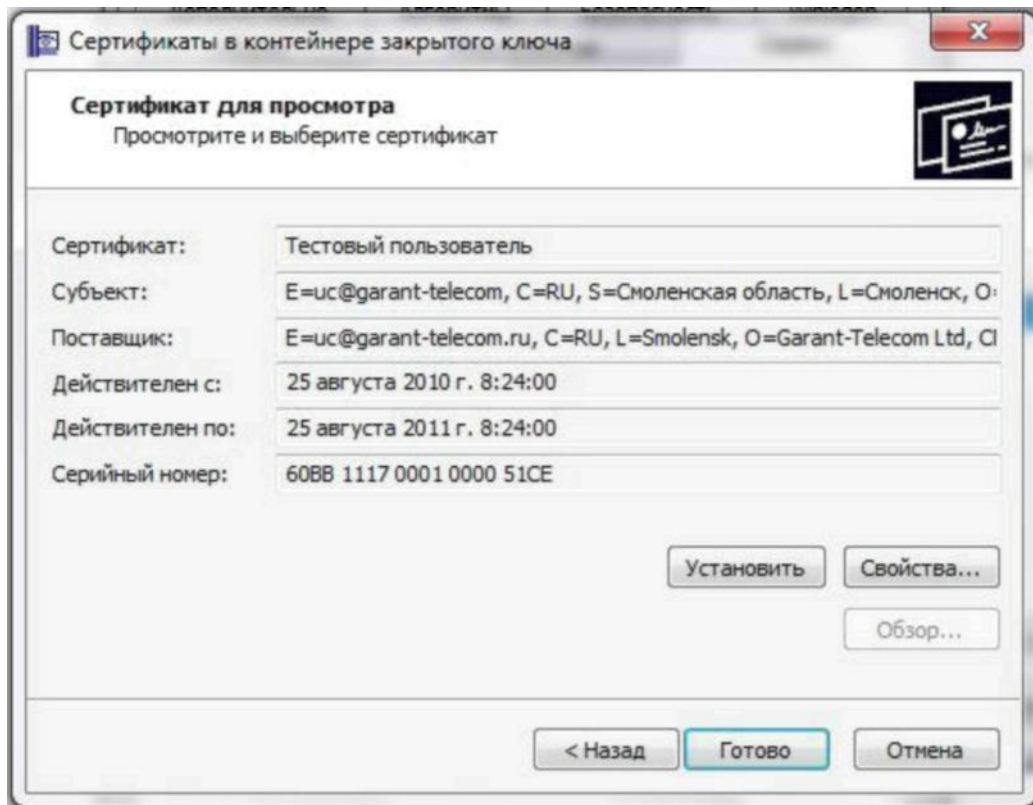
2. Зайдите на вкладку «Сервис», нажмите «Посмотреть сертификаты в контейнере»:



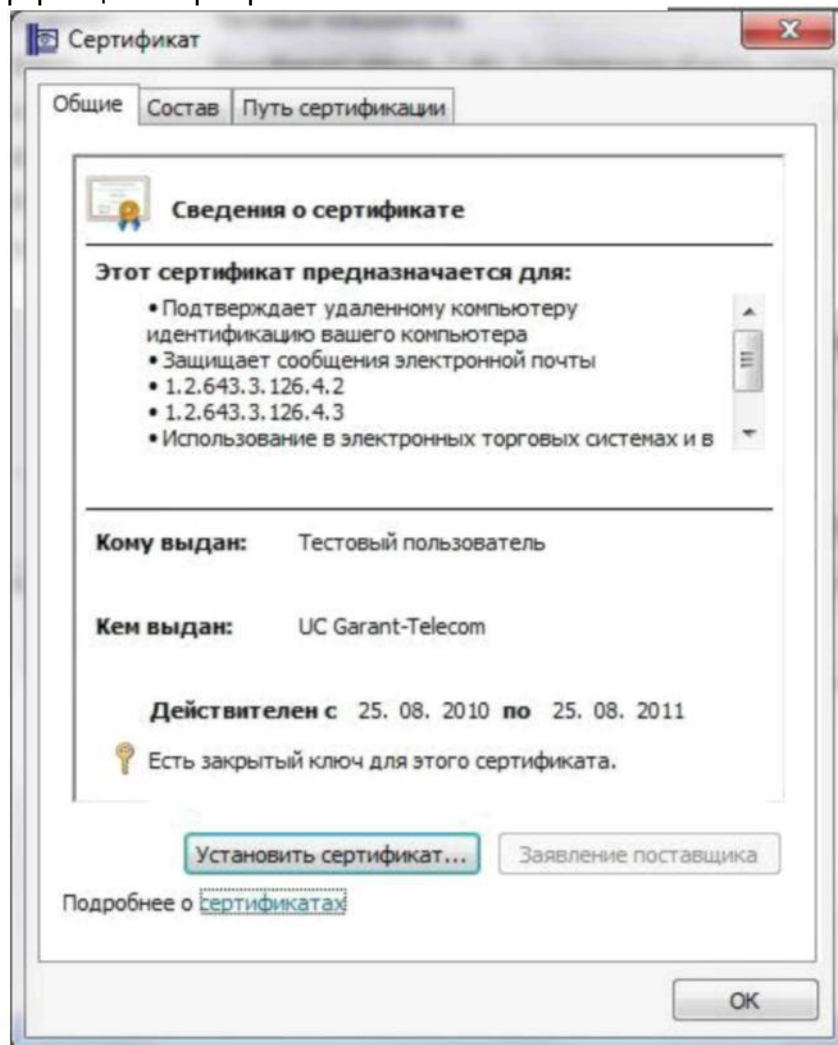
3. Нажмите «Обзор», появится список контейнеров:



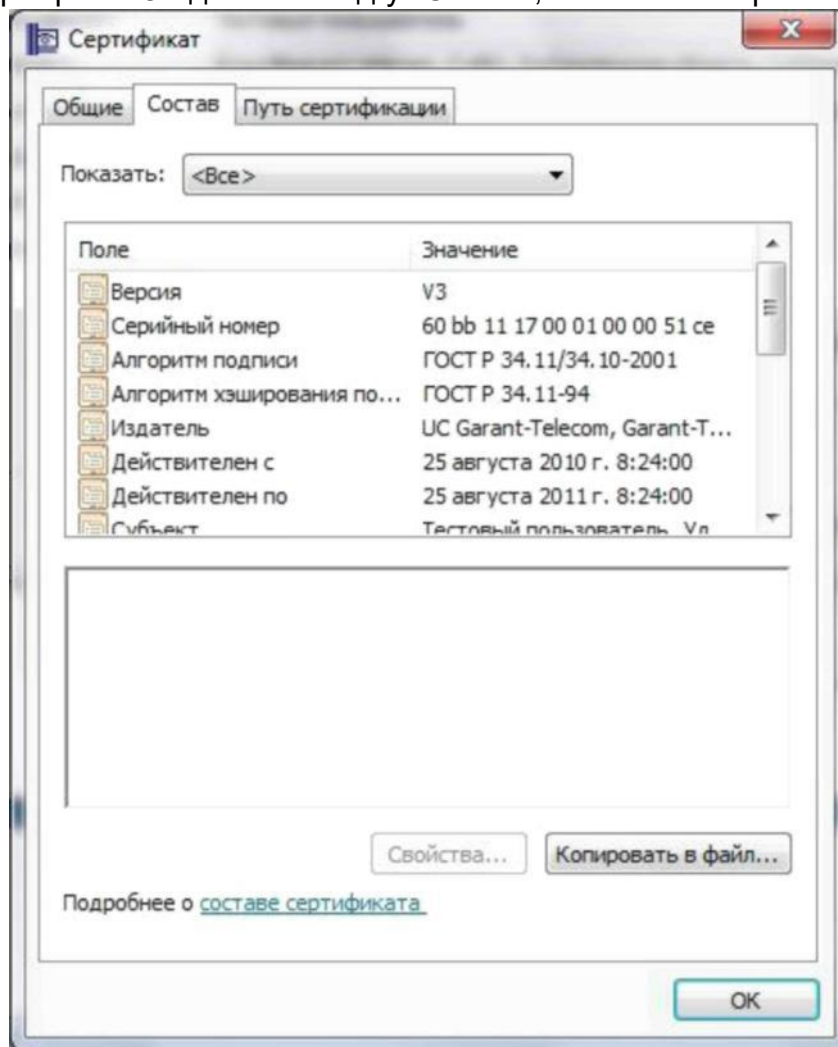
4. Выберите нужный контейнер, нажмите «ОК», «Далее»:



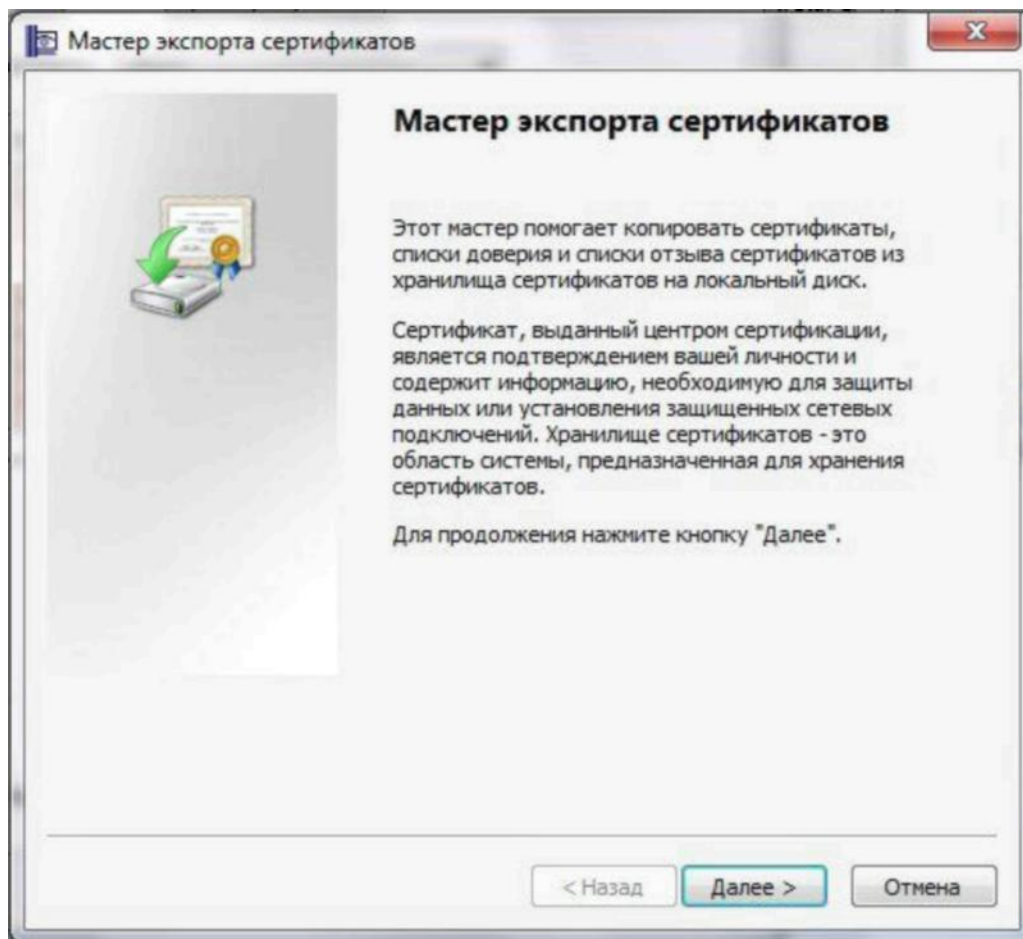
5. Откроется информация о сертификате. Нажмите «Свойства...»



