Lot-online

Всероссийская универсальная торговая площадка для продажи государственного и частного имущества

РУКОВОДСТВО ПО УСТАНОВКЕ И НАСТРОЙКЕ СРЕДСТВ ЭЛЕКТРОННОЙ ПОДПИСИ

Санкт-Петербург

2013 год

СОДЕРЖАНИЕ

1. Введение

Для того чтобы обеспечить возможность подписывать документы Электронной Цифровой Подписью (ЭП), необходимо выполнить следующую последовательность шагов:

- установить на Ваш компьютер криптографическое Программное Обеспечение (ПО);
- подключить полученный в Удостоверяющем центре брелок секретным ключом;
- загрузить в хранилище сертификатов личный сертификат, сертификаты Удостоверяющего центра и сертификаты Ваших доверенных лиц;
- установить дополнительное программное обеспечение для работы ЭП.

Все эти действия подробно описаны далее и не вызовут трудностей у пользователя при внимательном и последовательном выполнении требований настоящей инструкции.

Область применения

Данное руководство помогает пользователю системы настроить свой персональный компьютер на работу с электронной цифровой подписью при использовании ОС Windows XP/Vista/7. Для применения средств электронной цифровой подписи установите необходимое программное обеспечение, а также настройте компоненты системы согласно приведенным ниже инструкциям.

Уровень подготовки пользователя

Пользователь сайта должен обладать следующей квалификацией:

- Пользовательские навыки в работе с ПЭВМ;
- Пользовательские навыки работы с WWW–браузером Microsoft Internet Explorer;
- Базовые навыки по установке программного обеспечения для операционной системы Windows.

Перечень эксплуатационной документации, с которой необходимо ознакомиться пользователю

До начала работы пользователь должен ознакомиться с документами:

- Операционная система Windows. Руководство пользователя.

Обратите внимание, что список корневых сертификатов и удостоверяющих центров, авторизованных площадкой, расположен на странице http://lot-online.ru/static/ecp_list.html.

2. Инструкция пользователя по установке поддержки ЭП

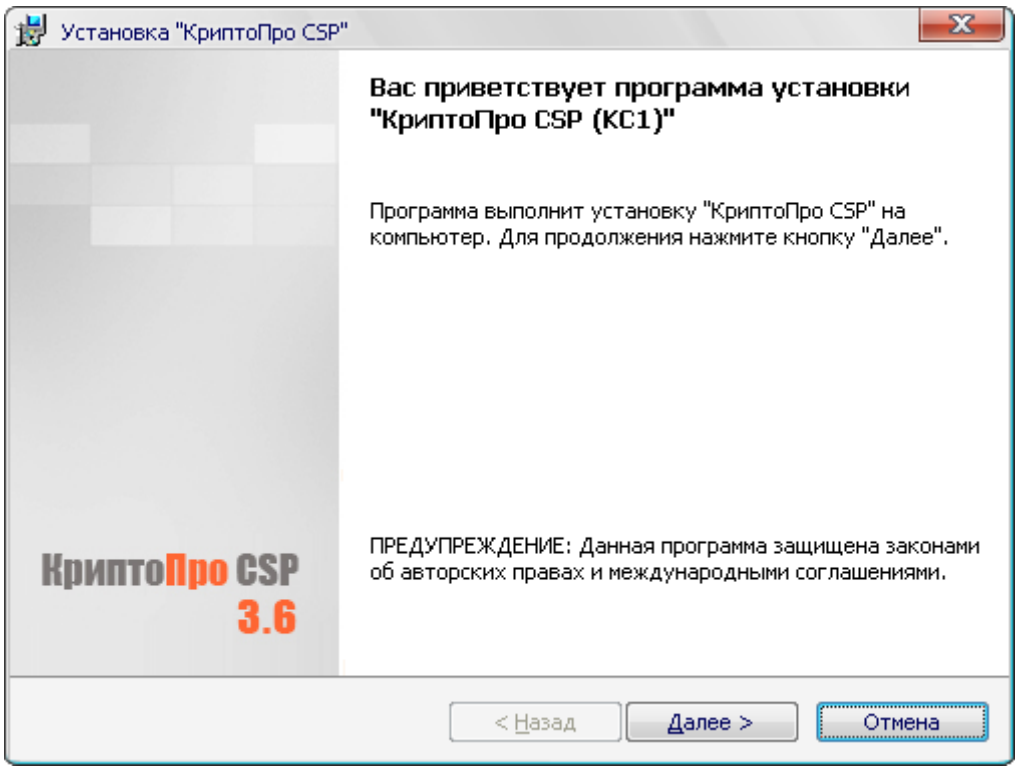
2.1. Установка и настройка «КриптоПро CSP»

Для применения средств ЭП при работе в системе Вам необходимо приобрести программное обеспечение «КриптоПро CSP» для ОС Windows (для Windows XP допустима установка как версии 3.0, так и версии 3.6, для Windows Vista/Windows 7 допустима только версия 3.6) согласно регламенту получения средств ЭП, опубликованному на сайте.

