Инструкция по работе с электронной подписью на портале Росреестра с использованием криптографических программных средств

Москва 2015

ОГЛАВЛЕНИЕ

1 ПОЛУЧЕНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ

Для формирования заявления и подачи документов в электронном виде на портале Росреестра необходимо использовать электронную подпись.

Электронная подпись (ЭП) предназначена для идентификации лица, подписавшего электронный документ, и является полноценной заменой (аналогом) собственноручной подписи в случаях, предусмотренных законом.

Правовые условия использования электронной подписи в электронных документах регламентирует Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи».

Получить юридически значимый сертификат электронной подписи можно в удостоверяющем центре.

Информация для удостоверяющих центров, исполнивших требования распоряжения Росреестра от 27.03.2014 № Р/32 размещена на Официальном сайте Росреестра по ссылке: https://rosreestr.ru/site/fiz/programmnoe-obespechenie/perechen-udostoveryayushchikh-tsentrov-ispolnivshikh-trebovaniya-rasporyazheniya-rosreestra-ot-27-03/?sphrase_id=674200.

Получить подробную информацию об электронной подписи, способах её получения и использования можно на сайте Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России): http://minsvyaz.ru/ru/activity/directions/4/#section-faq.

2 ПРЕДВАРИТЕЛЬНЫЕ УСТАНОВКИ

Для корректного использования сертификата электронной подписи при отправке документов и заявления в электронном виде на Портале Росреестра необходимо установить специализированное программное обеспечение: программное обеспечение КриптоПро либо программный компонент CAPICOM.

Список специализированных программных компонентов КриптоПро, необходимые для работы с ЭП:

1. КриптоПро CSP. Криптопровайдер КриптоПро CSP предназначен для:
   - авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной подписи;
   - обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты;
   - обеспечения аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;
   - контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;
   - управления ключевыми элементами системы в соответствии с регламентом средств защиты.

   Руководство по установке КриптоПро CSP находится по ссылке: http://cryptoarm.ru/Kak-ustanovit-KriptoPro-CSP.

2. CryptoPro Browser Plug-in. КриптоПро ЭЦП Browser plug-in предназначен для создания и проверки электронной подписи на веб-страницах с использованием криптопровайдера "КриптоПро CSP". Может использоваться в большинстве современных браузеров: Internet Explorer, Mozilla Firefox, Opera, Google Chrome, Apple Safari.
   CryptoPro Browser Plug-in доступен по ссылке: https://www.cryptopro.ru/products/cades/plugin.
3. КриптоАРМ Стандарт (либо Стандарт PRO). КриптоАРМ – программа, предназначенная для шифрования и расшифрования данных, создания и проверки электронной подписи с использованием сертификатов открытых ключей, для работы с сертификатами и криптопровайдерами. Используя криптопровайдер «КриптоПро CSP», программа «КриптоАРМ» позволяет работать с сертифицированными средствами, создавать электронную подпись, равнозначную собственноручной.
   Руководство пользователя доступно по ссылке: http://cryptoarm.ru/upload/docs/user_guide.pdf.

Программный компонент CAPICOM предназначен для электронной подписи данных, проверки ЭП, отображения информации об ЭП и сертификате, добавлять или удалять сертификаты, для шифрования и расшифровки данных. Компонент CAPICOM используется только в Internet Explorer. На данный момент поддержка CAPICOM производителем прекращена.

В большинстве случаев, программа установки программных компонентов универсальна для всех пользователей. Для стандартной установки надо лишь заполнять поля по необходимости, ставить галочки и нажимать “Далее”. При возникновении вопросов по инсталляции ПО, пригласите системного администратора или опытного пользователя.

3 НАСТРОЙКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КРИПТОПРО

Предварительные настройки

Для того, чтобы браузер не запрашивал каждый раз подтверждение доступа к хранилищу – добавьте адрес портала Росреестра в список доверенных веб-сайтов. Для этого

1. Выберите Пуск – КриптоПРО – Настройки ЭЦП Browser Plug-in

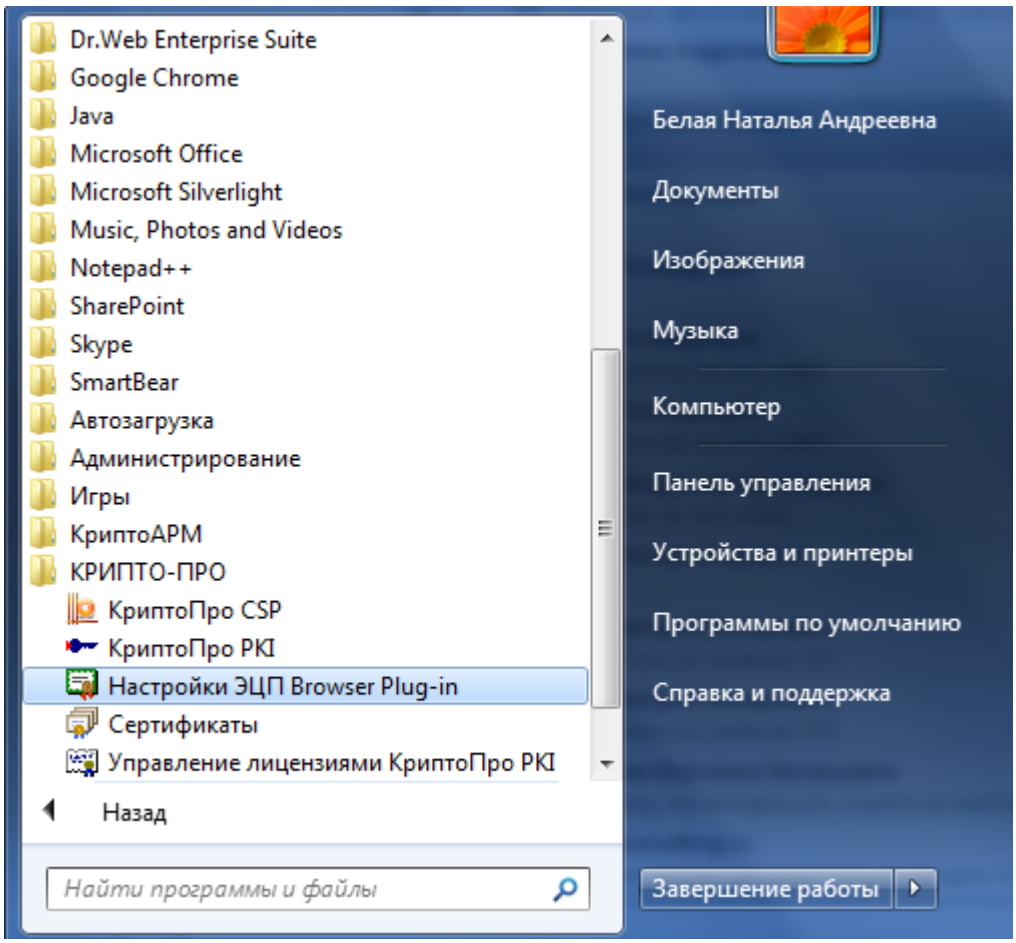

Рисунок 1.

2. Добавьте необходимый узел. Нажмите кнопку «Добавить». Убедитесь, что адрес появился в Списке доверенных узлов. Нажмите кнопку «Сохранить»

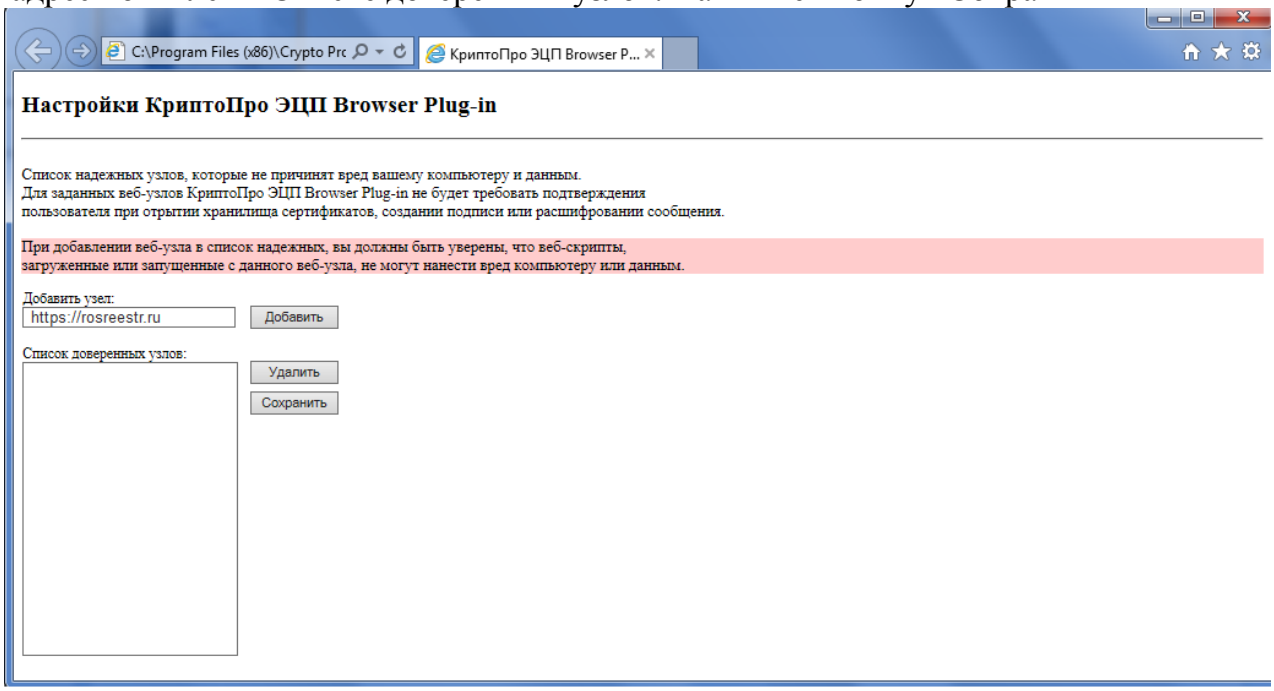

Рисунок 2.

Установка сертификата

1. Нажмите на иконку сертификата правой кнопкой мыши и выберите «Установить сертификат».

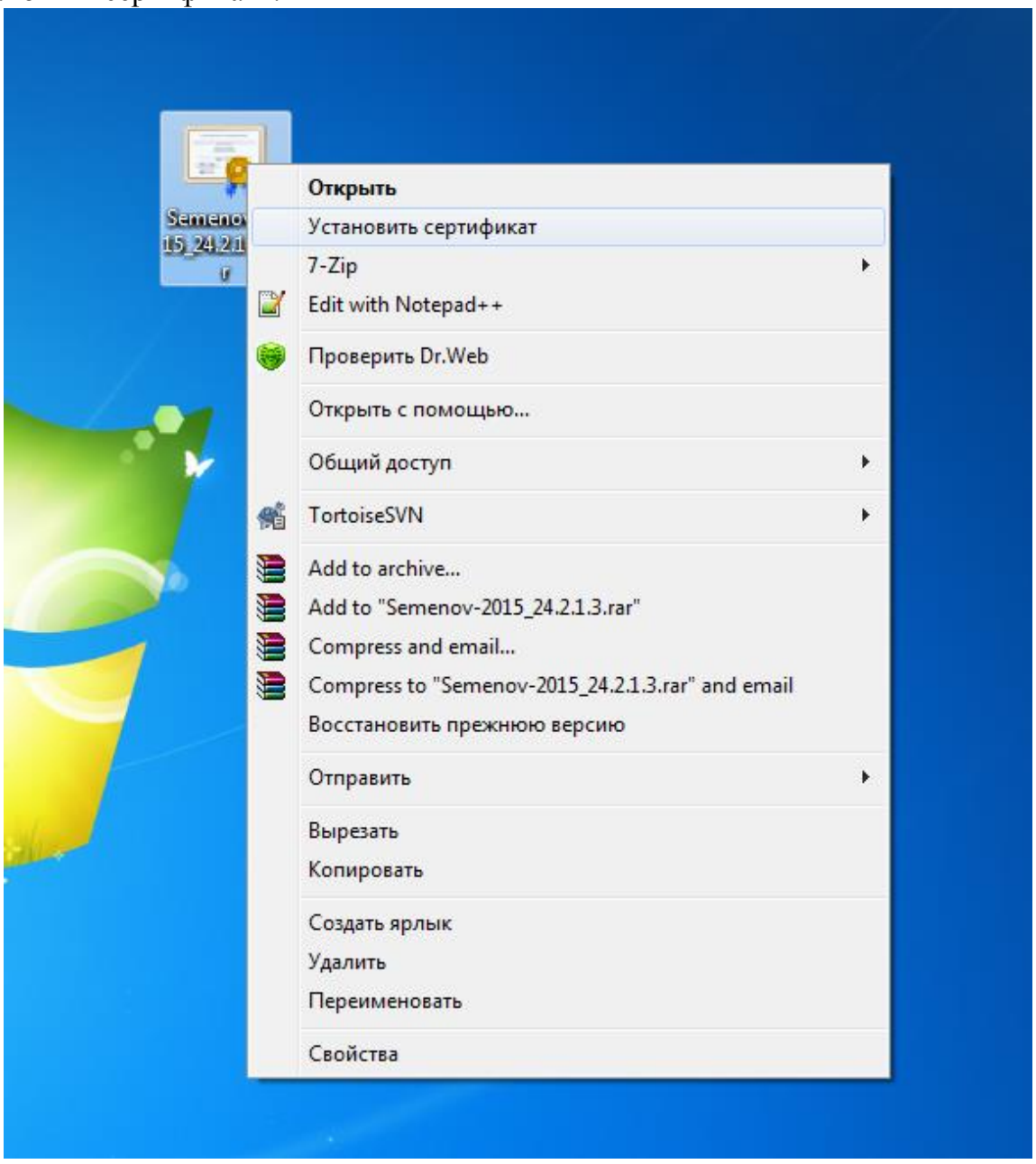

Рисунок 3.