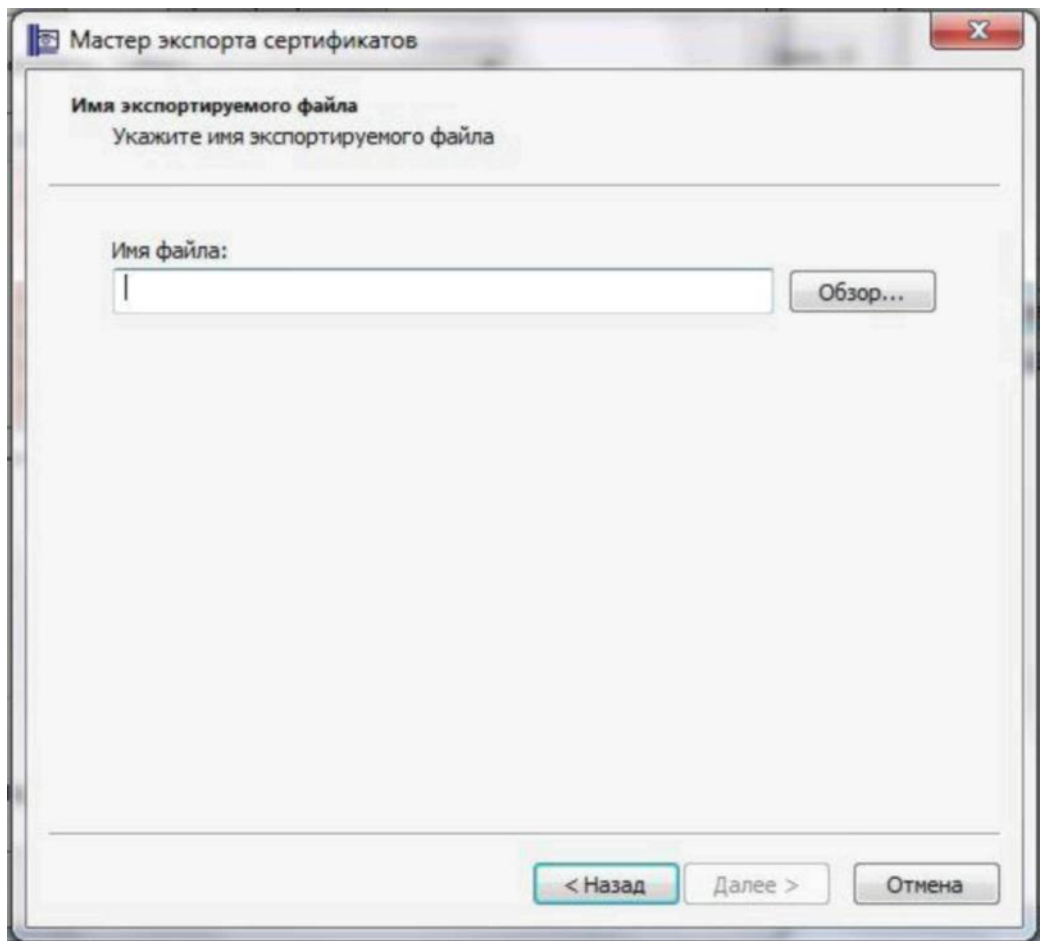
6. Откроется сертификат. Зайдите на вкладку «Состав», нажмите «Копировать в файл»:



7. Откроется мастер экспорта сертификатов:

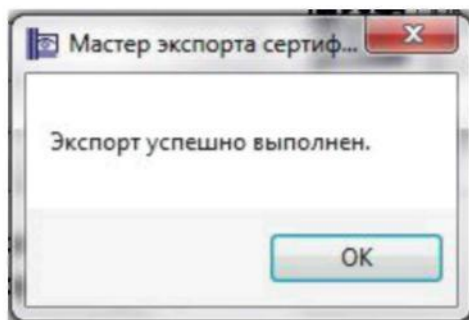


8. Нажимаете «Далее» 3 раза, ничего не меняя.
9. В окне имя файла нажмите «Обзор». Выберите, куда сохранить, сохраните:



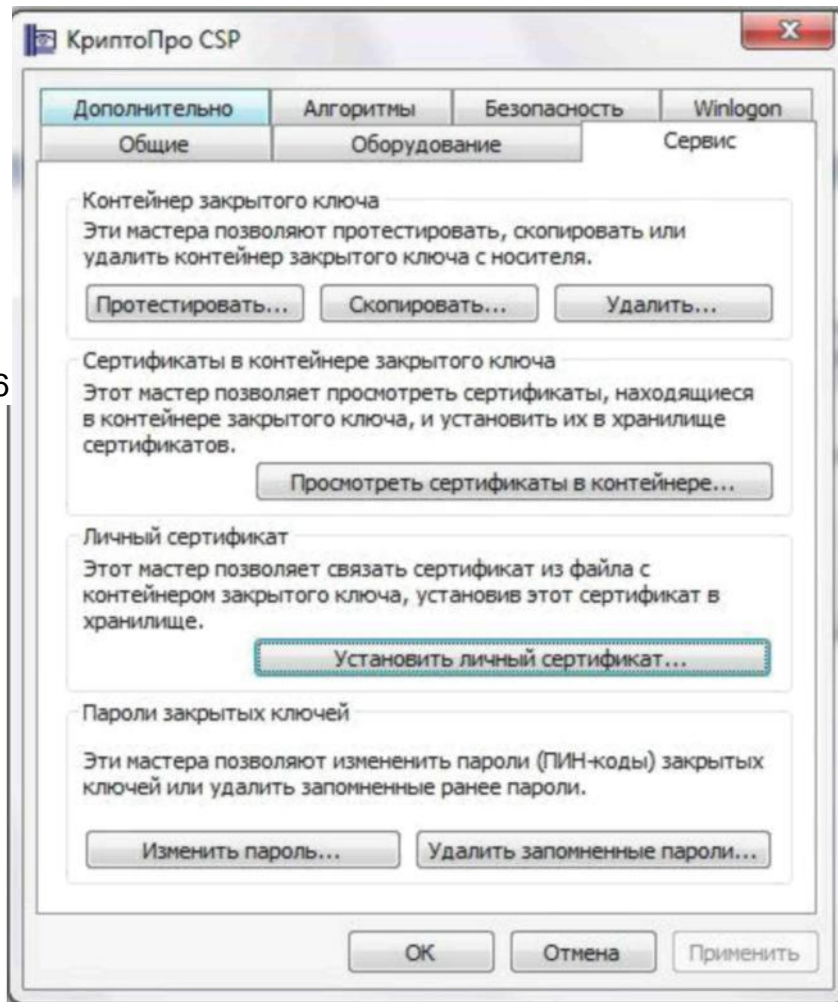
10. Экспорт завершен:

Нажмите «ОК»,
«Готово». 11.
Нажмите на вкладке
«Сервис» кнопку
«Установить личный
сертификат»:



13. Затем нажмите «Далее» 2 «Обзор», выберите нужный контейнер и нажмите «Далее»:

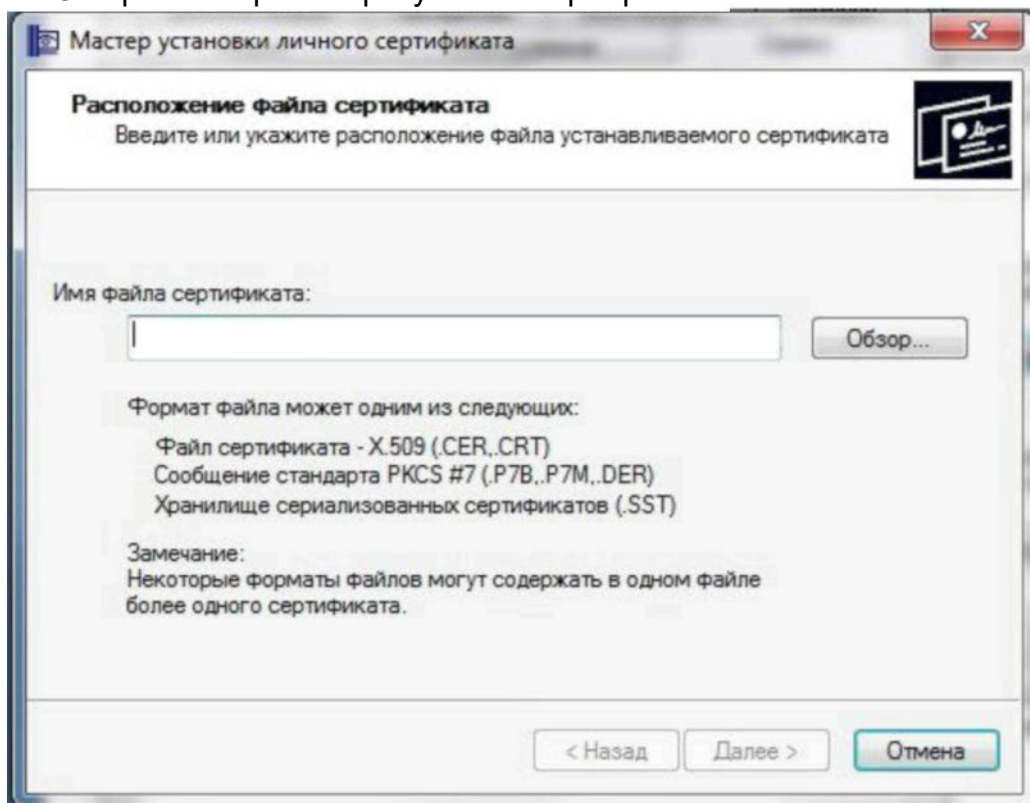
16

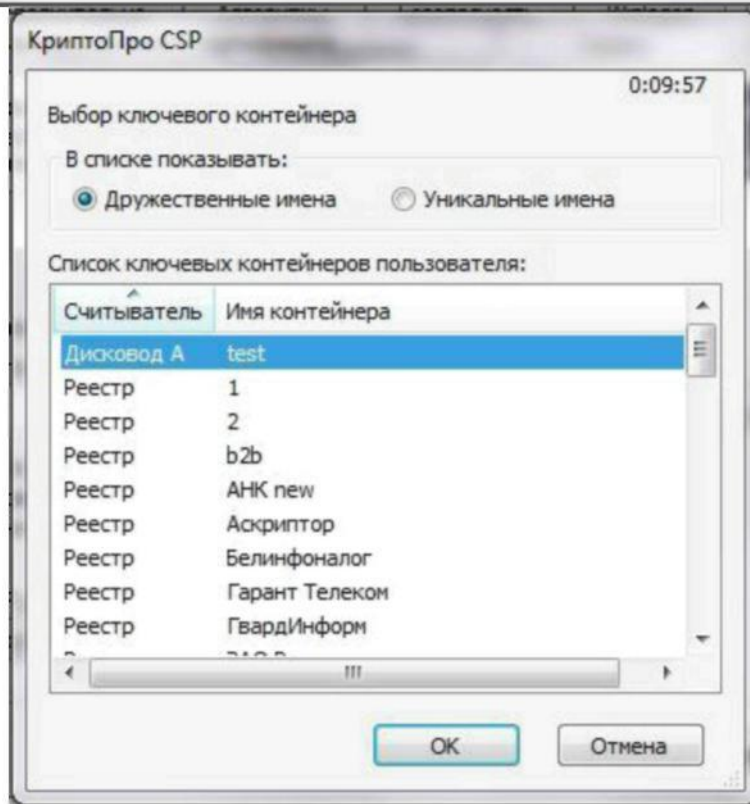
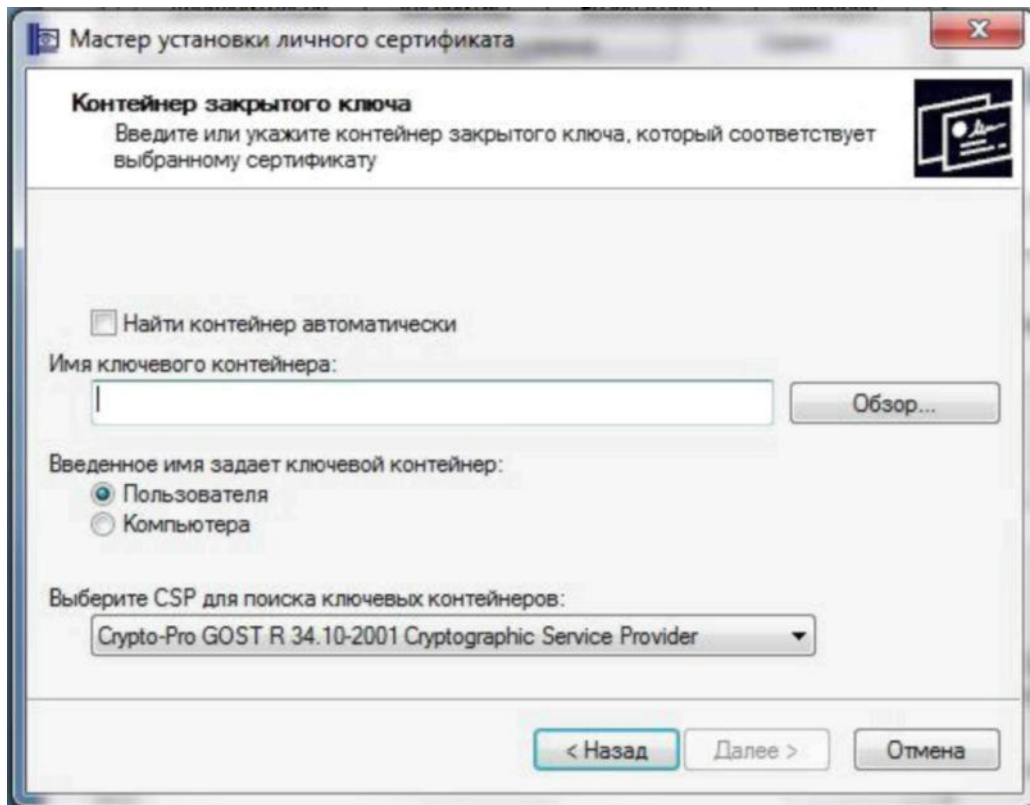


раза,

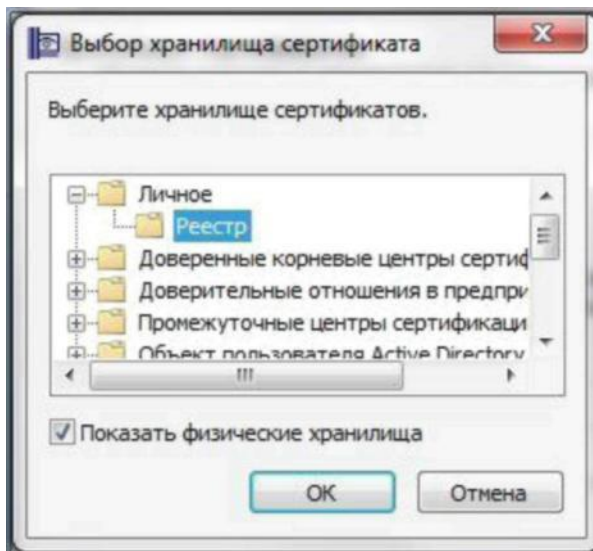
«ОК»,

12. Нажмите «Обзор» и выберите открытую часть сертификата:

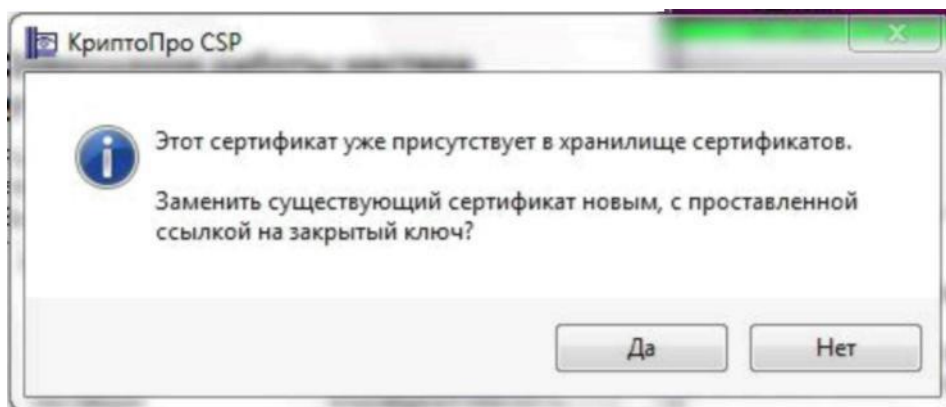




14. Имя хранилища сертификатов, нажмите «Обзор»:



Поставьте галочку «Показать физические хранилища» и выберите «Личное» – «Реестр». «ОК» – «Далее» – «Готово». 15. Если ранее была некорректная установка, появится окно:



Нажмите «Да». Установка личного сертификата завершена.

4.1.3 Установка личного сертификата при помощи VipNet CSP

Для установки корневого и личного сертификатов в хранилище Windows пользователям программы VipNet CSP необходимо:

1. Установка личного сертификата с ключевого носителя.

Ф Внимание! В зависимости от используемого Вами носителя ключевой информации используйте соответствующий пункт Инструкции.

Если ключи электронной подписи и сертификат хранятся на ключевом носителе eToken, воспользуйтесь пунктом 1а Инструкции.

Если ключи электронной подписи и сертификат хранятся на компакт-диске (CD), воспользуйтесь пунктом 1б Инструкции.

1а. Установка личного сертификата с ключевого носителя eToken.

а). Для корректной работы ключевого носителя eToken под управлением операционной системы Microsoft Windows необходимо установить программное обеспечение компании Аладдин РД **eToken PKI Client**.

- Для получения **eToken PKI Client** актуальной версии загрузите архив с дистрибутивом с web-ресурса http://iitrust.ru/downloads/PKIClient/PKIClient_x32.zip (для 32-х разрядной ОС Windows) или http://iitrust.ru/downloads/PKIClient/PKIClient_x64.zip (для 64-х разрядной ОС Windows) и сохраните загруженный архив с дистрибутивом на своем компьютере.

У Распакуйте архив, а затем запустите установку **eToken PKI Client** из файла **PKIClient x32 x.x SP1.msi** (для 32-х разрядной ОС Windows) или из файла **PKIClient x64 x.x SP1.msi** (для 64-х разрядной ОС Windows).

У Выполните установку **eToken PKI Client**, следуя инструкциям мастера установки.

У Установите содержащийся в том же архиве пакет обновлений **eToken PKI Client** из файла **PKIClient-x32-x-x-SP1.msp** (для 32-х разрядной ОС Windows) или **PKIClient-x64-x-x-SP1.msp** (для 64-х разрядной ОС Windows).

б). Установка личного сертификата с ключевого носителя eToken.

У Вставьте eToken в USB-порт компьютера.

У Запустите ViPNet CSP и убедитесь, что на закладке "Общие" включена опция "Включить поддержку работы ViPNet CSP через MS Crypto API" (Рис. 1).

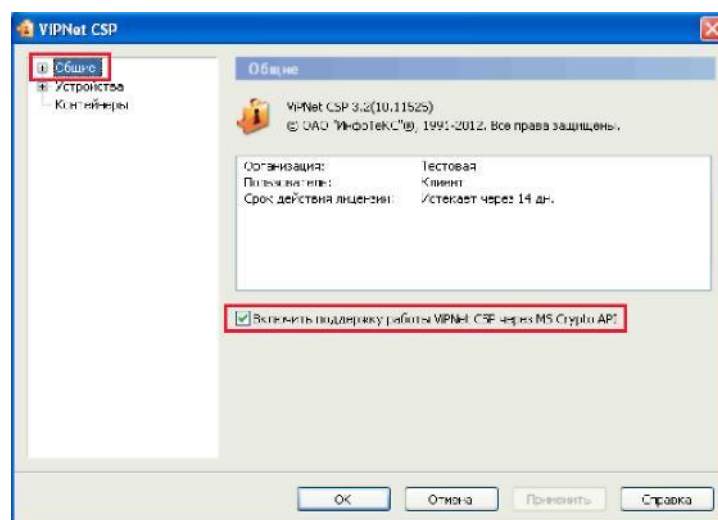


Рис. 1

У Перейдите на закладку "Устройства" (Рис. 2). В окне "Подключенные устройства" выберите "eToken Aladdin(хххххххх)", а в окне "Контейнеры ключей на устройстве" - контейнер ключей `sgn-xxxx-xxxx-xxxx-xxxx`. Затем нажмите клавишу "Просмотреть".

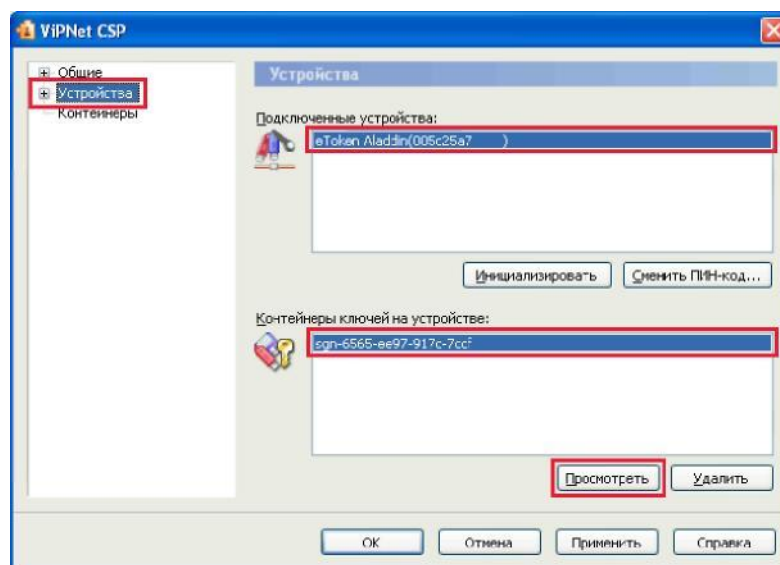


Рис. 2

У В окне свойств контейнера ключей (Рис. 3) в разделе "Закрытые ключи" выберите строку с реквизитами ключа и нажмите кнопку "Сертификат".

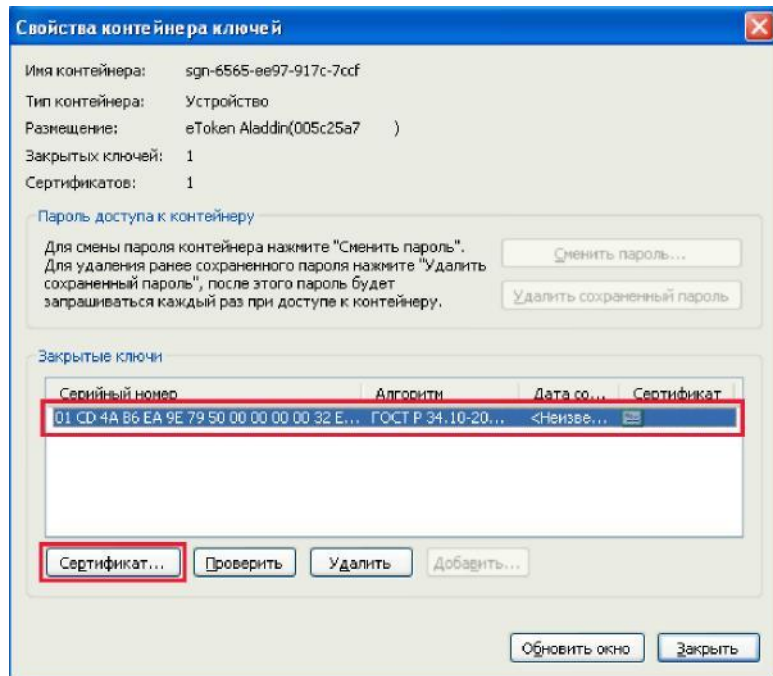


Рис. 3

Убедитесь, что выбран именно тот сертификат, который необходимо использовать, и нажмите клавишу "Установить сертификат" (Рис. 4).