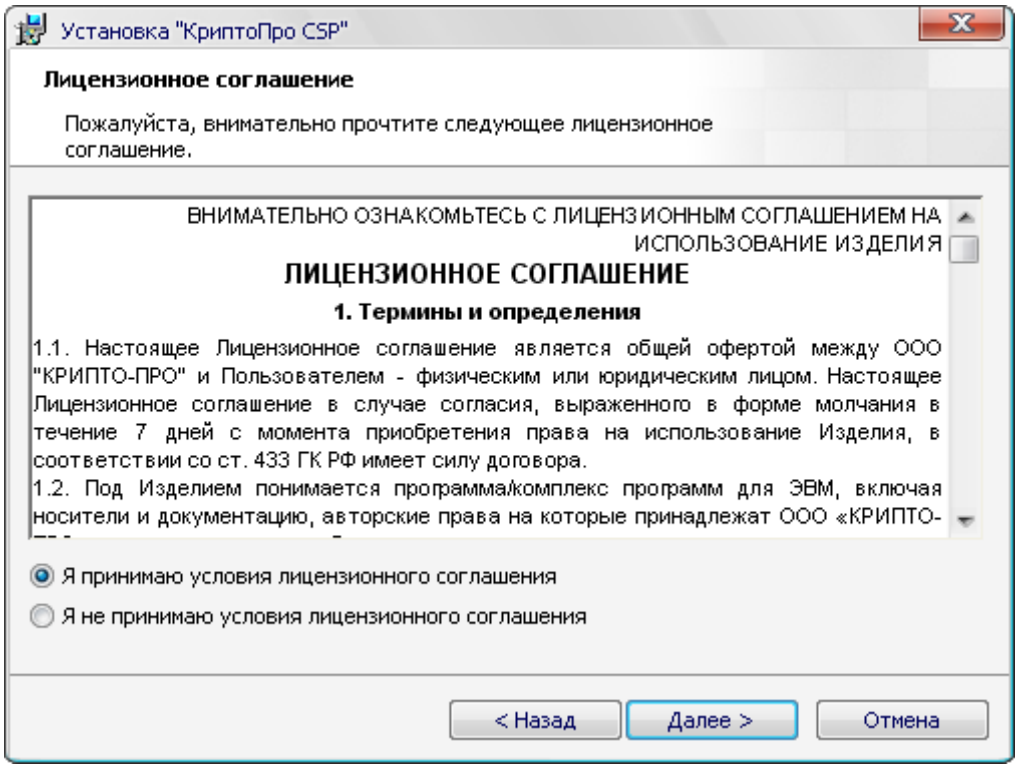
Для установки и настройки «КриптоПро CSP» Вы можете воспользоваться документацией по установке «КриптоПро CSP», размещенной на сайте производителя, либо выполнить перечисленные здесь действия.

Установка и настройка «КриптоПро CSP» версии 3.6

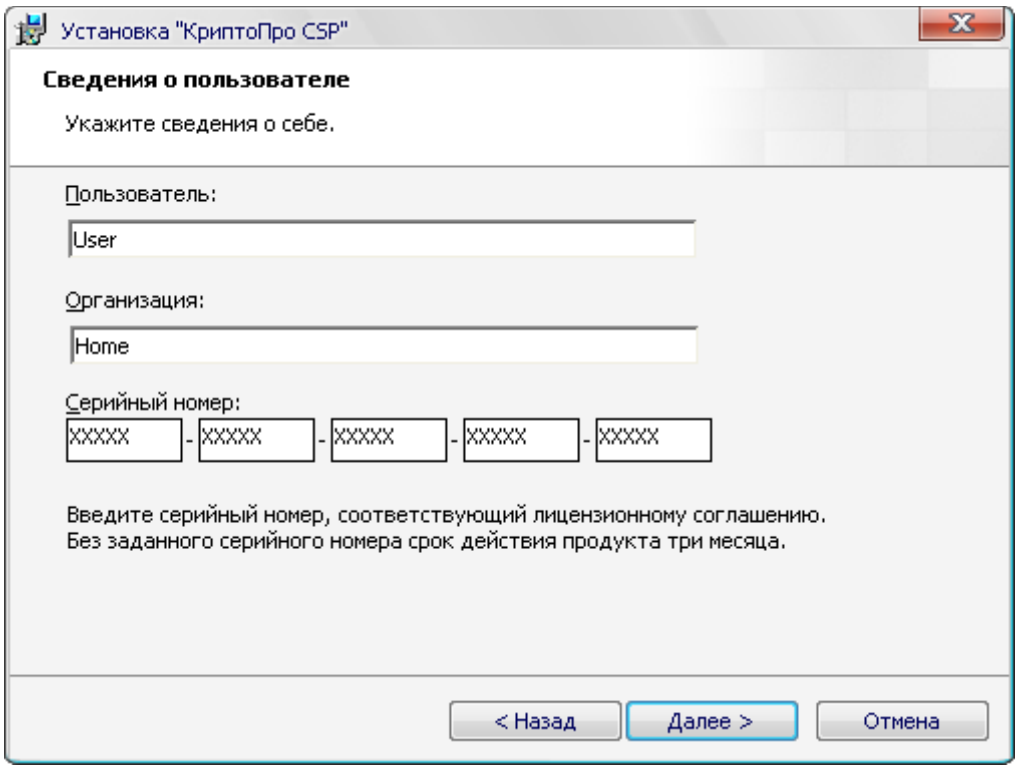
2.1.1) Запустите скачанный EXE-файл (csp-win32-kc1-rus.EXE), появится следующее окно, в котором нажмите кнопку «Далее»:



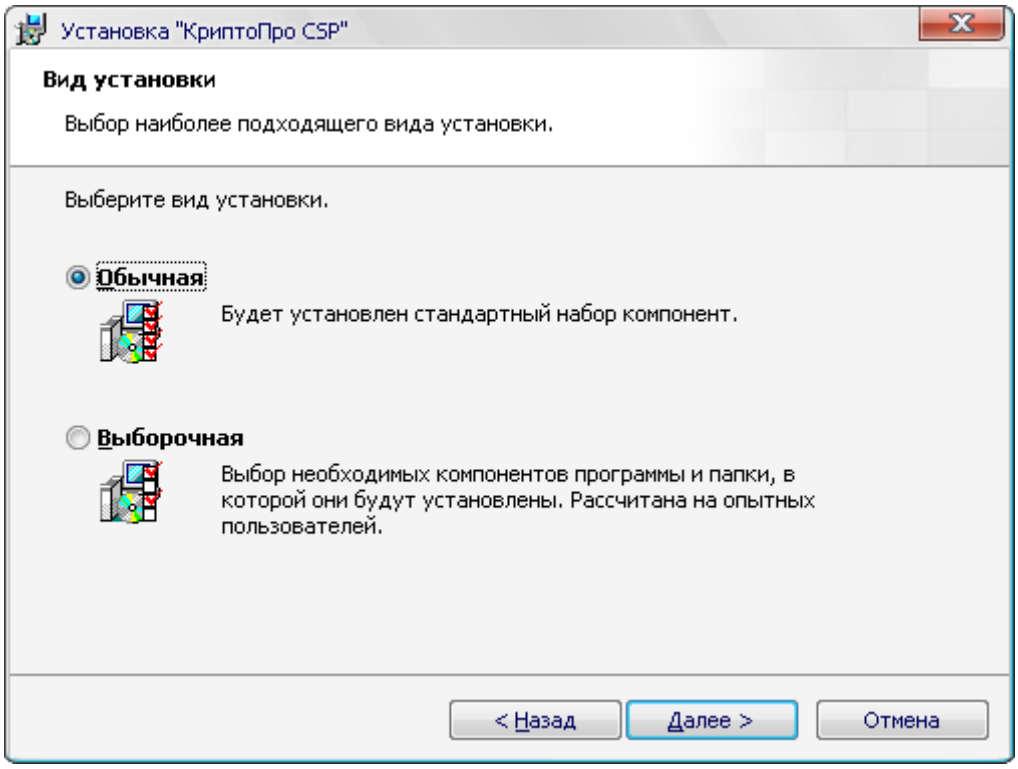
2.1.2) Появится следующее окно, в котором необходимо прочитать Лицензионное соглашение и после этого выбрать пункт «Я принимаю условия лицензионного соглашения», а затем нажать кнопку «Далее»:



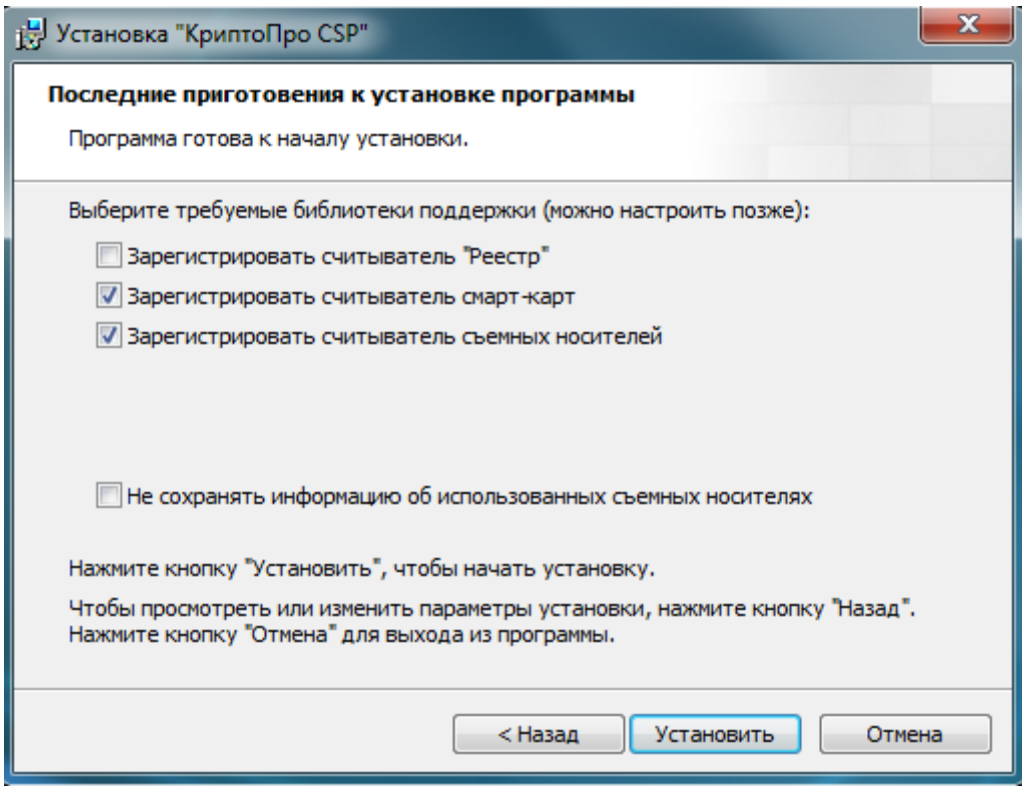
2.1.3) В следующем окне введите информацию о пользователе, организации и серийный номер (если вы купили «КриптоПро CSP»), затем нажмите кнопку «Далее»