2. В окне предупреждения системы безопасности нажмите «Открыть».

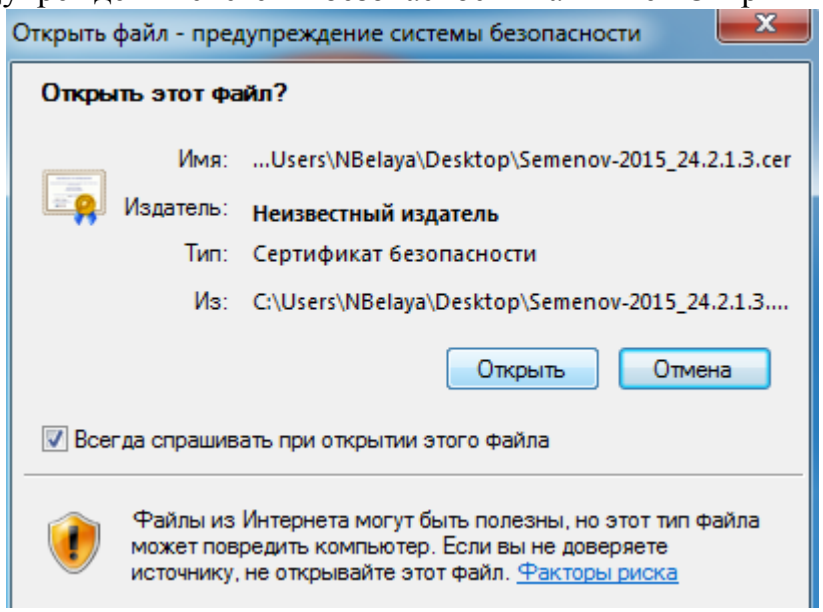

Рисунок 4.

3. Откроется мастер импорта сертификатов. Нажмите «Далее».

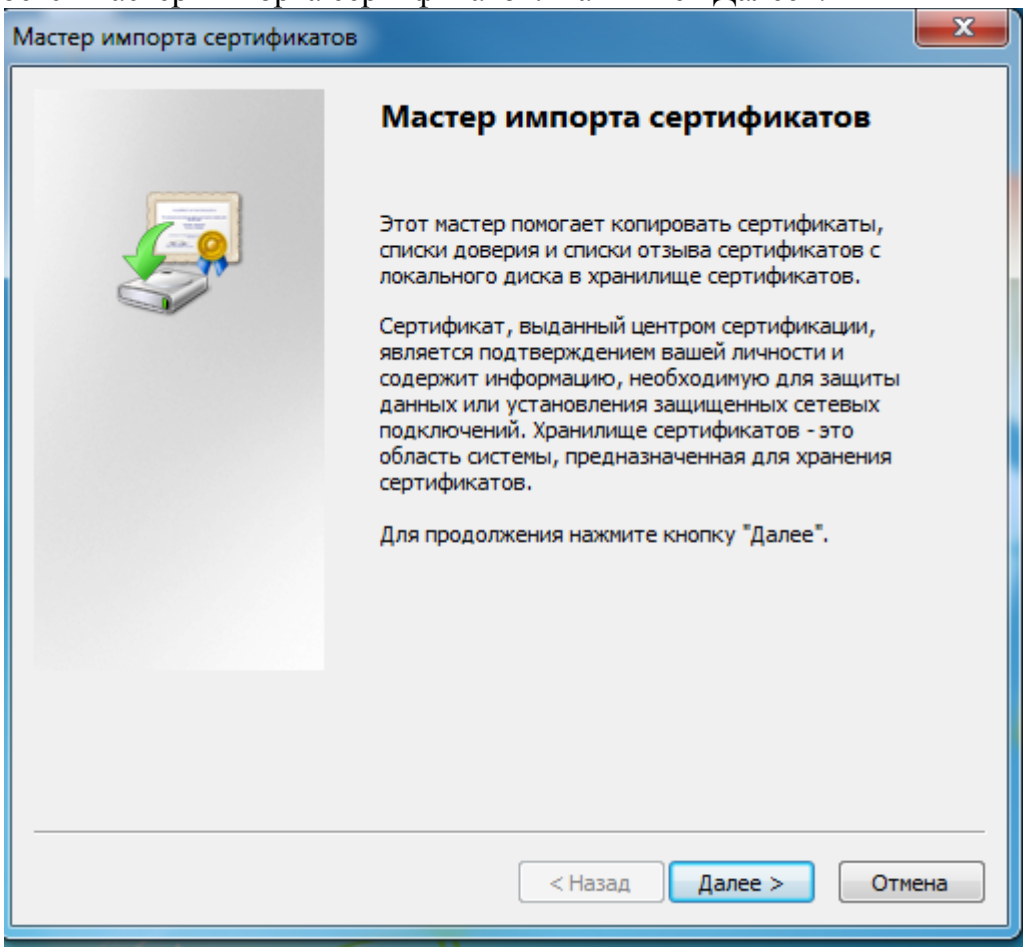

Рисунок 5.

4. В окне выбора хранилища сертификатов выберите «Поместить все сертификаты в следующее хранилище» и нажмите «Обзор».

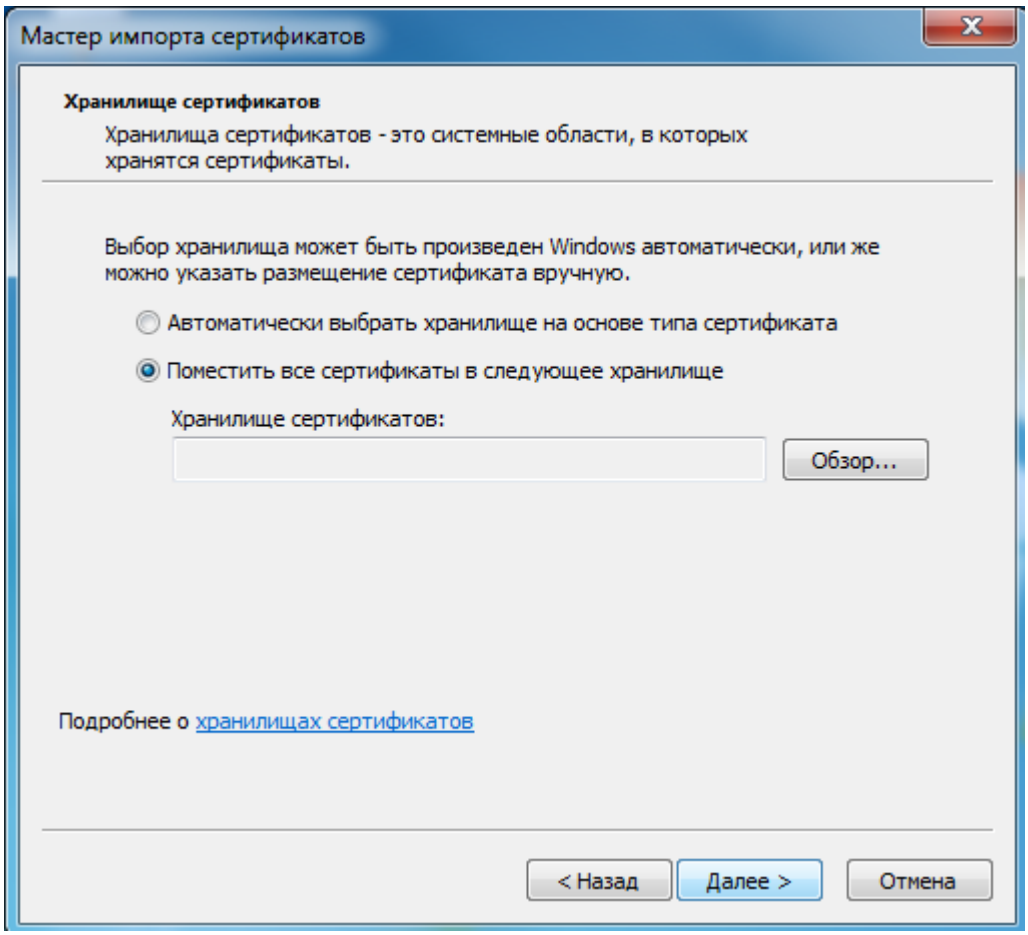

Рисунок 6.

5. Выберите «Доверенные корневые центры сертификации». Нажмите «ОК».

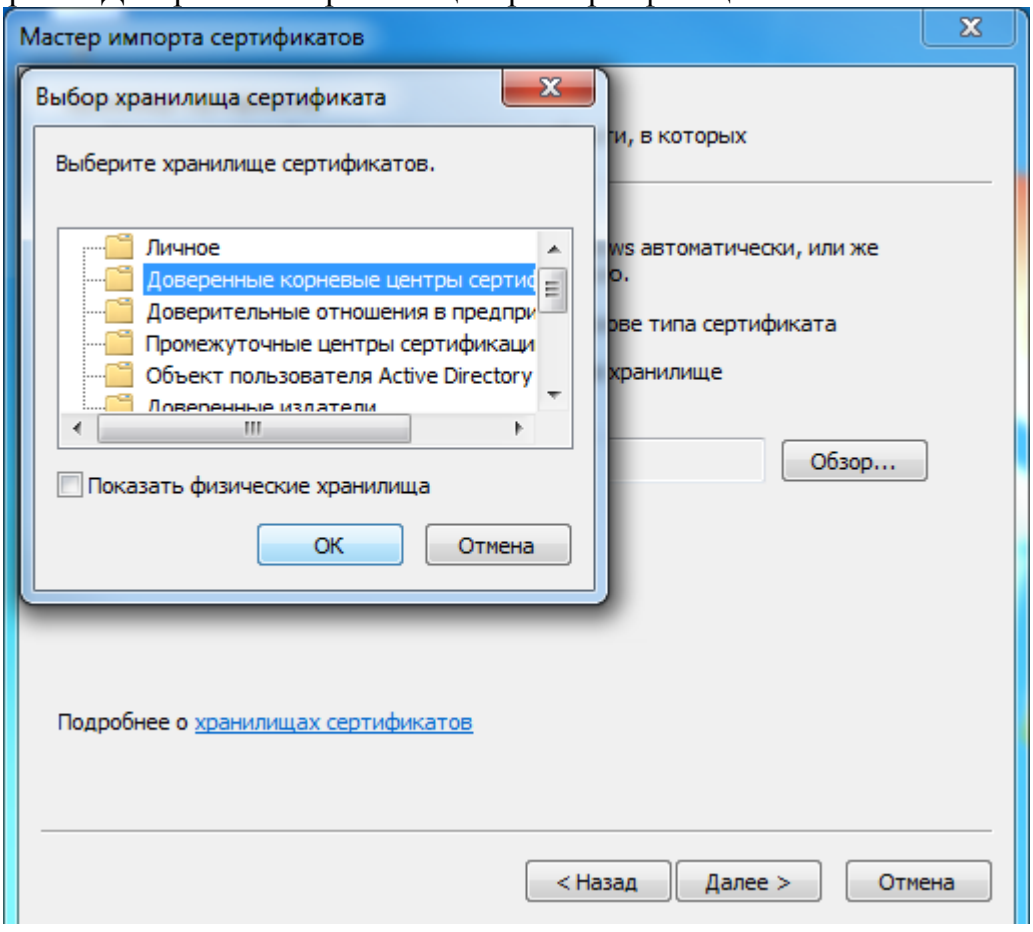

Рисунок 7.

6. Нажмите «Готово».