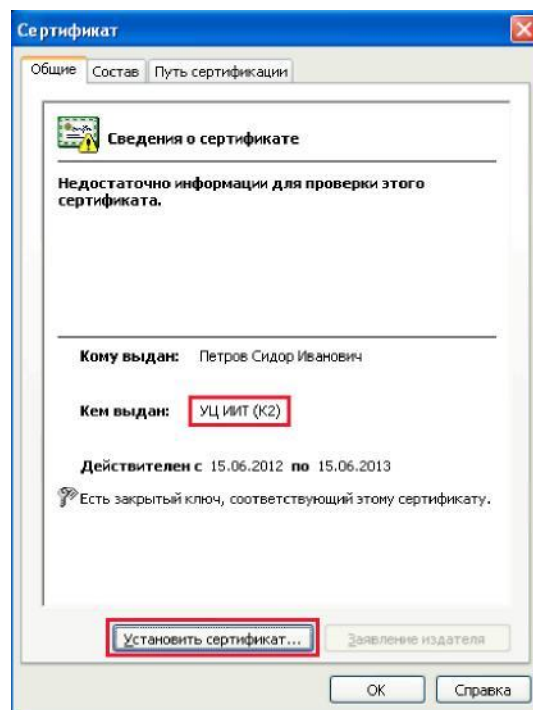


Рис. 4

Далее следуйте указаниям Мастера установки сертификатов. В ходе установки сертификата обращайте внимание на выбранные опции, которые должны соответствовать рисункам 5-6.

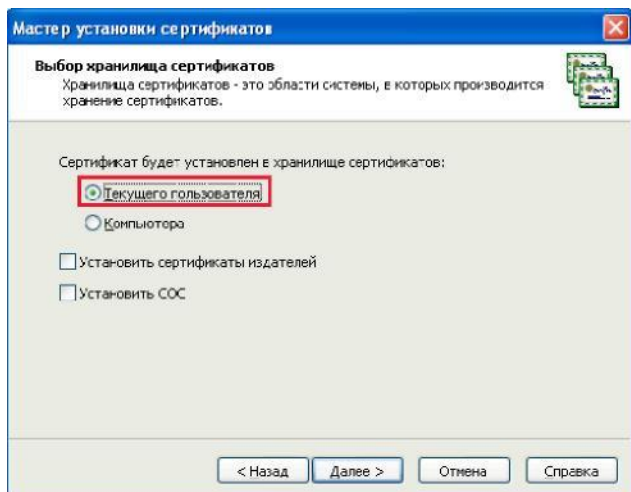


Рис. 5

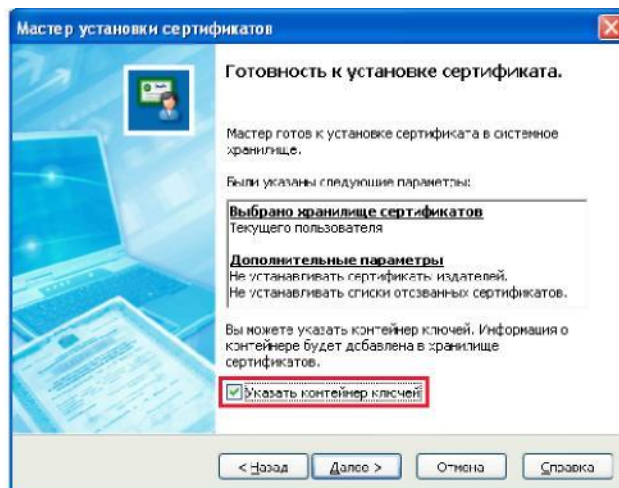


Рис. 6

У В появившемся на очередном шаге окне "ViPNet CSP - инициализация контейнера ключей" (Рис. 7) выберите устройство "eToken Aladdin(хххххххх)" и введите ПИН-код к нему.

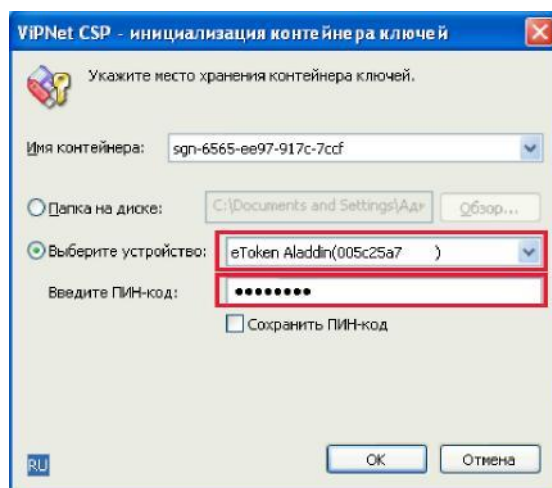


Рис. 7

• В появившемся окне (Рис. 8) повторно введите ПИН-код. На этом работа Мастера установки сертификата завершается (Рис. 9), нажмите "Готово" и переходите к следующему пункту инструкции.

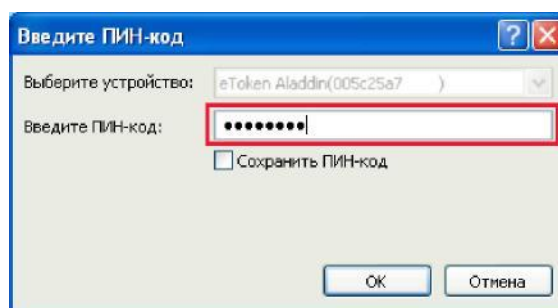


Рис. 8

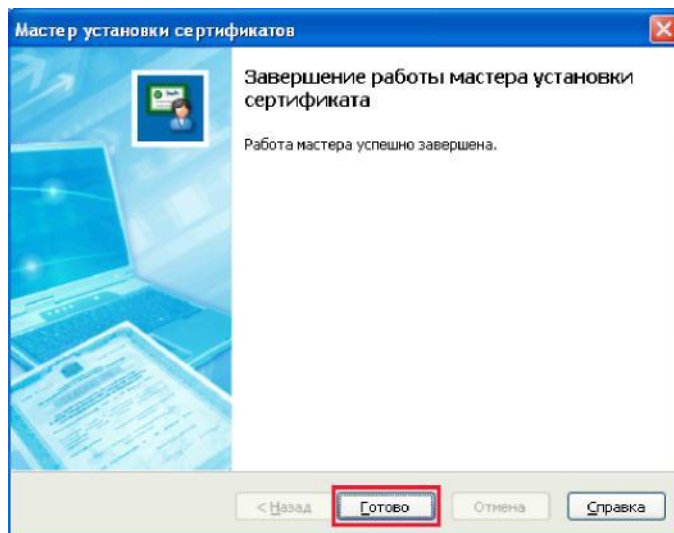


Рис. 916. Установка личного сертификата с компакт-диска (CD).

+ При работе Вы можете использовать ключи электронной подписи, размещенные на компакт-диске, а можете предварительно скопировать ключевой контейнер (файл с именем sgn-xxxx-xxxx-xxxx-xxxx) на жесткий диск Вашего компьютера.

- Запустите ViPNet CSP и убедитесь, что на закладке "Общие" включена опция "Включить поддержку работы ViPNet CSP через MS Crypto API" (Рис. 6)
- Перейдите на закладку "Контейнеры" (Рис. 10) и нажмите клавишу "Добавить".

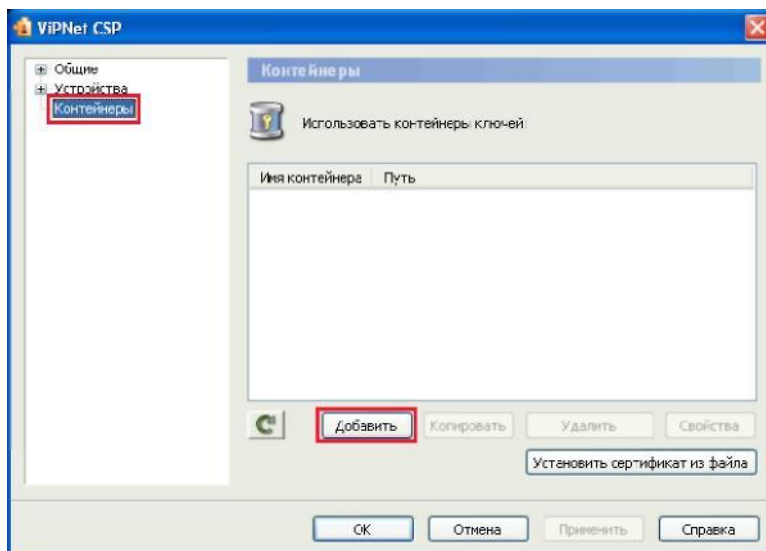


Рис. 10

У В окне "ViPNet CSP - инициализация контейнера ключей" (Рис. 11) нажмите клавишу "Обзор", в окне "Обзор папок" (рис. 12) укажите папку на жестком диске или компакт-диске, в которой размещен контейнер ключей электронной подписи, и нажмите "ОК" в окне "Обзор папок".

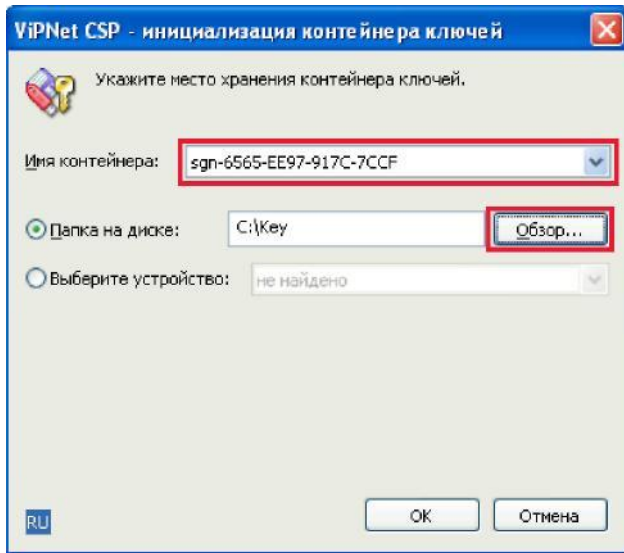


Рис. 11

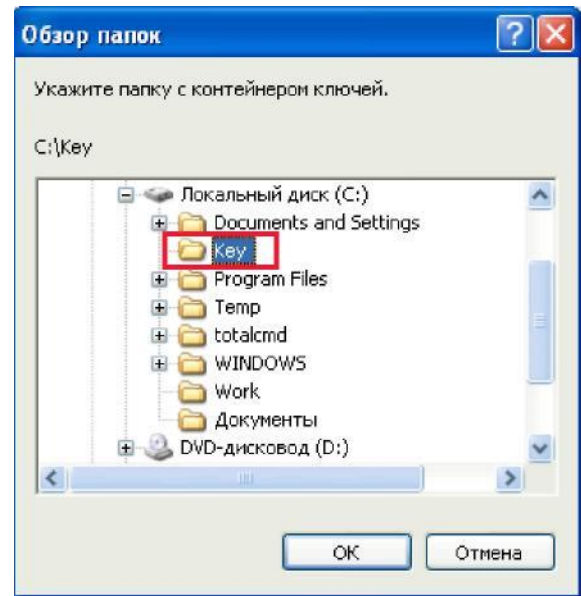


Рис. 12

- Убедитесь, что выбран именно контейнер ключей, а не иной файл. Т.е., в поле "Имя контейнера" окна "ViPNet CSP - инициализация контейнера ключей" (рис. 16) должно быть указано имя вида **sgn-xxxx-xxxx-xxxx-xxxx**. Если это не так, выберите необходимый файл контейнера ключей в раскрывающемся списке поля "Имя контейнера" (рис. 13) и нажмите "OK".