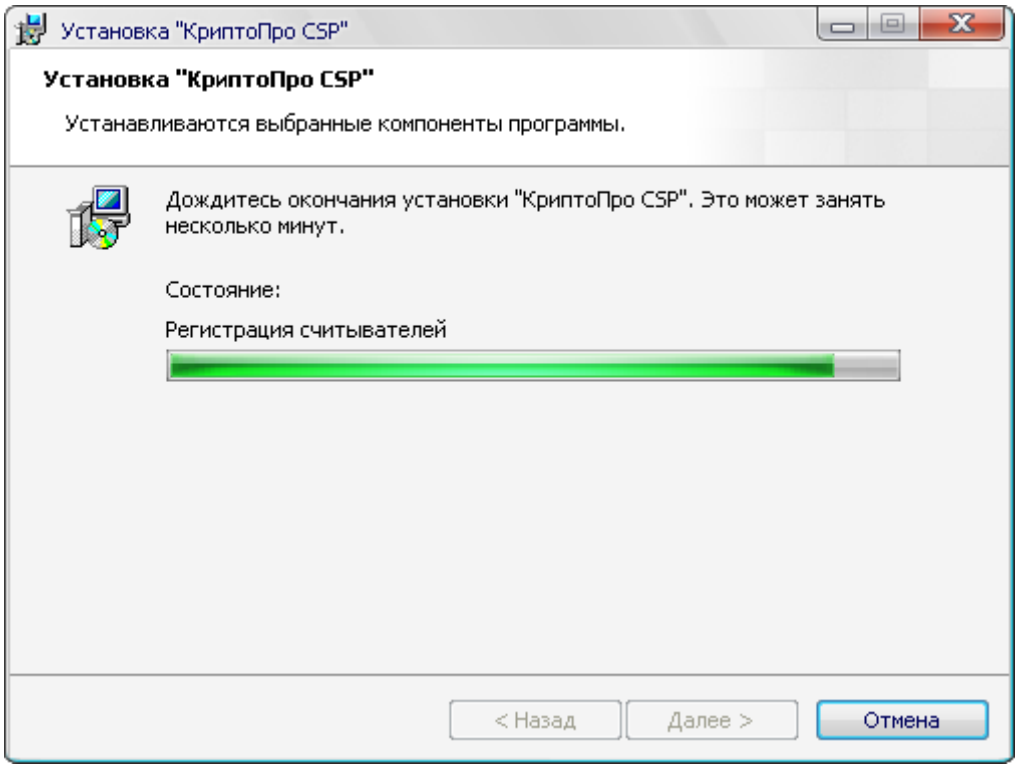
2.1.4) В следующем окне выберите пункт «Обычная» и нажмите кнопку «Далее»