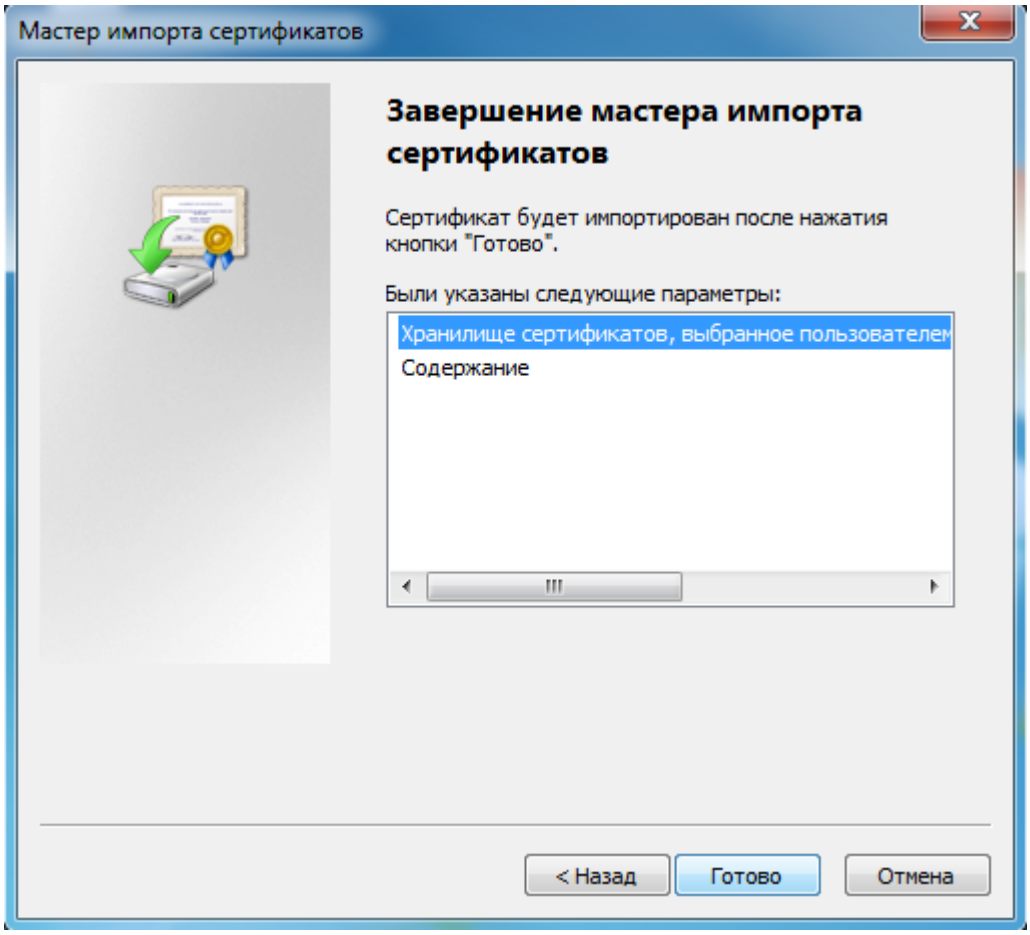

Рисунок 8.

7. Сертификат успешно импортирован в Доверенные корневые центры сертификации.

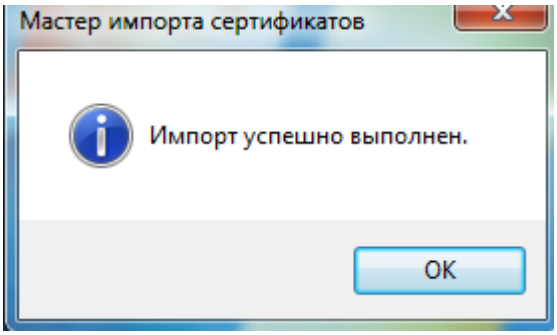

Рисунок 9.

Электронная подпись при подаче документов

3.1.1 Подписание документа

Для того чтобы подписать документ:

1. В главном окне программы КриптоАРМ Стандарт откройте раздел Подпись.

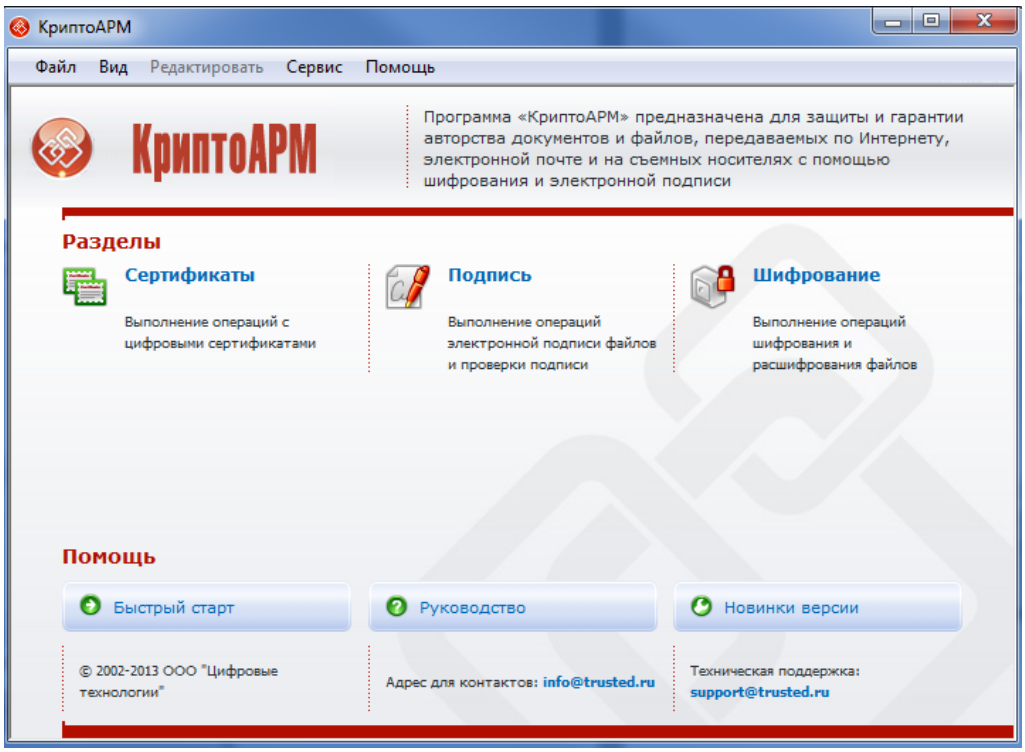

Рисунок 10.

2. Выберите пункт «Подписать».

3. Откроется Мастер создания электронной подписи.

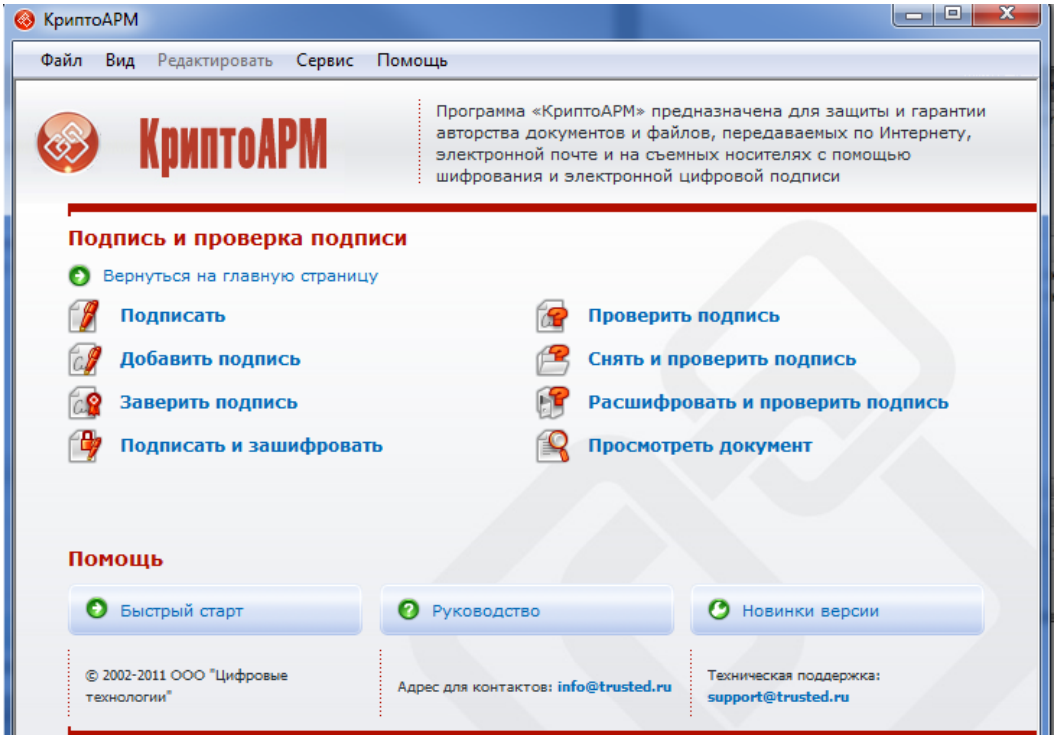

Рисунок 11.

Альтернативный вариант:

Можно подписать документ в проводнике, для этого:

1. Нажмите правой кнопкой мыши на документе, который хотите подписать.
2. Выберете «КриптоАРМ – Подписать…».

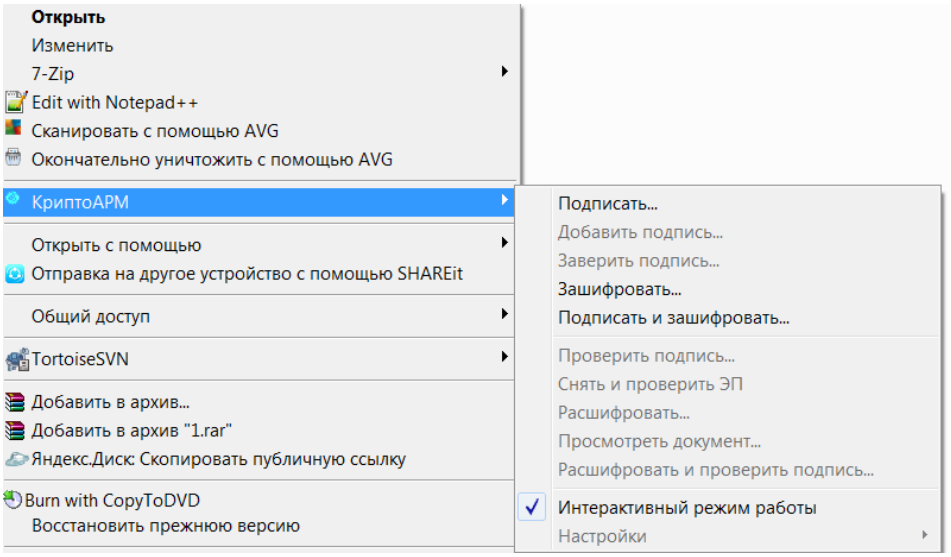

Рисунок 12.

3. Откроется Мастер создания электронной подписи.

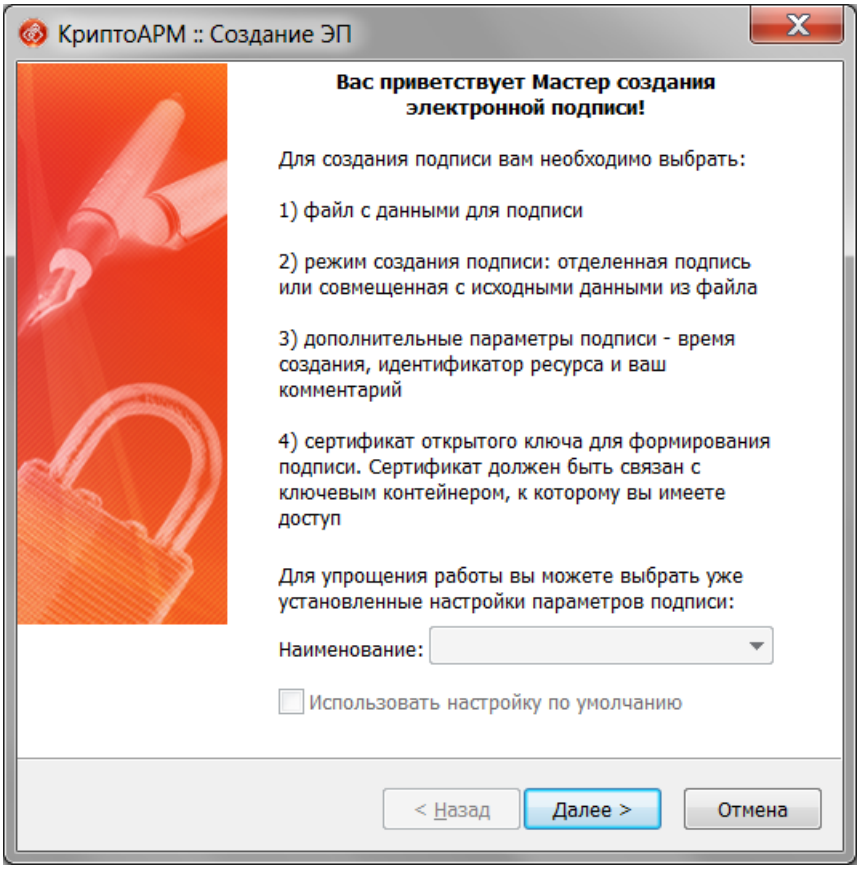

Рисунок 13.

4. Ознакомьтесь с процессом подписания документа и нажмите кнопку «Далее».
5. В появившемся окне выберите папку с файлами или отдельный файл, которые необходимо подписать (при альтернативном варианте подписания из проводника файл добавляется автоматически).