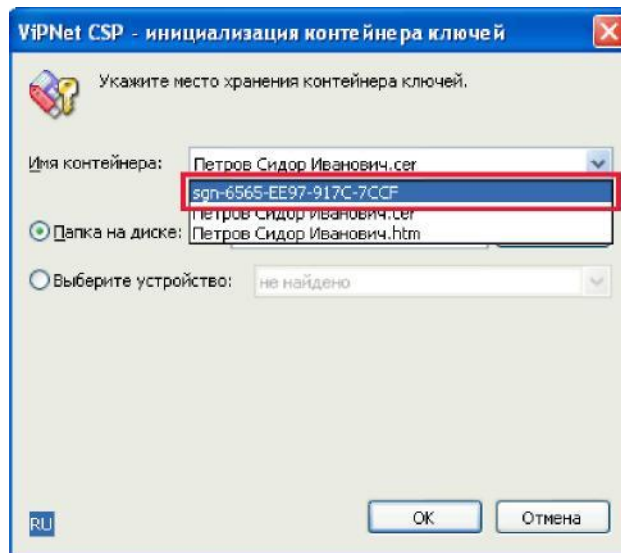


Рис. 13

После выбора контейнера ключей появится окно с запросом об установке найденного контейнере сертификата (рис. 14). Нажмите "Да", в результате сертификат будет установлен системное хранилище, а контейнер ключей добавлен в перечень используемых (рис. 15).

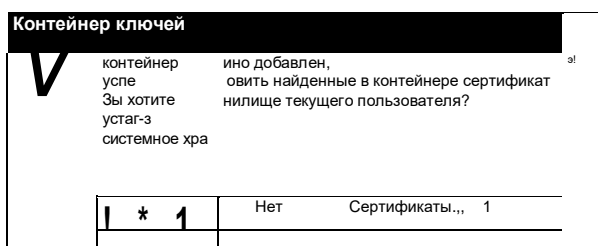


Рис. 14

- Нажмите "OK" (рис. 15) и переходите к выполнению следующего пункта инструкции.

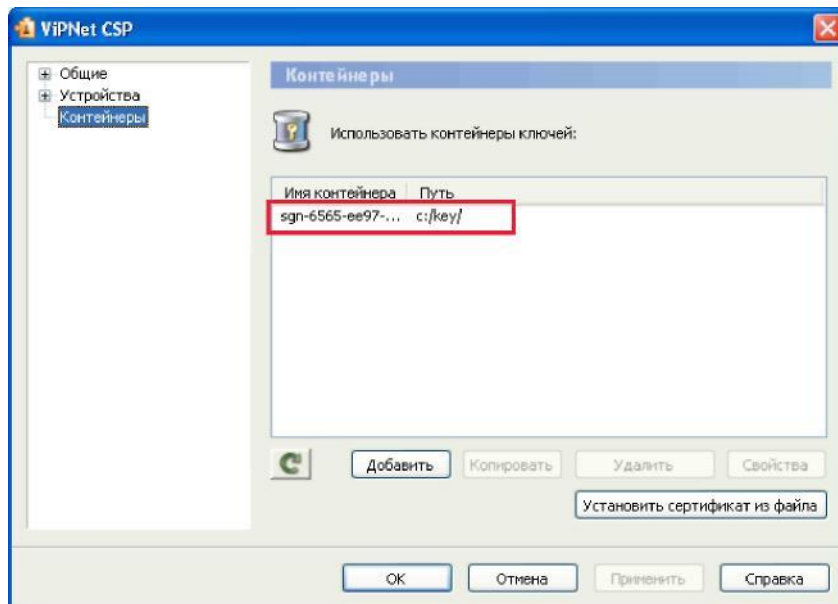
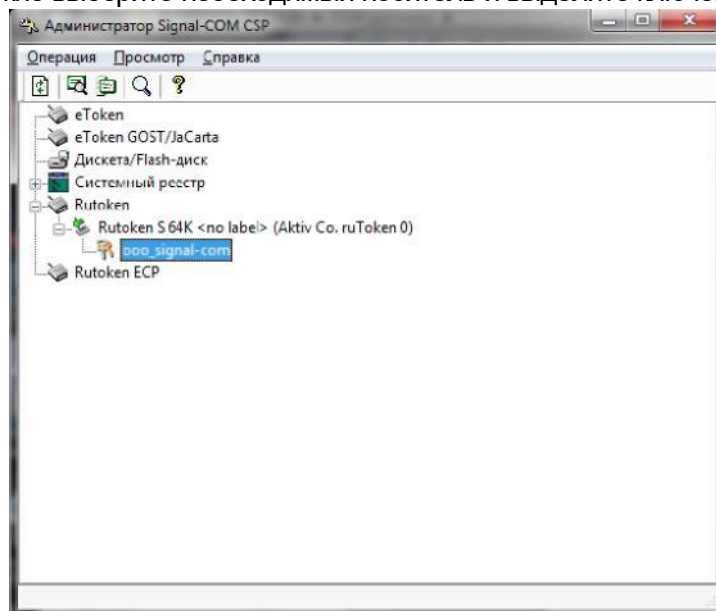


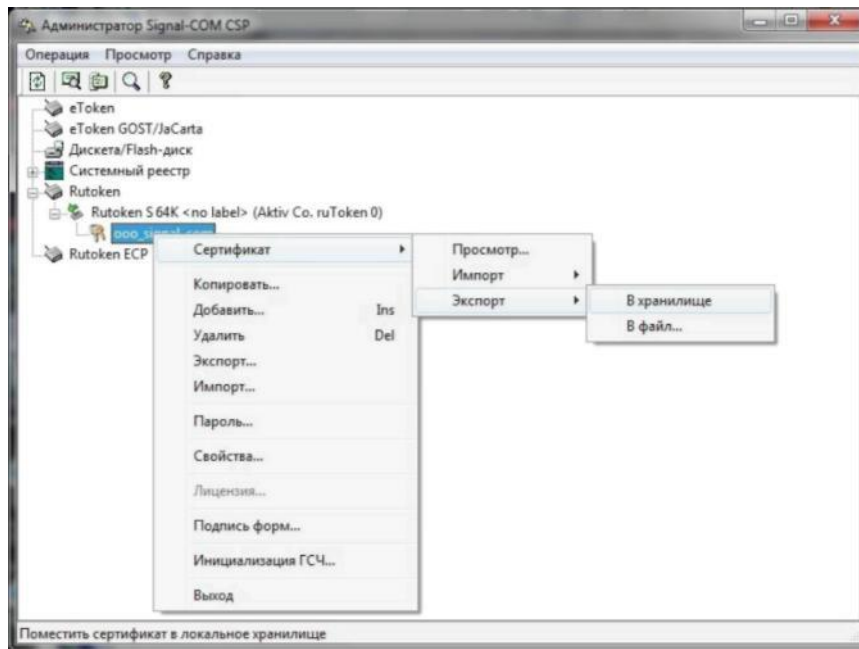
Рис. 15

4.1.4 Установка личного сертификата при помощи Signal-COM CSP

1. Запустите провайдер «Администратор Signal-COM CSP»
2. В появившемся окне выберите необходимый носитель и выделите ключевой контейнер.



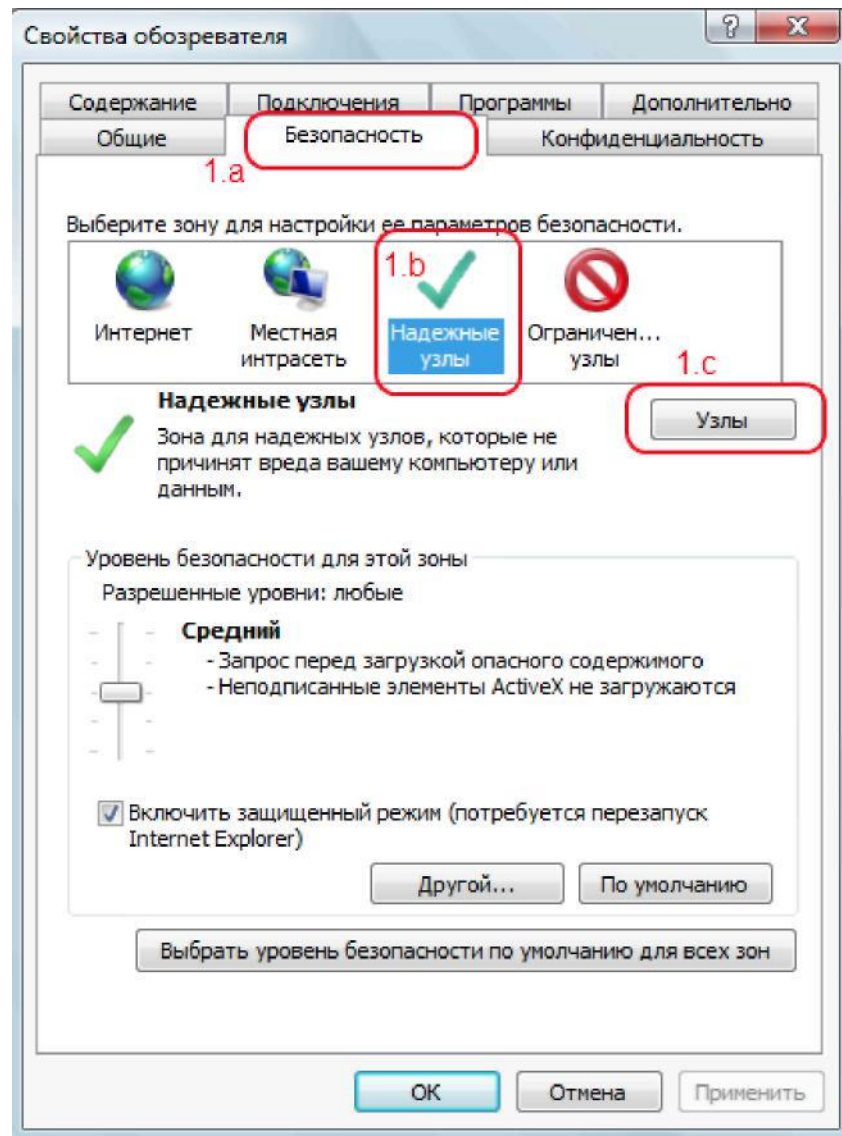
3. Нажмите на ключевом контейнере правой кнопкой мыши и выберите: «Сертификат» - «Экспорт» - «В хранилище»