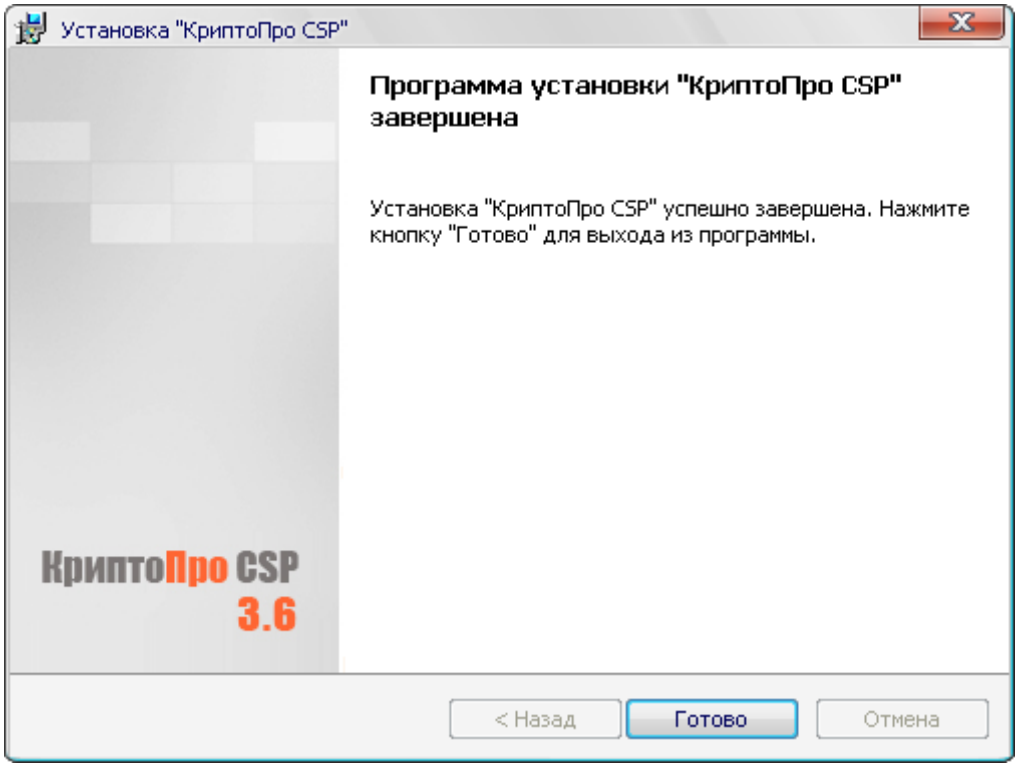
2.1.5) В следующем окне выбрать пункты «Зарегистрировать считыватель смарт-карт» и «Зарегистрировать считыватель съемных носителей» и нажать «Установить»



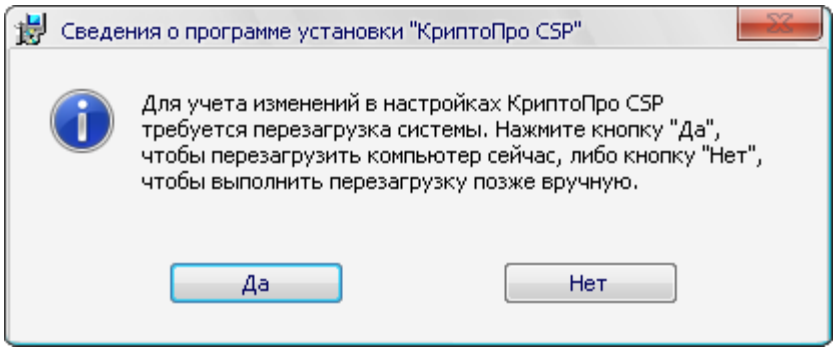
2.1.6) Начнется установка «КриптоПро CSP» (как показано на рисунке). Дождитесь окончания установки.



2.1.7) После окончания установки появится следующее окно, в котором нажмите кнопку «Готово»



2.1.8) После этого появится окно с запросом перезагрузки компьютера, нажмите «Да»



После перезагрузки компьютера, установка «КриптоПро CSP» будет завершена.

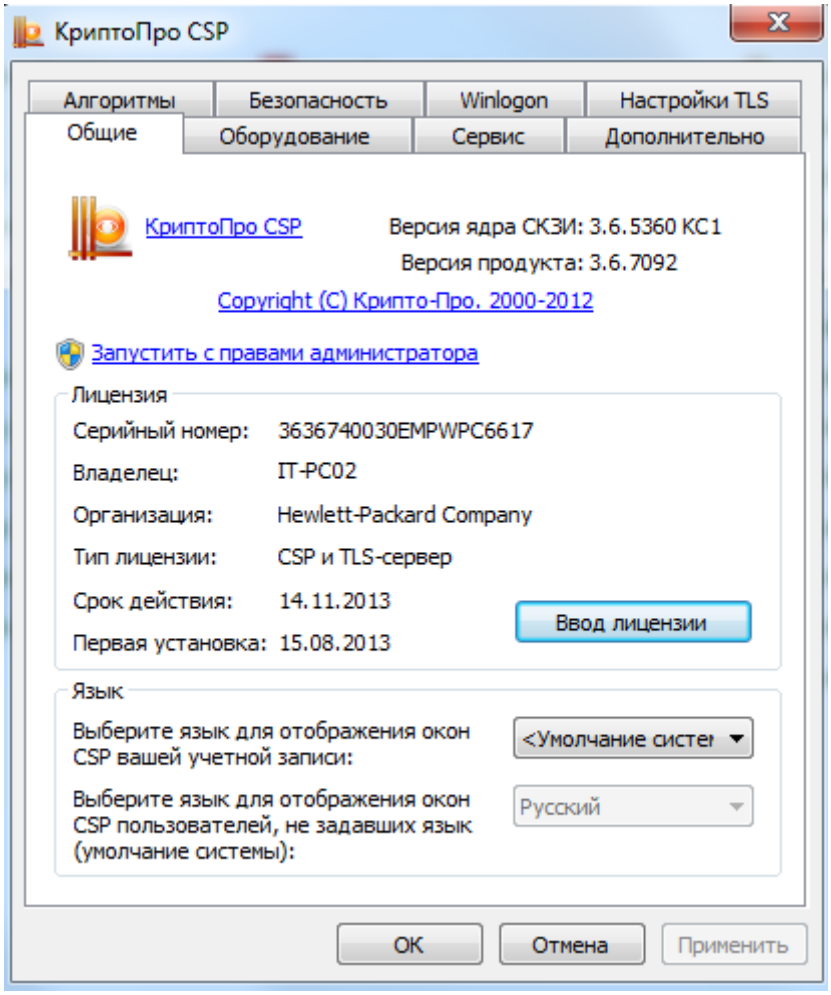
2.2. Порядок ввода лицензии в КриптоПро 3.6