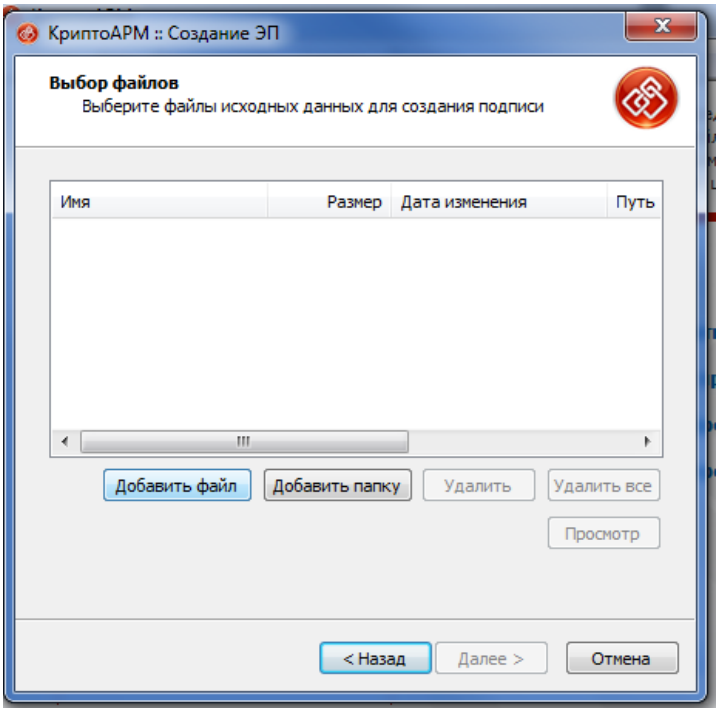

Рисунок 14.

6. Нажмите кнопку «Далее».

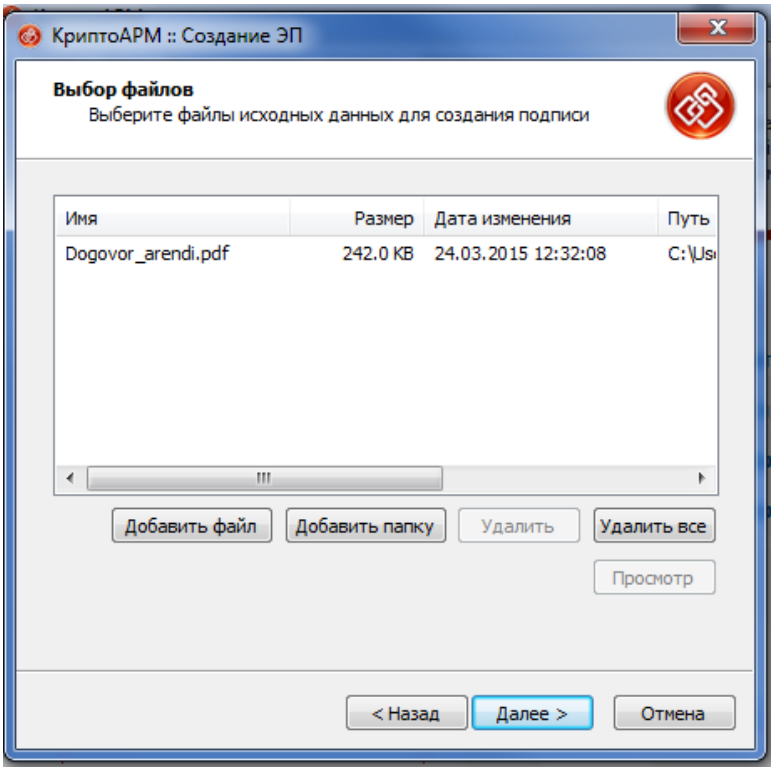

Рисунок 15.

7. Выберете желаемый выходной формат .sig – DER-кодировка. Нажмите кнопку «Далее».

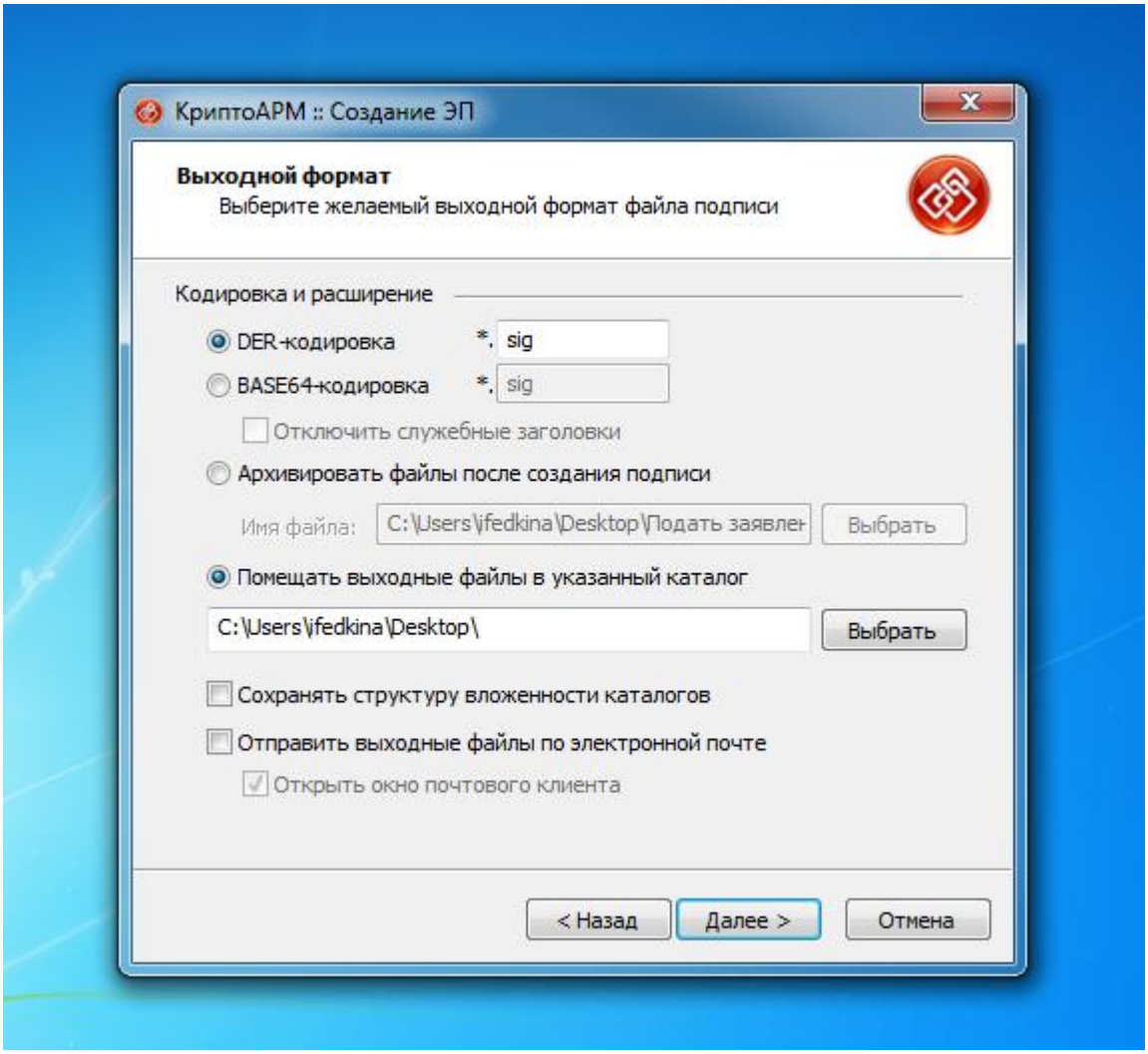

Рисунок 16.

8. Установите флаг «Включить время создания подписи». Установите флаг «Сохранить подпись в отдельном файле» для создания отсоединенной ЭП. Нажмите кнопку «Далее».

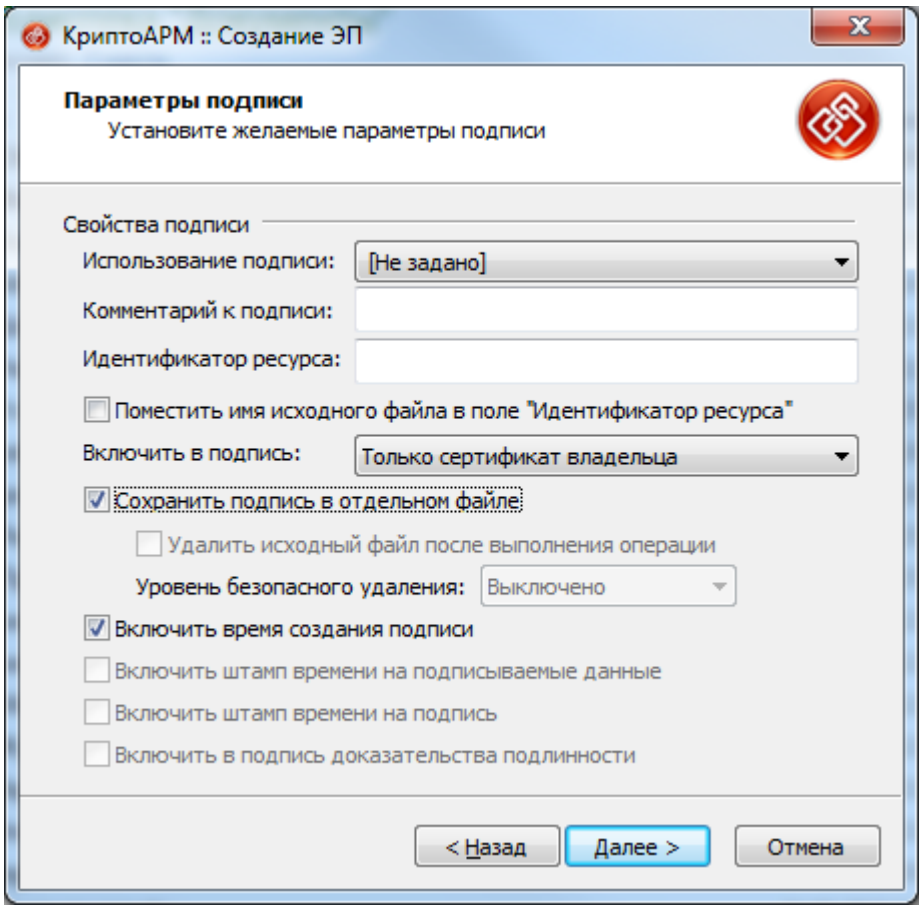

Рисунок 17.

9. Выберите сертификат для создания подписи, т.е. ваш личный сертификат, которым Вы собираетесь подписать документ. Хеш алгоритм определится автоматически.

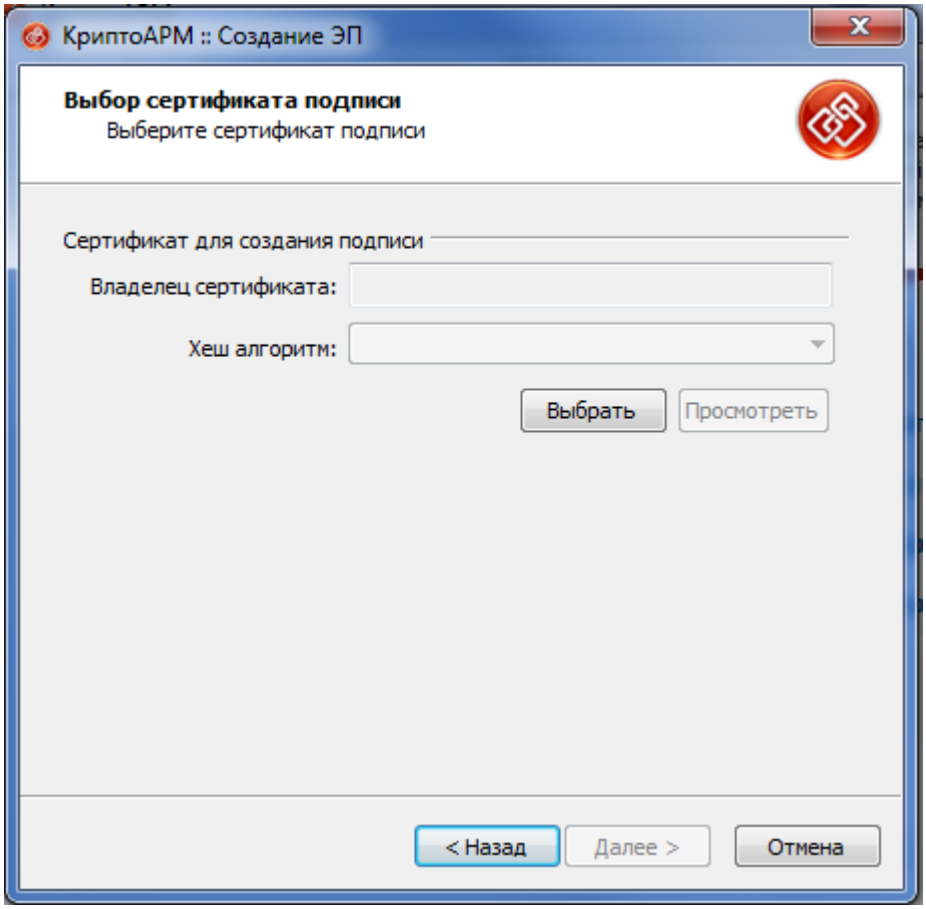

Рисунок 18.