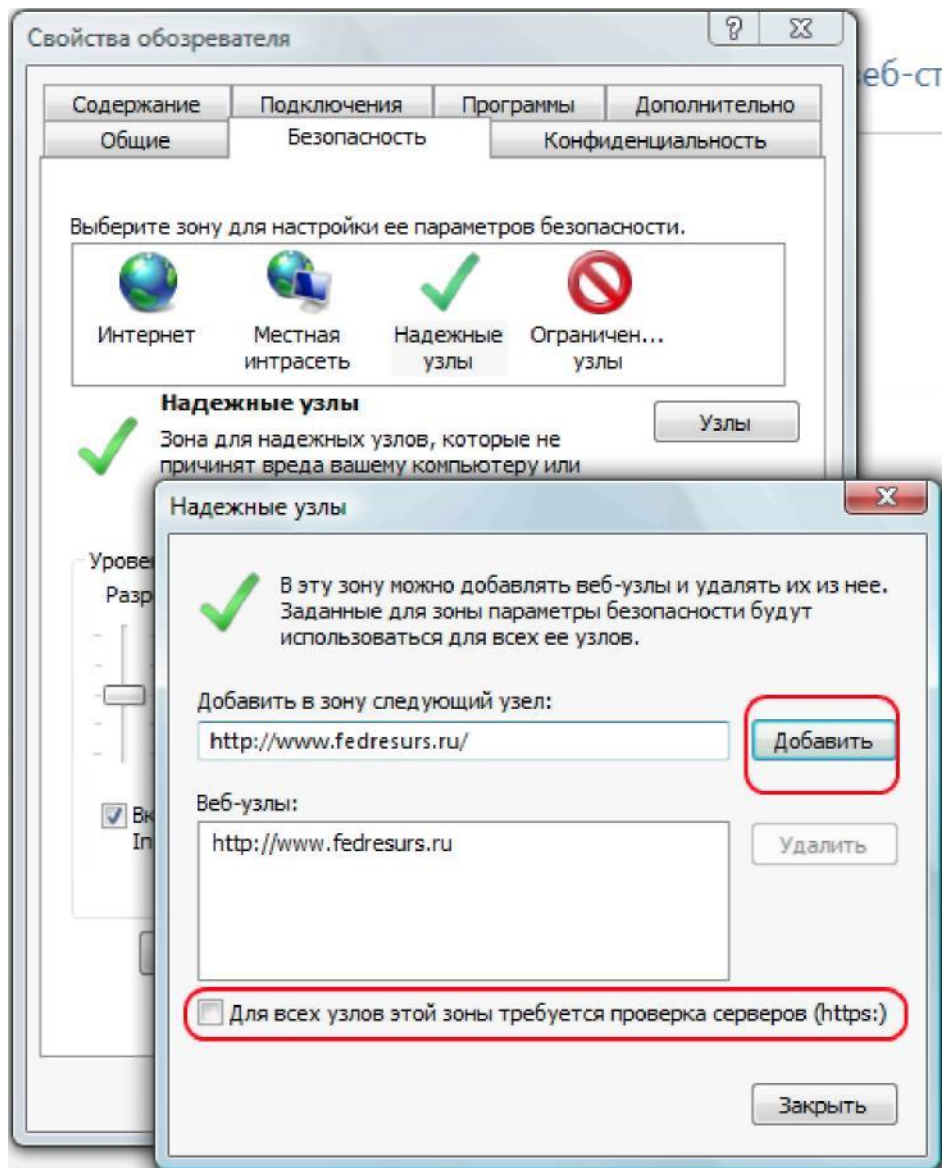
2. **Добавление сайта ЕФРСФДЮЛ в доверенные узлы**

Для возможности запуска ActiveX-компонента в браузере Internet Explorer, сайт ЕФРСФДЮЛ (<http://www.fedresurs.ru/>) должен быть включен в доверенные узлы. Делается это в настройках браузера (пример дан для браузера Internet Explorer 8): 1. Открыть меню «Сервис\Свойства обозревателя».

- a. Перейти на вкладку «Безопасность»;
- b. Выбрать «Надежные узлы»;
- c. Нажать на кнопку «Узлы»:



2. В открывшемся окне снять флажок «Для всех узлов этой зоны требуется проверка серверов», вписать в поле «Добавить в зону следующий узел:» значение <http://www.fedresurs.ru/>, нажать кнопку «Добавить»:




3. Закреть окно настроек и браузер.

3. **Разрешение запуска ActiveX-компонента подписи ЭП в браузере Internet Explorer**

Браузер Internet Explorer блокирует запуск ActiveX-компонентов. Для разрешения запуска, необходимо произвести следующие действия:

1. Открыть страницу проверки подписи на открытом сайте системы (<http://www.fedresurs.ru/Help>). Нажать кнопку проверить:

Проверка подписи


2. Если браузер заблокировал запуск ActiveX-компонента, в верхней части страницы появится сообщение:

9 Л"»^{этого} веб-угла нужна («дующая надстройка: 4nf oTeCS [ГССЗРСогшГ от "InfoTeK (неподтвержденный издатель)", Если в» доверяете этому веб-уму и этой надстроим и разрешаете ее вмаянвия. щелкните мась... X

А так же надпись о том, что не установлено программное обеспечение, необходимое для подписи сообщения.



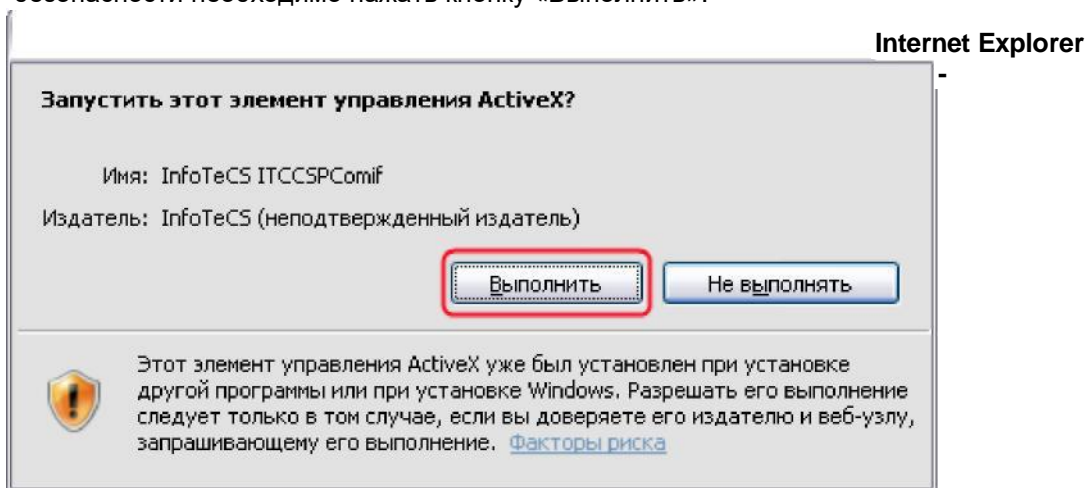
У Вас не установлено программное обеспечение для электронной подписи. Подробную информацию о его установке Вы можете получить в разделе "Помощь" открытого сайта.

3. Необходимо кликнуть мышью на желтой полоске с надписью и выбрать пункт меню «Запустить надстройку»

Щ Для этого копуша нужна (ядующая надстройка: Inf oTeCS 1GCC5PCortГ от "inf oTeCS (неподтвержденный издатель)". Если ем доверяете этому веб-уту и лей надстройке и **разсеаняте** ее выполнянча, щелкните мвеь...



4. Система попросит подтвердить запуск ActiveX-компонента, в окне предупреждения системы безопасности необходимо нажать кнопку «Выполнить»:

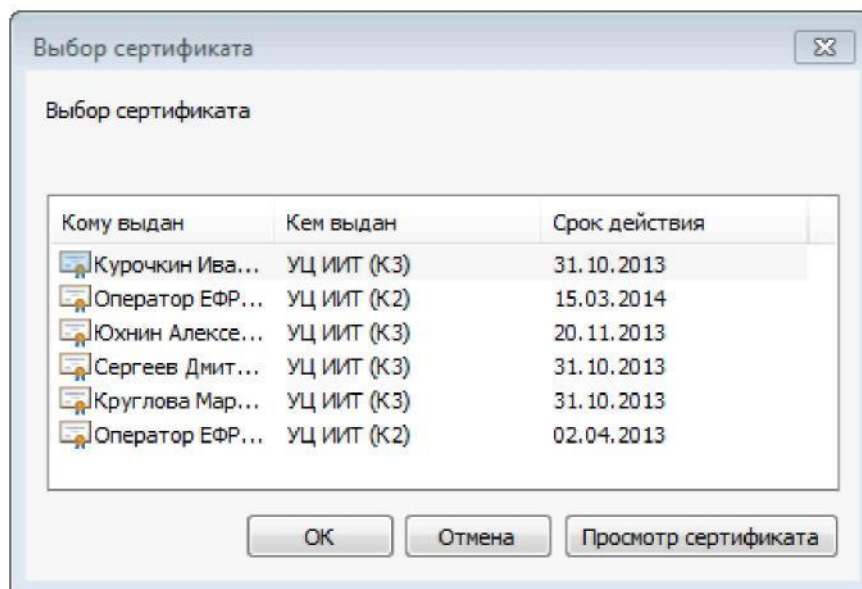


предупреждение системы безопасности

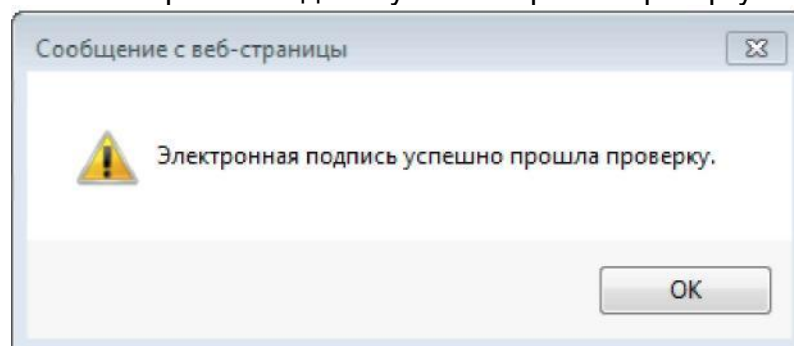
5 Проверка системы подписи

Проверку работоспособности системы подписи можно осуществить на странице <http://www.fedresurs.ru/help>. Порядок проверки:

1. Открыть страницу <http://www.fedresurs.ru/help>.
2. Нажать кнопку «Проверить». Откроется окно выбора сертификата



3. Выбрать сертификат, нажать кнопку «ОК». В зависимости от настроек используемого криптопровайдера может потребоваться ввод пароля или подключение ключевого носителя.
4. Будет произведена проверка подписи на сервере. Если подпись прошла проверку, будет выдано сообщение «Электронная подпись успешно прошла проверку»:



6 Решение вопросов с неработоспособностью системы подписи

1. Сообщение «Не установлено программное обеспечение ...»

При проверке подписи в разделе Помощь, после нажатия кнопки «Проверить» на странице <http://www.fedresurs.ru/Help> появляется надпись «Не установлено программное обеспечение, необходимое для подписи»



У Вас не установлено программное обеспечение для электронной подписи. Подробную информацию о его установке Вы можете получить в разделе "Помощь" открытого сайта.

Возможны 3 варианта:

1. Не установлен ActiveX-компонент. Необходимо произвести его установку в соответствии с инструкцией в разделе 32.
2. Запуск ActiveX-компонента в Internet Explorer запрещен. Необходимо разрешить его запуски и выполнение в соответствии с разделом 43
3. Используется браузер Internet Explorer в операционной системе Windows 7 64-bit (как определить версию системы, указано в разделе 71). В операционной системе Windows 7 64-bit из-за особенностей системы безопасности компонент подписи может быть запущен только в браузере Mozilla FireFox или Internet Explorer 32-bit. Инсталлятор браузера FireFox можно скачать на странице производителя <http://www.mozilla.com/ru/firefox/>, рекомендуется использовать версии от 8 и выше. Браузер бесплатен и полностью поддерживается функционалом АИС «СВЕДЕНИЯ О ФАКТАХ ДЕЯТЕЛЬНОСТИ ЮРИДИЧЕСКИХ ЛИЦ».