В этой главе описываются шаги по вводу лицензии для криптографической программы КриптоПро CSP.

При установке программного обеспечения КриптоПро CSP без ввода лицензии, пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер с бланка Лицензии (поставляется отдельно на бумажном носителе формата А4).

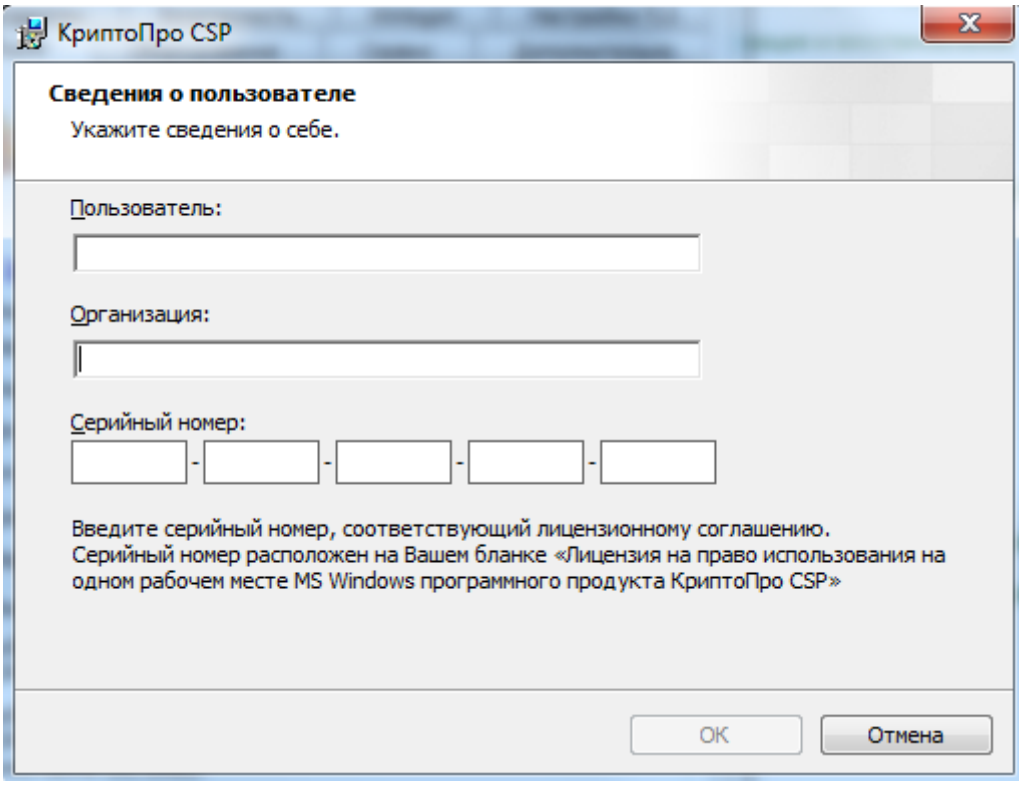
2.2.1) Выберите пункт меню Пуск - Настройка - Панель управления - КриптоПро CSP.

2.2.2) В окне Свойства КриптоПро CSP на вкладке «Общие» нажмите на кнопку «Ввод лицензии».



2.2.3) В открывшемся окне КриптоПро CSP заполните поля «Пользователь» и

«Организация», а также введите серийный номер КриптоПро (указан в лицензии) и нажмите кнопку ОК.



3. Установка драйверов ключевых носителей под ОС Microsoft Windows 7/ 2008/ Vista/ 2003/ XP/ 2000.

3.1. Установка драйверов Rutoken под ОС Microsoft Windows.