10. Нажмите кнопку «Далее».

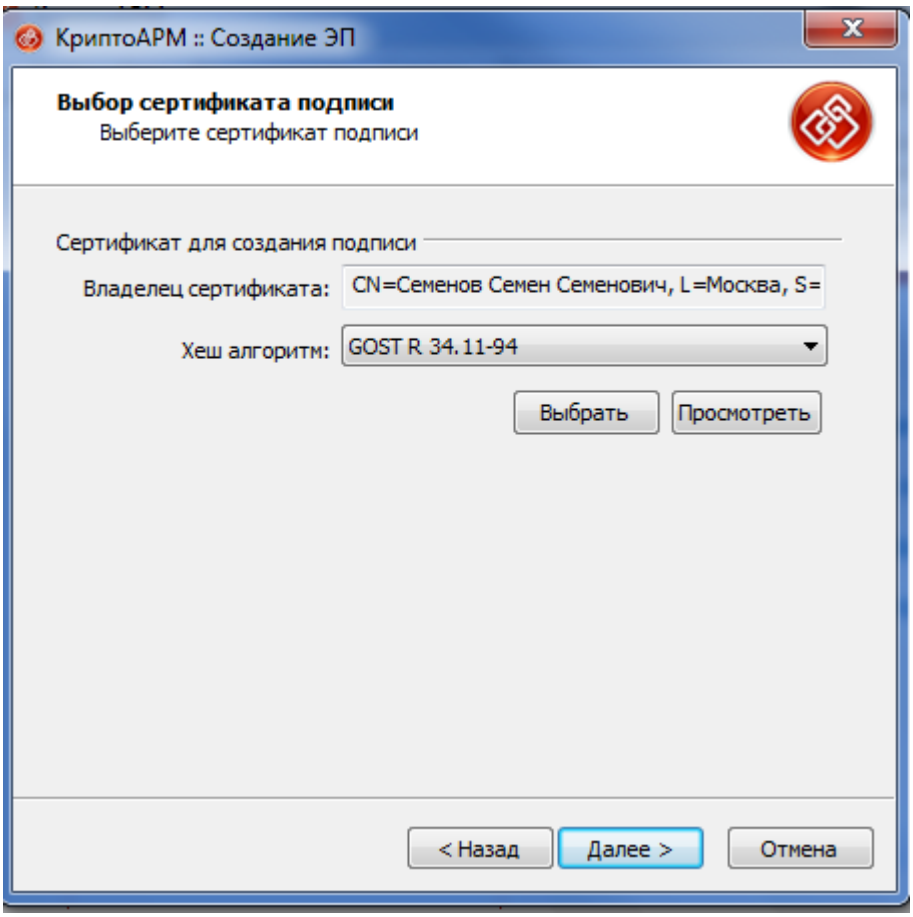

Рисунок 20.

11. После сбора данных для создания ЭП возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был подписан файл. Нажмите «Готово».

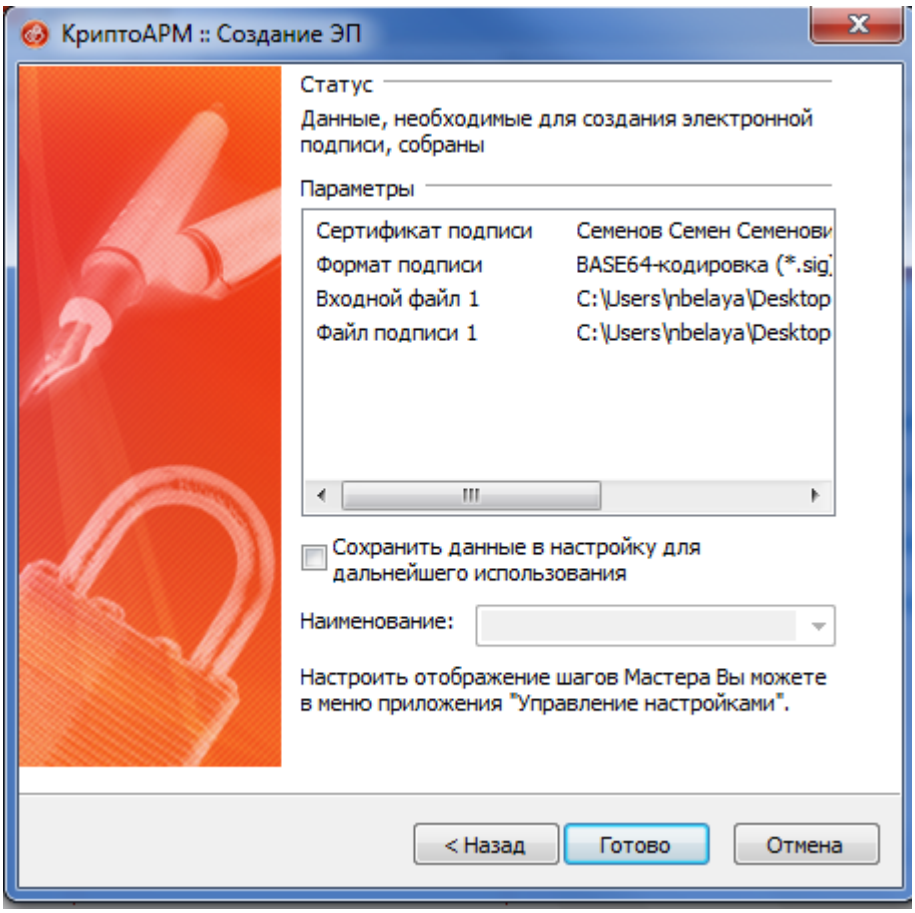

Рисунок 21.

12. Начнется процесс подписи файла. Остановить процесс можно, нажав на кнопку «Отмена».

13. Сформированный файл подписи по умолчанию будет сохранен в тот же каталог, в котором находится файл с исходными данными. Имя файла подписи совпадает с именем подписываемого файла, дополненным расширением (*.sig).

14. После завершения операции возникнет окно «Результат выполнения операции». Чтобы просмотреть детальную информацию о результатах создания подписи и используемых параметрах (имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции), нажмите кнопку «Детали>>».

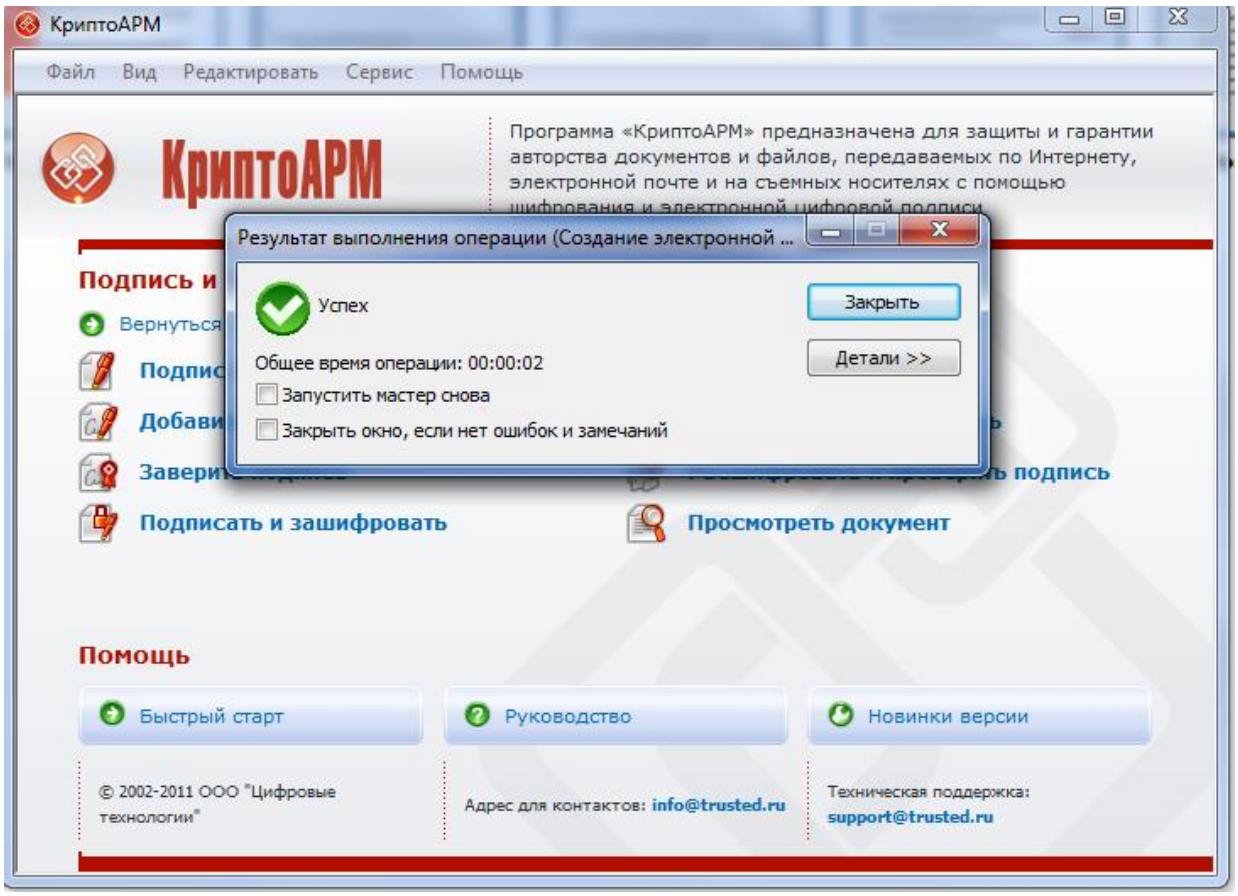

Рисунок 22.

3.1.2 Добавление дополнительной подписи

Для того чтобы добавить подпись к уже подписанному файлу:

1. В главном окне откройте раздел «Подпись».
2. Выберите пункт «Добавить подпись...».

Альтернативный вариант:

1. Нажмите правой кнопкой мыши на файле подписи, в который хотите добавить подпись.
2. Выберете «КриптоАРМ – Добавить подпись…».

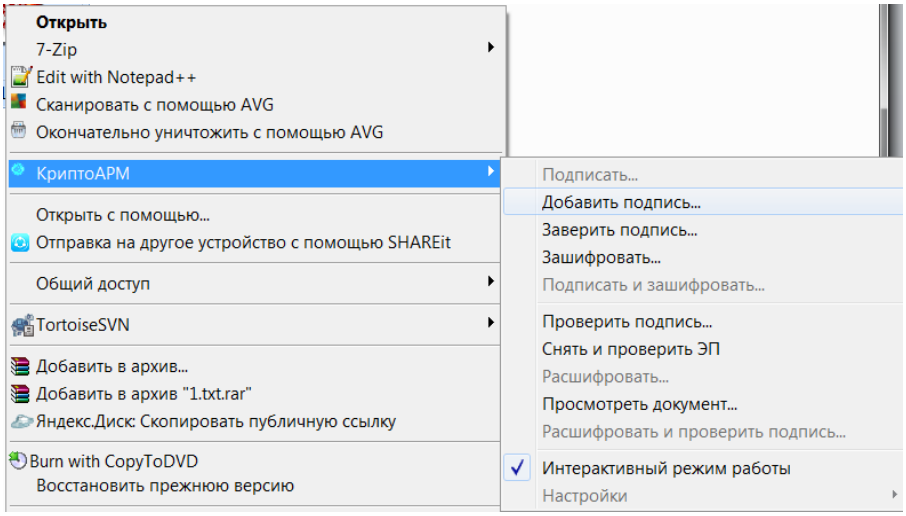

Рисунок 23.

3. Откроется «Мастер создания запроса». Ознакомьтесь с порядком и требованиями создания подписи. Нажмите кнопку «Далее».