2. Сообщение «Сертификат не выбран»

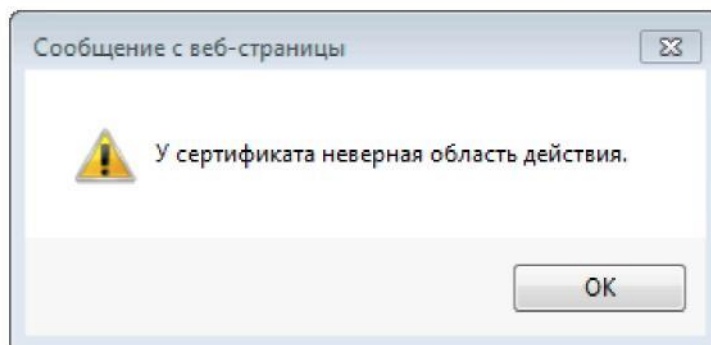
После нажатия кнопки «Проверить подпись» появляется сообщение «Сертификат не выбран». При этом, окно выбора сертификата не появляется.

Варианты:

1. Сертификаты (пользовательский и/или корневой) не были добавлены в локальное хранилище. Необходимо добавить их в соответствии с инструкциями в разделе 41.
2. Если используется браузер Internet Explorer, сайт <http://www.fedresurs.ru> необходимо добавить в доверенные узлы. Как это сделать, описано в разделе 42.

3. У сертификата неверная область действия

После нажатия кнопки «Проверить подпись» появляется сообщение «У сертификата неверная область действия». При этом, окно выбора сертификата не появляется.

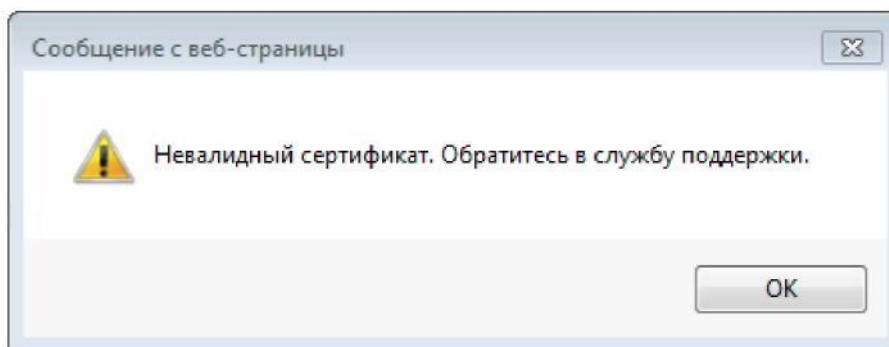


Варианты:

1. Сертификат не содержит в расширении Extended Key Usage объектный идентификатор, определяющий область применения сертификата в соответствии с Регламентом применения ЭП в ЕФРСФДЮЛ. Необходимо обратиться в удостоверяющий центр или в службу поддержки пользователей по адресу bhelp@interfax.ru.

4. При входе в личный кабинет сообщение «Невалидный сертификат»

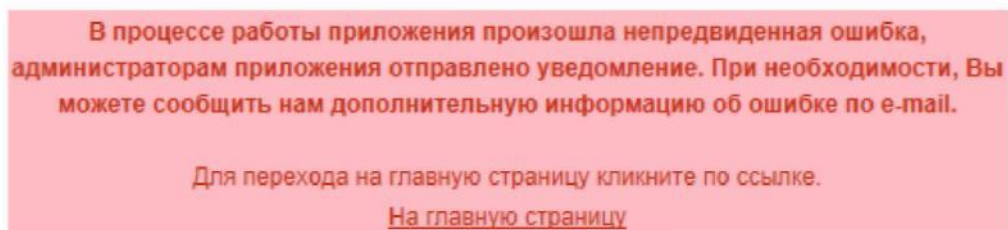
При входе в личный кабинет по сертификату сообщение «Невалидный сертификат. Обратитесь в службу поддержки».



Необходимо обратиться в службу поддержки пользователей по адресу bhelp@interfax.ru.

5. При проверке подписи – «красная ошибка»

При проверке подписи – «красная ошибка»:

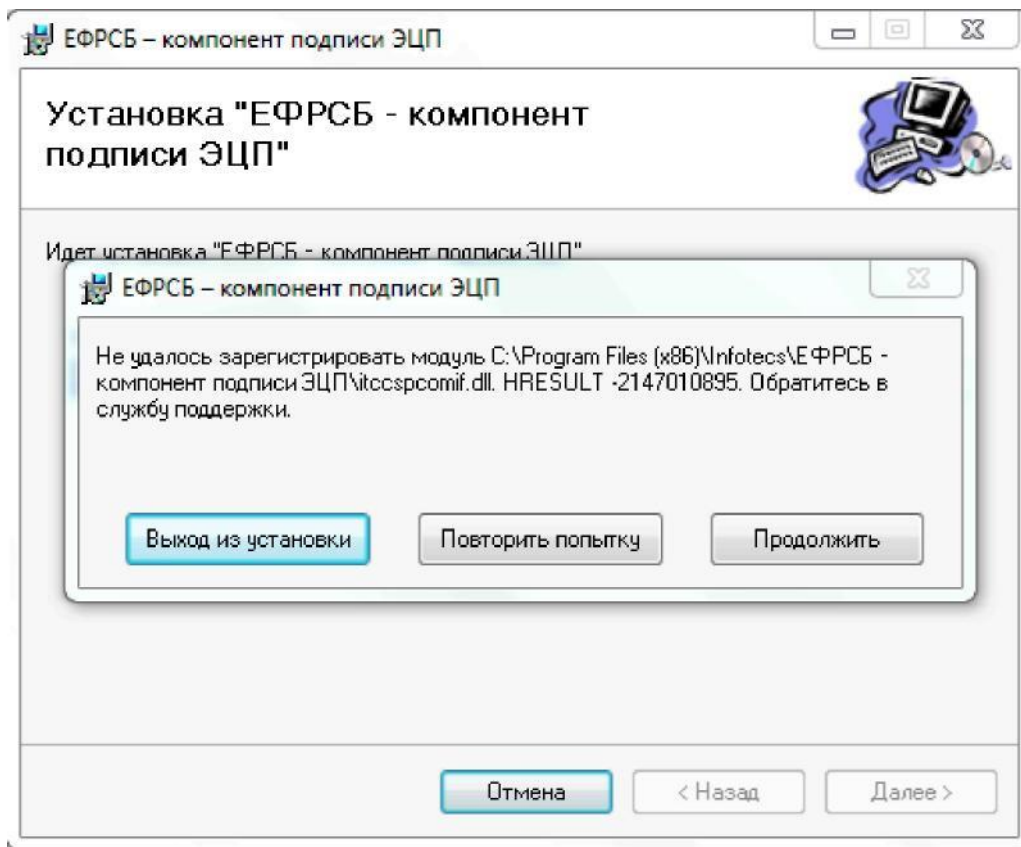


Если при проверке подписи – «красная ошибка», необходимо обратиться в службу поддержки пользователей по адресу bhelp@interfax.ru. Необходимо сообщить время, когда производилась проверка подписи и название удостоверяющего центра, в котором был получен сертификат подписи.

Желательно приложить к письму скриншот экрана с сообщением об ошибке (как сделать скриншот, описано в разделе 73).

6. При установке ActiveX-компонента подписи возникает ошибка «Не удалось зарегистрировать модуль...»

Сообщение об ошибке выглядит вот так:



Для устранения ошибки необходимо скачать дистрибутив Microsoft Visual C++ 2008 Redistributable Package (x86) по ссылке:

<http://www.microsoft.com/downloads/en/details.aspx?familyid=9b2da534-3e03-4391-8a4d-074b9f2bc1bf&displaylang=en> (на странице нажать кнопку Download). После скачивания, запустить файл vc_redist_x86.exe для установки компонента.


Важно! В Windows 7 необходимо запускать инсталлятор от имени администратора (кликнуть правой кнопкой мыши, в меню выбрать "Запустить от имени администратора").

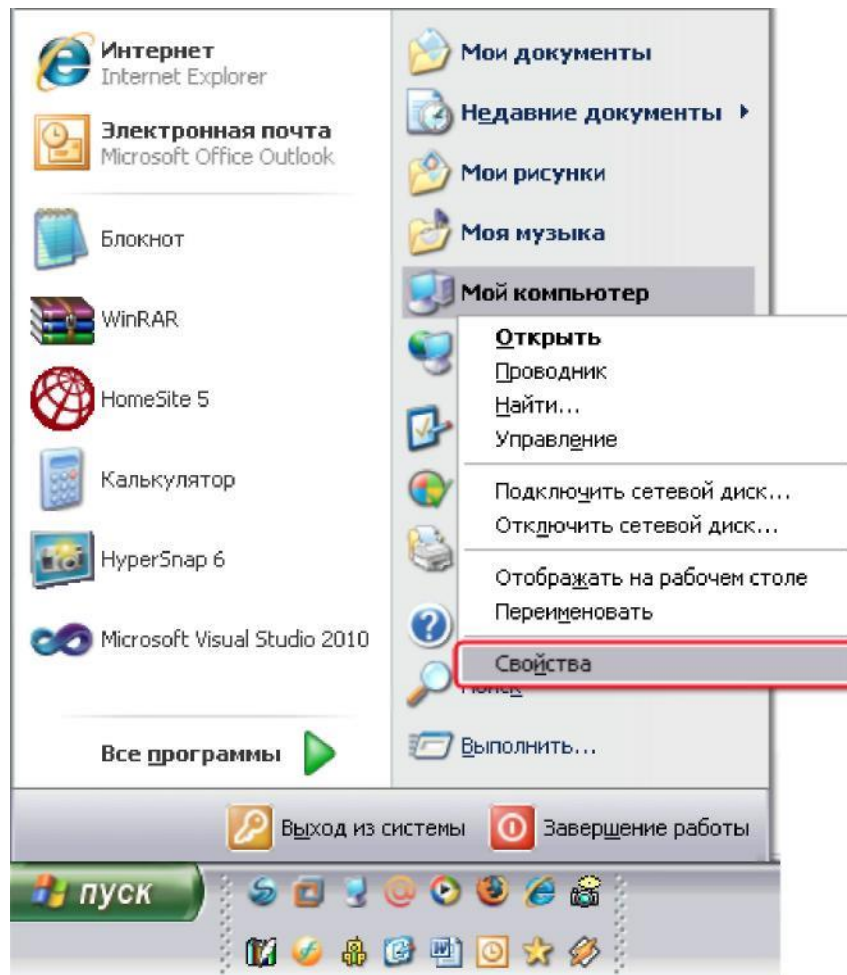
7 Приложения

Поведение ActiveX компонента зависит от того, в какой операционной системе и в каком браузере работает пользователь. Для разных операционных систем и браузеров применяются различные методы решения возникающих вопросов. Имеет значение не только версия системы, но и ее разрядность (64 или 32) – это особенно важно для операционных систем Windows 7 и Vista; также может иметь значение номер сервис-пака (SP).