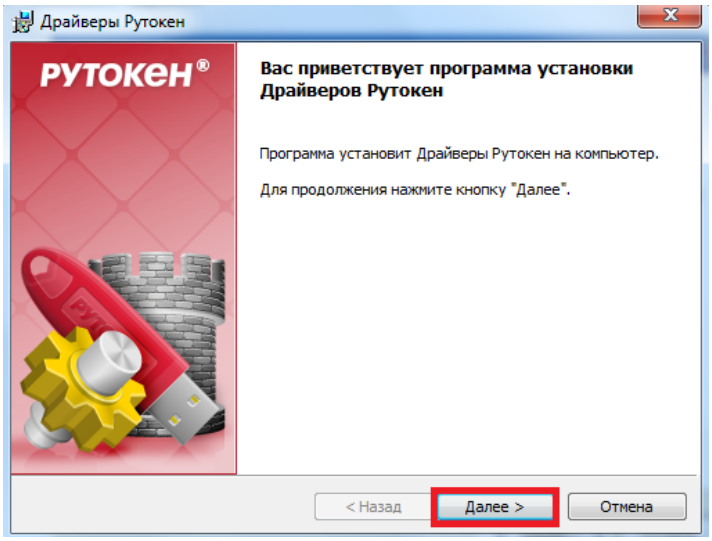
В этой главе описываются шаги по установке драйверов для ключевых носителей Rutoken.
Rutoken - один из видов ключевых носителей (токен), персональное средство аутентификации, которое при использовании вставляется в USB-порт.
Для того чтобы данные носители работали с СКЗИ, необходимо после их установки отдельно устанавливать драйвера Rutoken, которые необходимы для полноценной работы электронных идентификаторов, сервисных утилит, а также любых решений на основе Rutoken.
Электронный идентификатор - персональное средство аутентификации и защищенного хранения пользовательских данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронно-цифровой подписью (ЭП)

Важная информация:

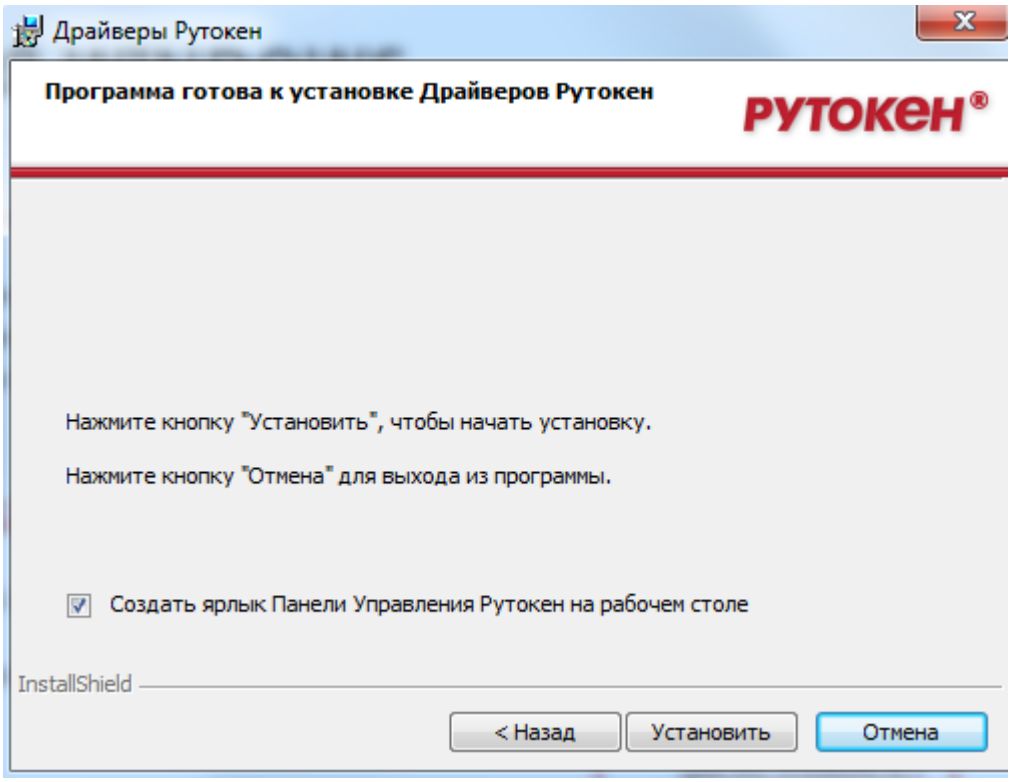
Для установки драйверов Rutoken под Операционные Системы Microsoft Windows 7/2008/Vista/2003/XP/2000 различной разрядности используйте:
http://www.rutoken.ru/support/download/drivers-for-windows/

Перед началом установки драйверов рекомендуется закрыть все работающие приложения. Для установки драйверов необходимы права администратора системы. Перед началом установки драйверов рекомендуется отсоединить идентификатор Rutoken от USB - порта компьютера.