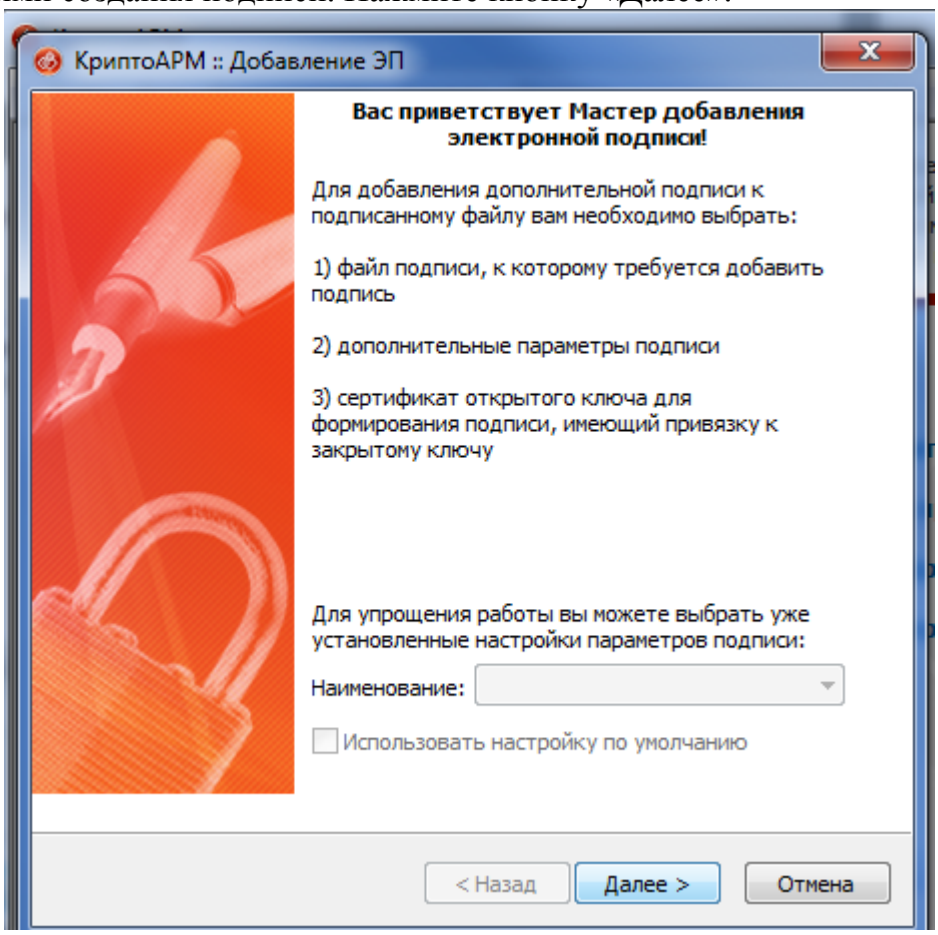

Рисунок 24.

4. Выберите папку с файлами или отдельный файл, которые необходимо подписать (при альтернативном варианте добавления подписи из проводника файл добавляется автоматически). Нажмите кнопку «Далее».

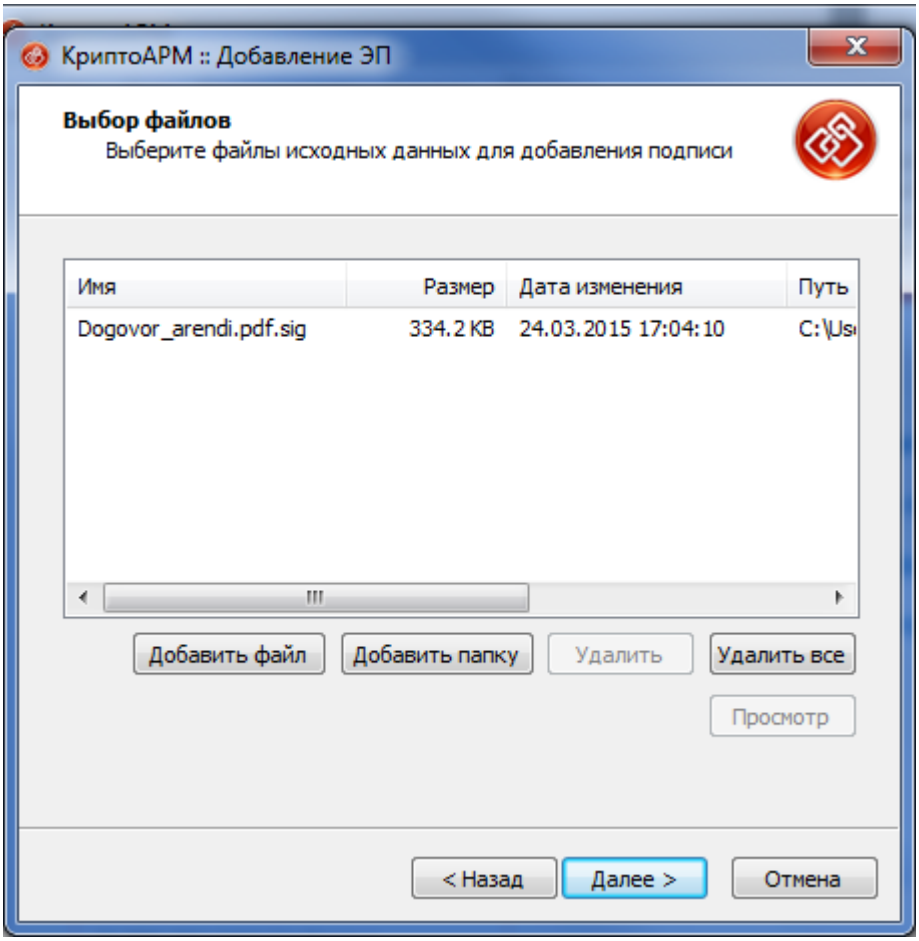

Рисунок 25.

5. Выберите сертификат для добавления подписи. Хеш алгоритм определится автоматически.
6. После сбора данных для добавления подписи возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был подписан файл. Для продолжения нажмите на кнопку «Готово».

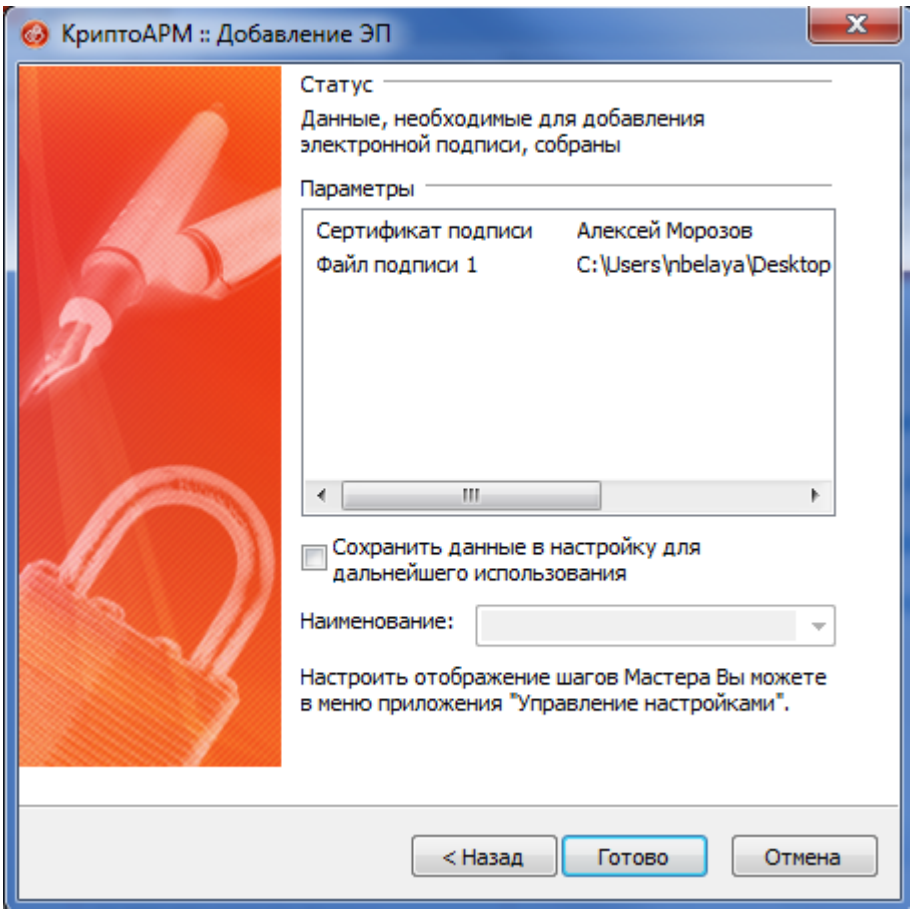

Рисунок 26.

7. Данные будут подписаны с использованием сертификата. Начнется процесс подписи файла. Вы можете прервать его, нажав на кнопку «Отмена».
8. После завершения операции возникнет окно «Результат выполнения операции». Чтобы просмотреть детальную информацию о результатах добавления подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите на кнопку «Детали >>».

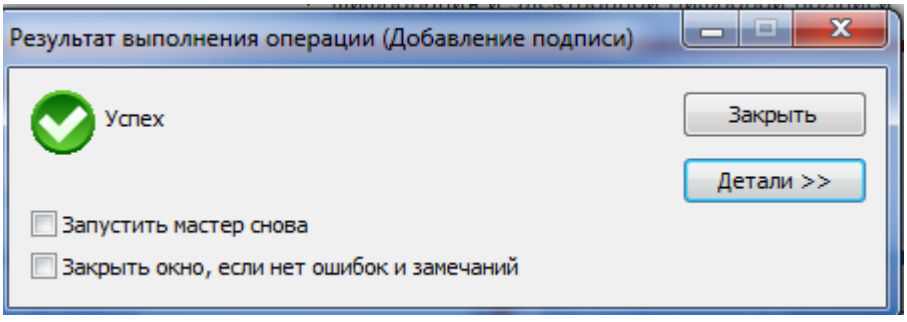

Рисунок 27.

9. Если Вы хотите просмотреть, кто еще кроме Вас поставил подпись под документом, выделите строчку с операцией и нажмите на кнопку «Менеджер сообщения».

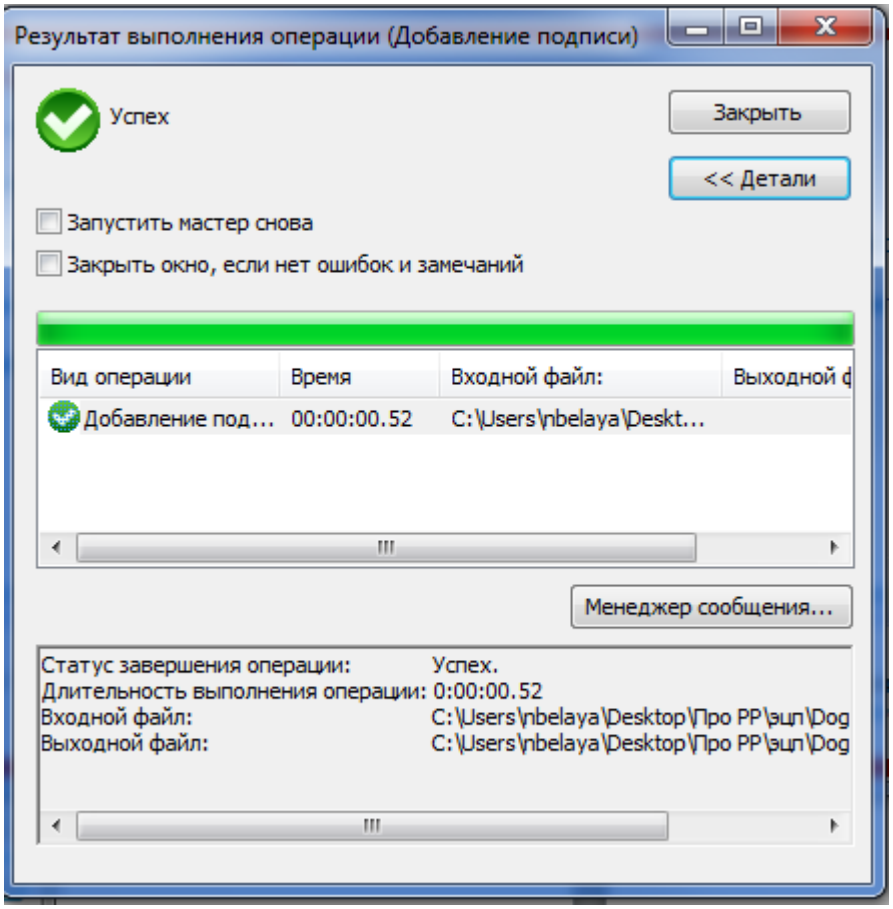

Рисунок 28.

10. Откроется окно «Управление подписанными данными», которое содержит дерево подписей.