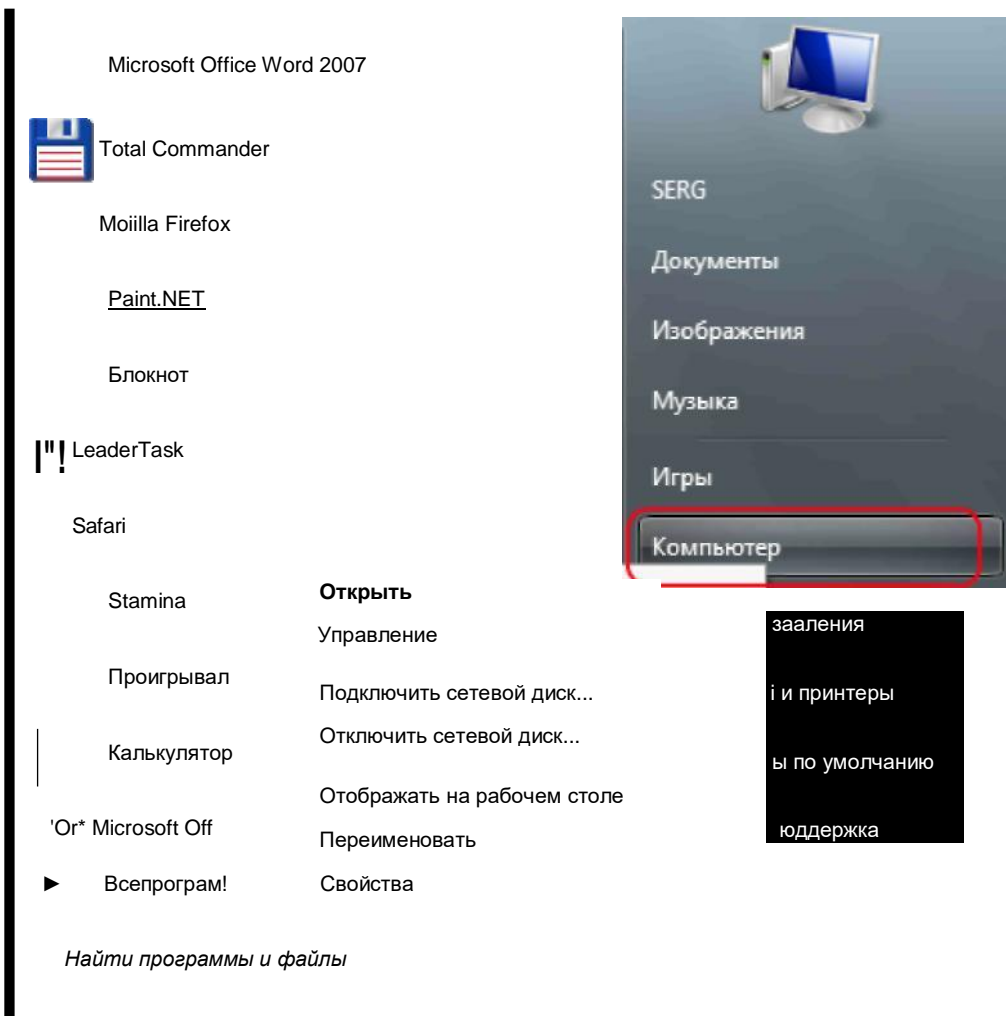
1. Как определить версию Windows



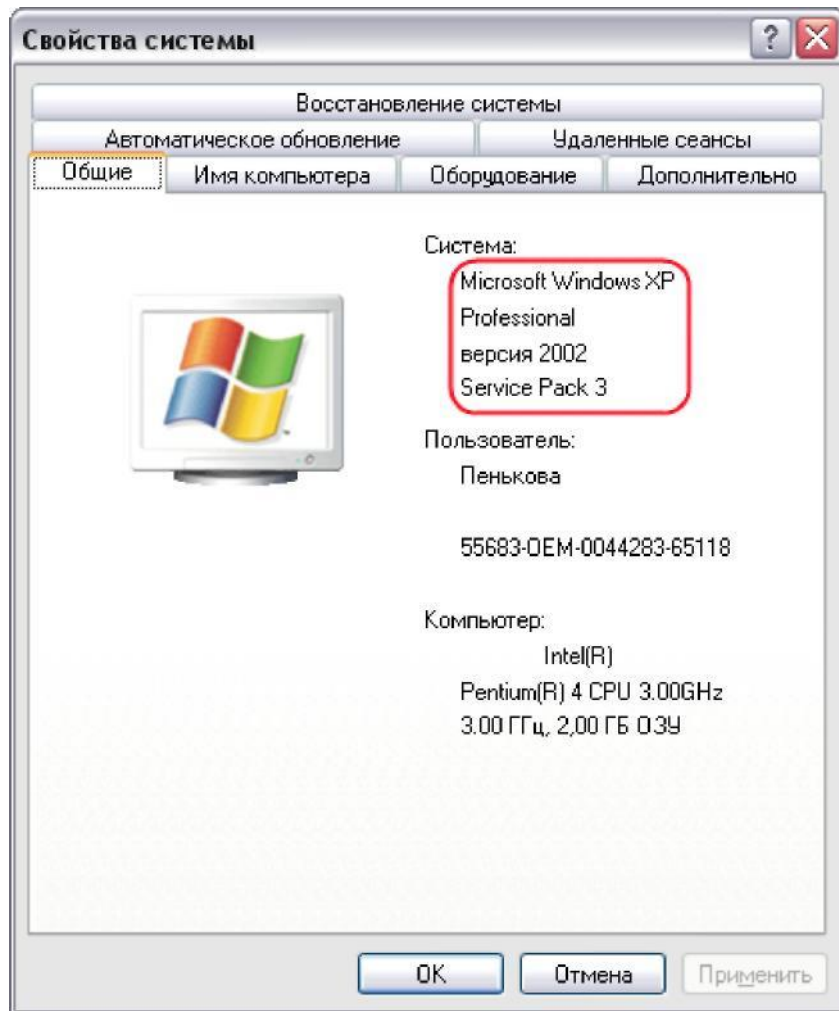
1. Открыть главное меню по кнопке Пуск (в Windows XP), или  (в Windows Vista/7)
2. Найти пункт меню «Мой компьютер» (в Windows XP) или «Компьютер» (в Windows Vista/7), нажать на нем правой кнопкой, выбрать в выпадающем меню пункт «Свойства»
 - а. Внешний вид главного меню в операционной системе Windows XP:



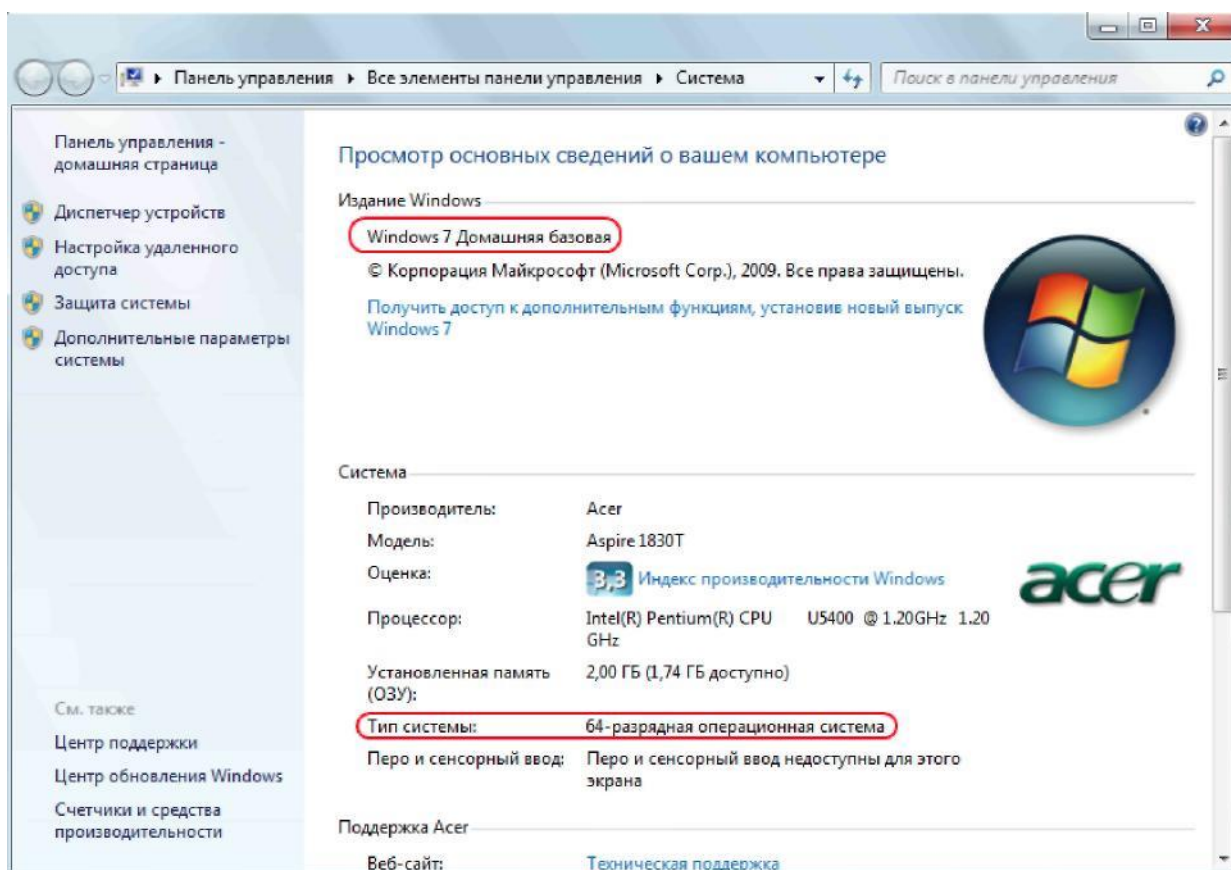
b. Главное меню в Windows 7 или Vista:



3. В открывшемся окне найти версию операционной системы.
 - а. Для Windows XP окно с версией операционной системы выглядит так:



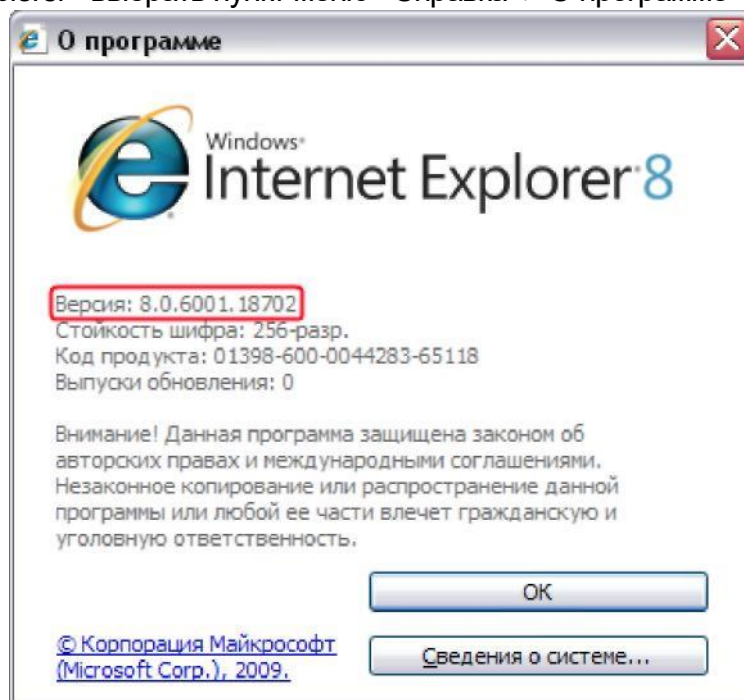
- b. Для Windows 7 или Vista окно со сведениями о компьютере и операционной системе выглядит следующим образом.



На рисунках выше выделены сведения, которые необходимо сообщить в службу технической поддержки по запросу или учесть при выполнении некоторых инструкций, приведенных в настоящем документе.

2. Как определить версию браузера

1. В Internet Explorer - выбрать пункт меню «Справка -> О программе»:



2. В Mozilla Firefox – выбрать пункт меню «Справка-> О Mozilla Firefox»:



3. Как сделать скриншот

Скриншот – это «фотография» рабочего стола. Он часто бывает необходим для решения проблем, связанных с работой системы.

1. Нажать на клавиатуре кнопку «PrtSc» (PrintScreen) она расположена в правой верхней части клавиатуры, рядом с кнопкой F12.
2. Открыть Word.
3. Нажать Ctrl+V, после этого в документе Word появится рисунок с изображением рабочего стола.
 - а. П.п. 2-5 необходимо повторить столько раз, сколько скриншотов нужно сделать.
4. Сохранить документ.
5. Выслать сохраненный документ на адрес bhelp@interfax.ru.