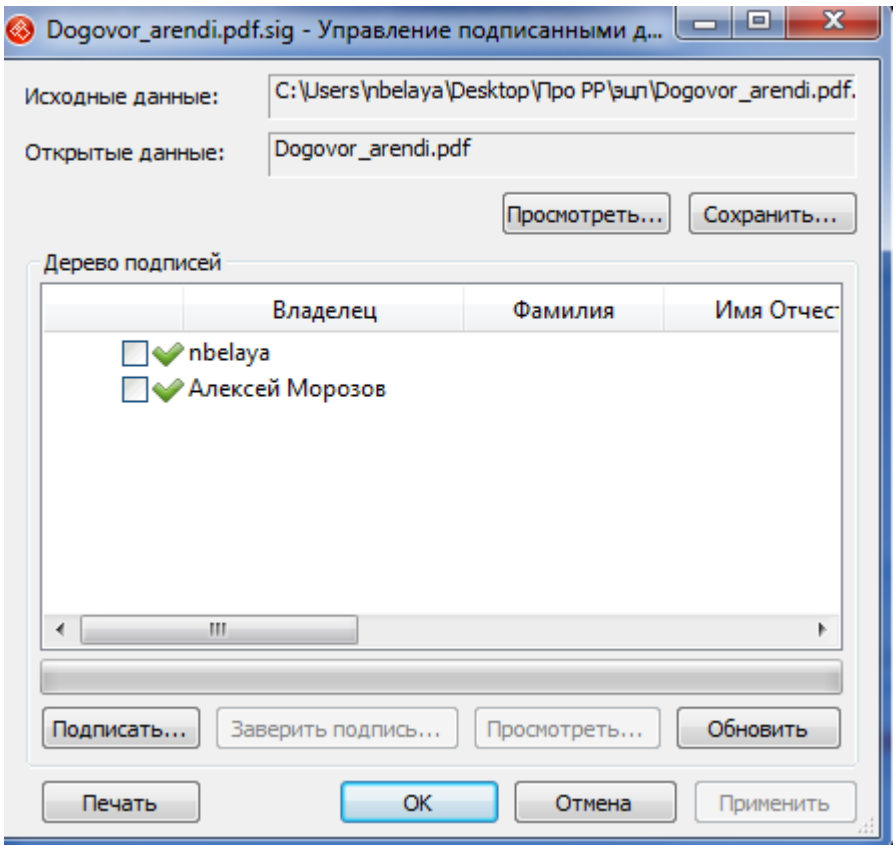

Рисунок 29.

Внимание! Не следует переименовывать файл документа и файл подписи после подписания. В противном случае ЭП будет недействительной.

11. Прикрепите файл документа и файл подписи при создании заявления на портале Росреестра

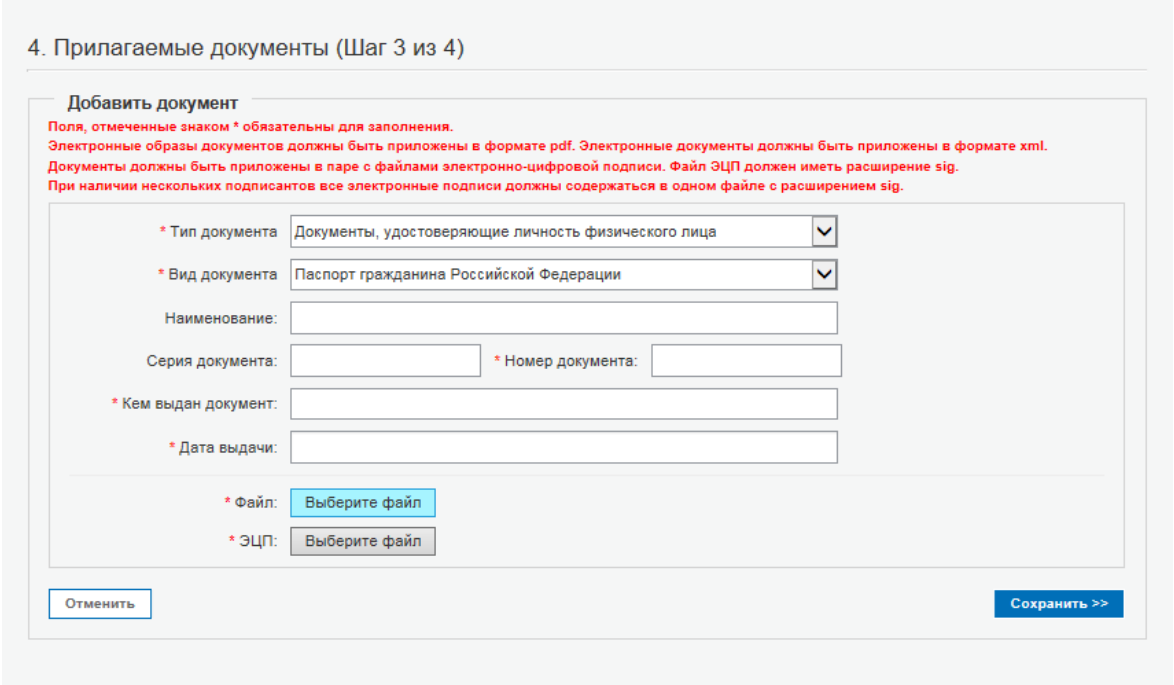

Рисунок 30.

3.1.3 Подпись при отправке заявления

1. После заполнения всех полей заявления и прикрепления подписанных документов, на шаге «Проверка введенных данных» нажмите «Подписать заявление»

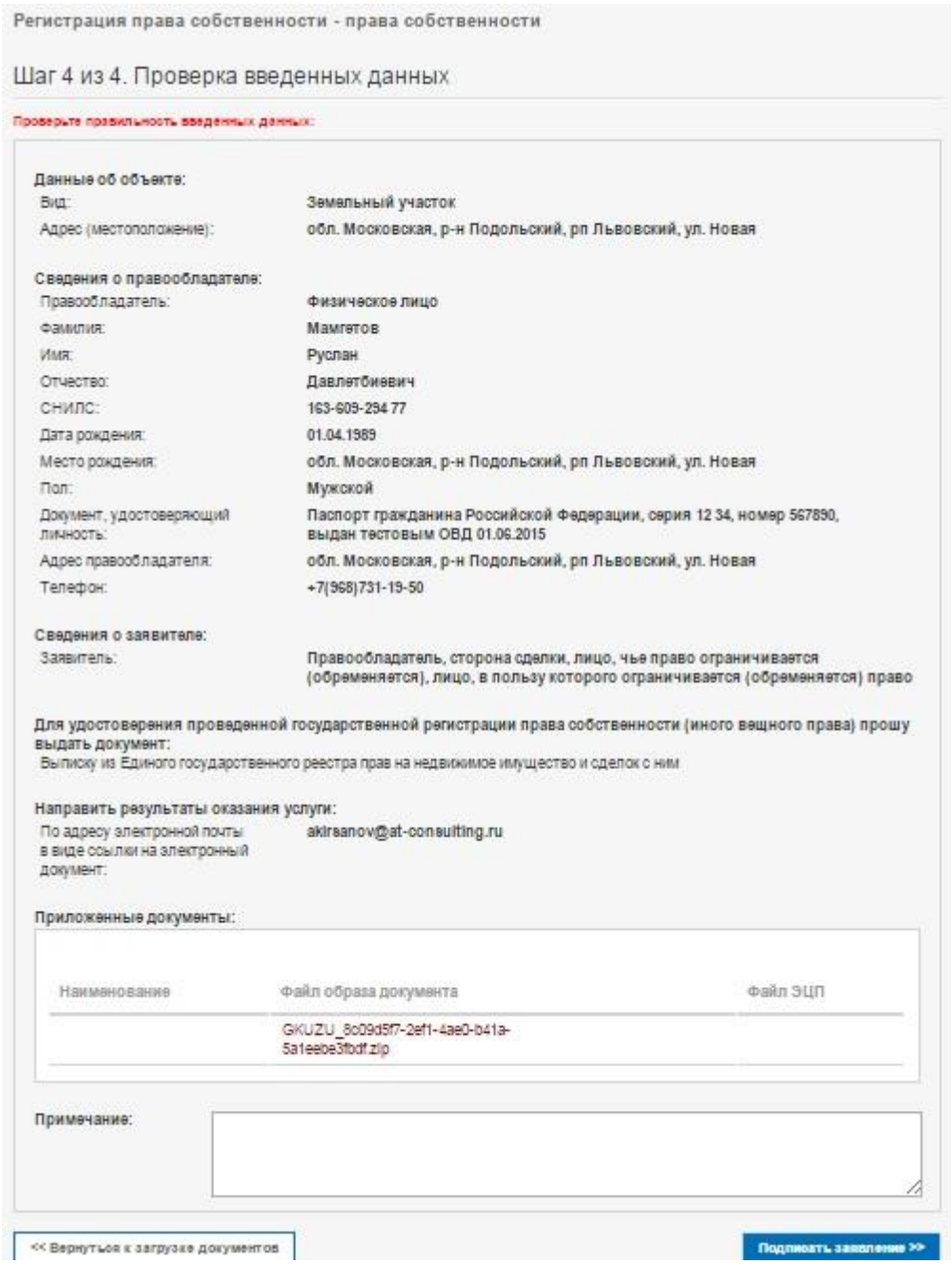

Рисунок 31.

2. Выберите необходимый сертификат

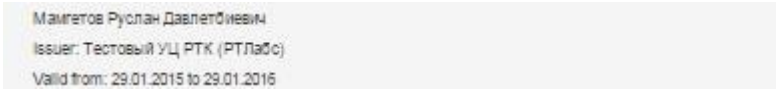

Рисунок 32.

3. Если Вы устанавливали пароль для контейнера, введите его. Нажмите «ОК»

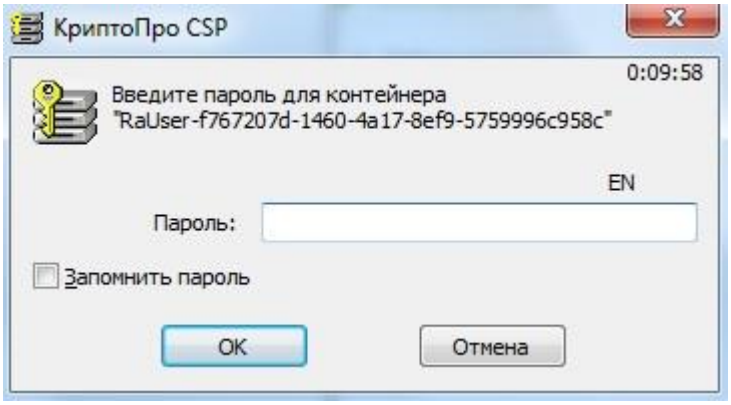

Рисунок 33.

4. Заявление успешно подписано. Нажмите «Отправить заявку».

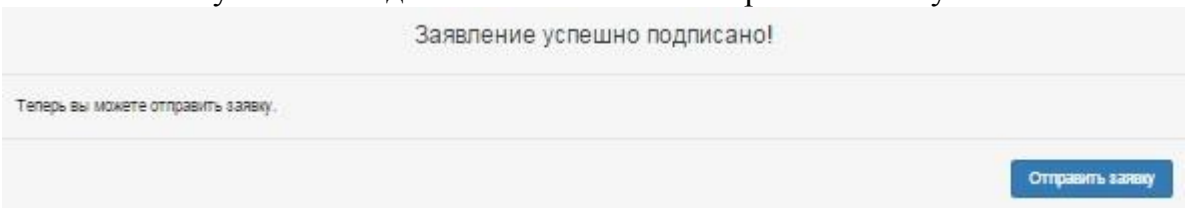

Рисунок 34.

5. Подписанное заявление отправлено на обработку.

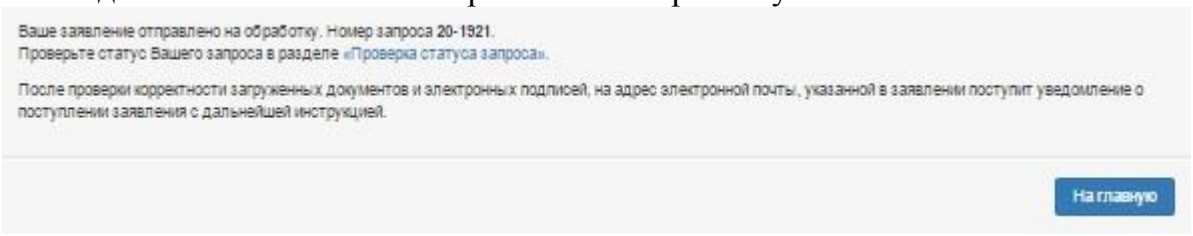

Рисунок 35.

4 ИНСТРУКЦИЯ ПО УСТАНОВКЕ КОМПОНЕНТА CAPICOM

Инструкция по установке компонента CAPICOM приводится на примере ОС Windows 7.

1. Для установки CAPICOM необходимо скачать его на сайте: http://www.microsoft.com/ru-ru/download/details.aspx?id=25281 .
2. Запустите установочный файл и следуйте указаниям инсталлятора.
3. После установки CAPICOM, по умолчанию он устанавливается в C:\Program Files\Microsoft CAPICOM 2.1.0.2 SDK\ , необходимо зарегистрировать dll библиотеку.

Для этого необходимо:

1. Перейти на компьютере в

Пуск - Панель управления - Учетные записи пользователей.

2. Выбрать:
   - Изменение параметров контроля учетной записи.
   - И выставить параметр контроля так, как показано на рис. 36.

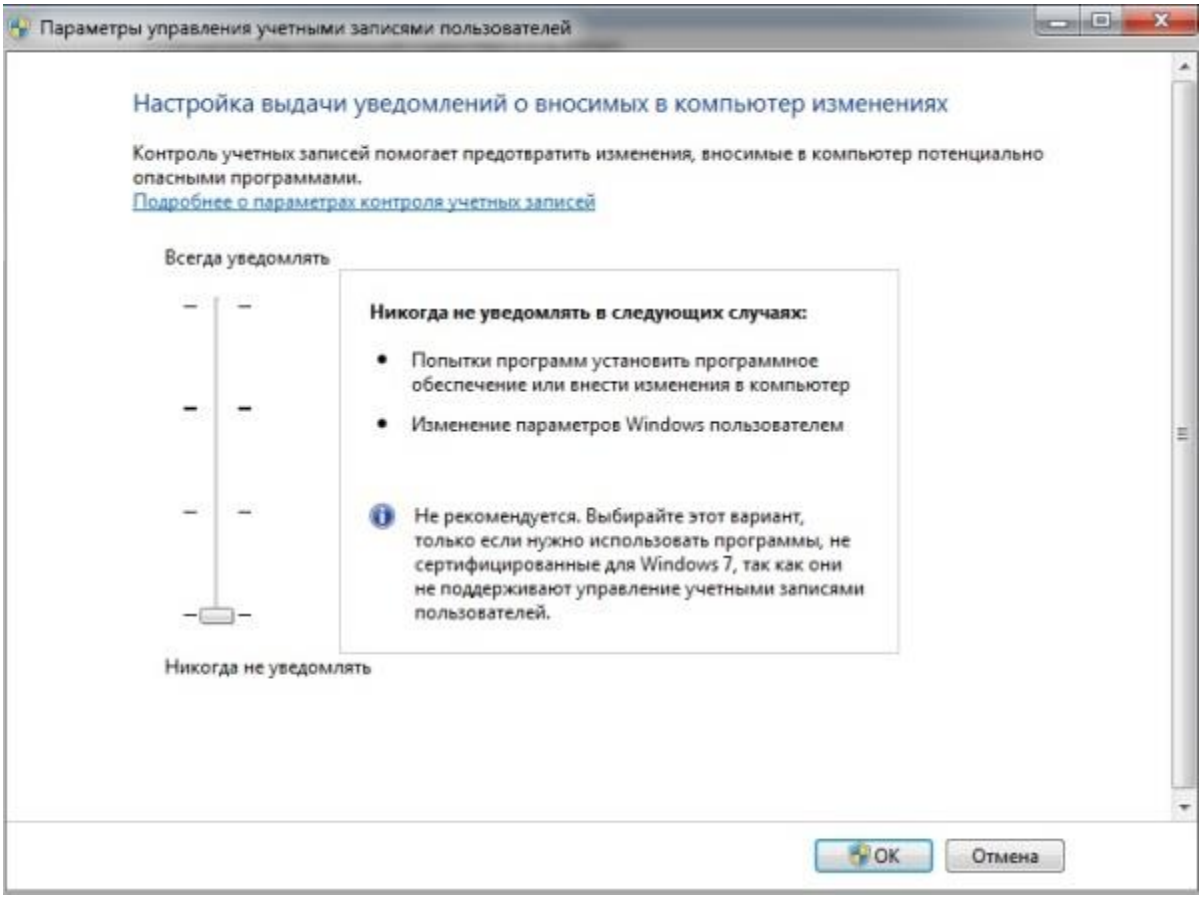

Рисунок 36

3. Перезагрузить компьютер (обязательно, иначе изменения не применятся).
4. Скопировать содержимое директории C:\Program Files\Microsoft CAPICOM 2.1.0.2 SDK\Lib\X86 (это два файла capicom.dll и capicom.pdb) в директорию C:\Windows\System32 для 32 bit систем, или для систем 64 bit в директорию C:\Windows\SysWOW64.
5. Зайти в командную строку (cmd):

   Пуск – в поле «Найти программы и файлы» ввести команду «cmd» (рис. 37).

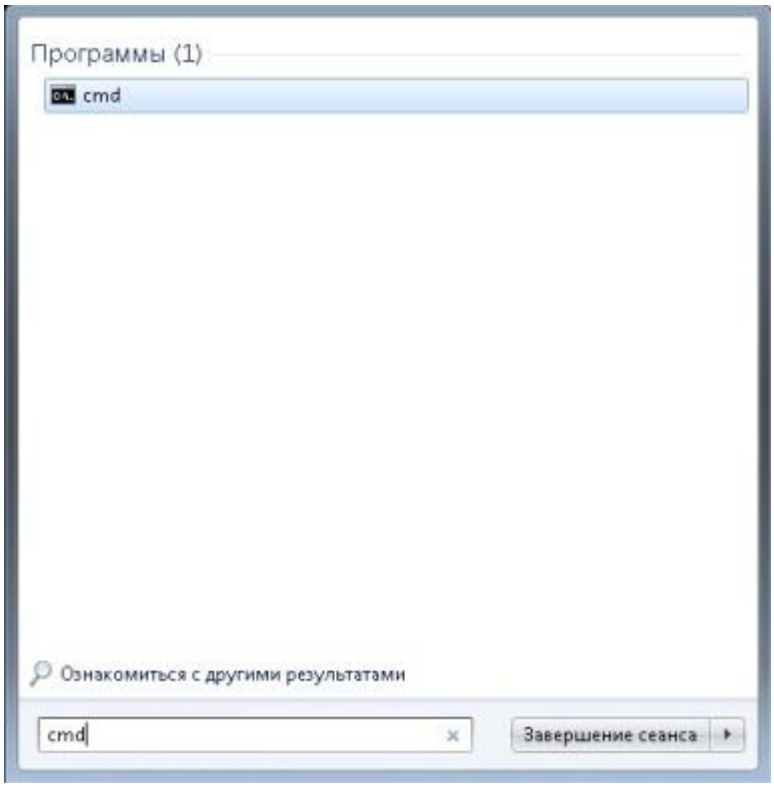

Рисунок 37

6. Выбрать из списка найденную программу.
7. Далее в командной строке ввести следующую запись:

для систем 32 bit cd C:\Windows\System32 (для систем 64 bit cd C:\Windows\SysWOW64) regsvr32.exe capicom.dll (нажать ввод).

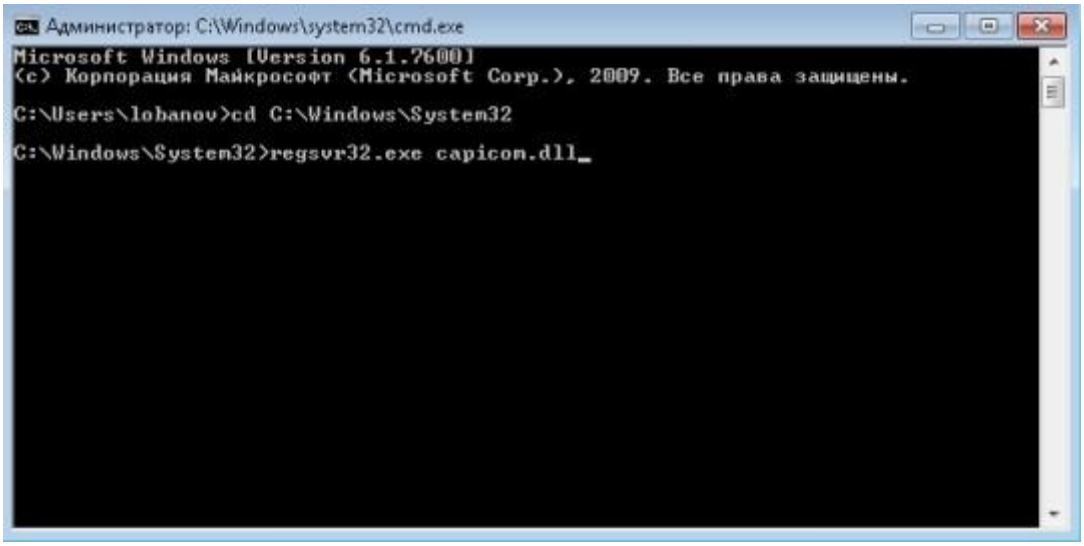

Рисунок 38

Результат выполнения должен быть следующим, рис. 39

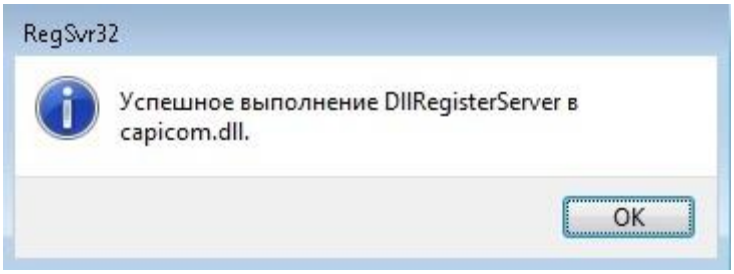

Рисунок 39

ПРИЛОЖЕНИЕ А

ВОЗМОЖНЫЕ ПРОБЛЕМЫ ПРИ ПОДПИСАНИИ И СПОСОБЫ ИХ РЕШЕНИЯ

1. ПРОБЛЕМЫ С ПОДПИСАНИЕМ ЗАЯВЛЕНИЙ В GOOGLE CHROME, ЯНДЕКСБРАУЗЕР, OPERA.

1.1. Не происходит выбора сертификата и операции подписания.

Описание проблемы:

- не выходит окно выбора сертификата;
- не происходит операции подписания с выводом сообщения об успешном подписании;

Причина:

Проблема 1:

Существующий Плагин «КриптоПро Браузер плагин» разрабатывался компанией КриптоПро на основе уже устаревшей системы NPAPI, с помощью которой в браузер встраиваются плагины. В Chrome ver.42 отключена технология NPAPI. Это также затрагивает браузеры: Crome, ЯндексБраузер, Opera, базирующиеся на Chromium.

Варианты решения:

1. Рекомендуется использовать другие браузеры, такие как Internet Explorer Firefox, Safari до момента доработки «КриптоПро Браузер плагин» до поддержки PPAPI.
2. Чтобы пользователи КриптоПро смогли заранее подготовиться к смене технологии, КриптоПро выпустили предварительную версию КриптоПро ЭЦП Browser plug-in, которая работает без NPAPI.

http://www.cryptopro.ru/news/2015/03/novaya-versiya-kriptopro-etsp-browser-plug.

3. Возможно временно активировать плагины NPAPI в Chrome версий от 42 – 44. Для этого в настройках браузера необходимо выполнить действия, описанные по ссылке: https://support.google.com/chrome/known-issues/15036?hl=ru.

Этот способ будет доступен до выхода Chrome ver.45 в 2015 году.

1.2. Сертификат не найден в хранилище

Описание проблемы:

После выбора сертификата для подписи выходит окно с надписью «Сертификат не найден в хранилище».

Причина:

На локальном месте пользователя произведена некорректная установка сертификата ЭП.

Варианты решения:

1. На компьютере пользователя должен быть установлен только один криптопровайдер. Использование разных криптопровайдеров на одном рабочем месте приводит к конфликту механизмов шифрования. Рекомендуется установить криптопровайдер КриптоПро CSP.
2. Сертификат должен быть установлен для Пользователя, а не для локального компьютера. Необходимо проверить, не добавлен ли Ваш личный сертификат в хранилище сертификатов для локального компьютера, в противном случае его необходимо удалить. Личный сертификат должен храниться только в "Сертификаты - текущий пользователь -> Личное -> Реестр -> Сертификаты". Также проверьте хранилища "Другие пользователи" для локального компьютера и текущего пользователя. Личного сертификата там также быть не должно, если он есть, его необходимо удалить.
3. Проверить, установлены ли корневые сертификаты издателя. Если в цепочке сертификации не указан корневой сертификат издателя или у Вас возникают трудности с его получением, то Вам необходимо обратиться в Удостоверяющий центр, где была приобретена электронная подпись.

2. ПРОБЛЕМЫ С ПОДПИСАНИЕМ ЗАЯВЛЕНИЙ В INTERNET EXPLORER

Описание проблемы:

Не выходит окно выбора сертификата; не происходит операции подписания с выводом сообщения об успешном подписании.

Причина:

Для сервиса Государственной регистрации права - Неправильно установлен сертификат на рабочем месте пользователя.

Варианты решения:

Заново переустановить сертификат в хранилище.

3. ПРОЧИЕ ПРОБЛЕМЫ, СВЯЗАННЫЕ С ПОДПИСАНИЕМ

Описание проблемы:

При попытке подписания выходит сообщение о том, что произошла технологическая ошибка.

Причина:

1. Просрочен сертификат, которым осуществляется попытка подписания.
2. Фильтрация ActiveX в Internet Explorer, которая запрещает сайтам устанавливать и использовать такие приложения, как «КриптоПро плагин». Это повышает безопасность работы в Интернете, но может отразиться на работе некоторых сайтов. Например, если включена фильтрация ActiveX, могут не работать некоторые видео, игры и другое интерактивное содержимое.

Варианты решения:

1. Приобрести действующий сертификат.
2. Отключить фильтрацию ActiveX в браузере согласно инструкции: http://windows.microsoft.com/ru-ru/internet-explorer/use-activex-filtering#ie=ie-11.