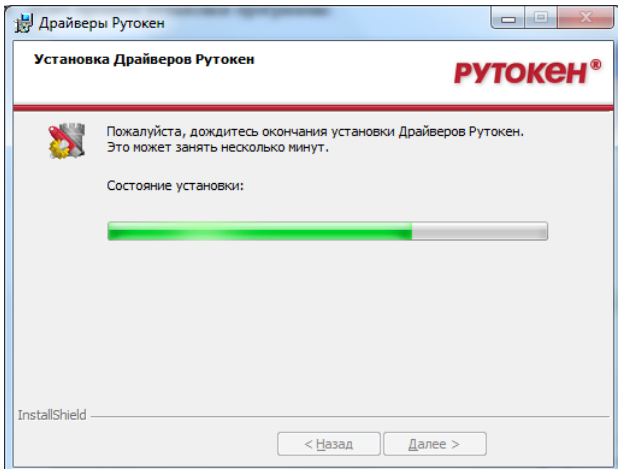
3.1.1) Запустите программу установки драйверов Rutoken и следуйте ее указаниям. На представленных ниже рисунках показаны основные этапы работы мастера установки.
Нажмите кнопку "Далее".



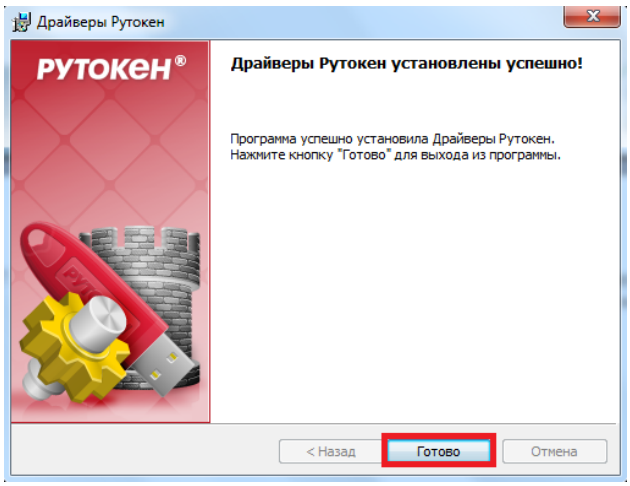
3.1.2) Нажмите на кнопку "Установить".



3.1.3) После этого начнется процесс установки программы.

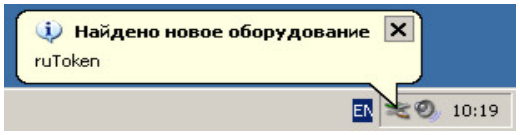


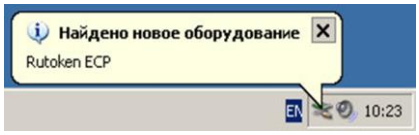
3.1.4) Установка драйвера на ruToken завершена. Нажмите кнопку "Готово".

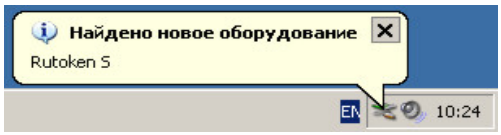


Во время установки драйверов, возможно, потребуется перезагрузка компьютера – выполните это требование.

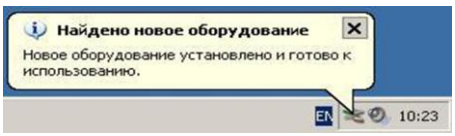
3.1.5) После окончания установки драйверов подсоедините идентификатор Rutoken к USB-порту компьютера. В области уведомлений Панели задач появятся сообщения, свидетельствующие об обнаружении системой подключенного электронного ключа Rutoken (в зависимости от модели подключаемого токена):







и сообщение о готовности Rutoken к использованию:



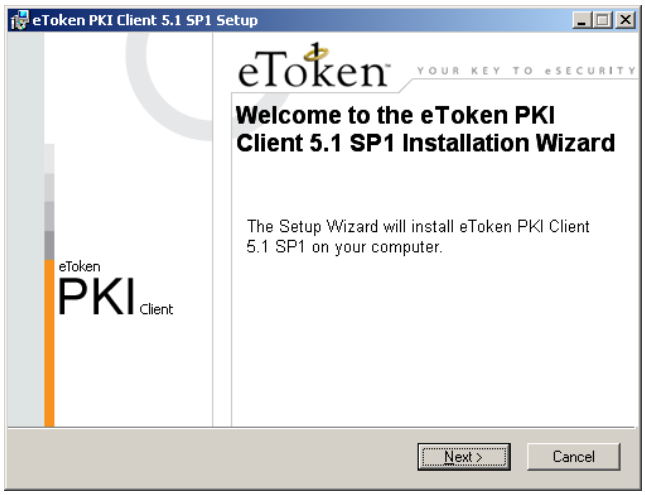
3.2. Инструкция по установке драйвера eToken.

eToken – один из видов ключевых носителей (токен), персональное средство аутентификации, которое при использовании вставляется в USB-порт. Для того, чтобы данные носители работали с СКЗИ, необходимо после их установки отдельно устанавливать драйвера eToken, необходимые для полноценной работы электронных идентификаторов, сервисных утилит, а также любых решений на основе eToken.

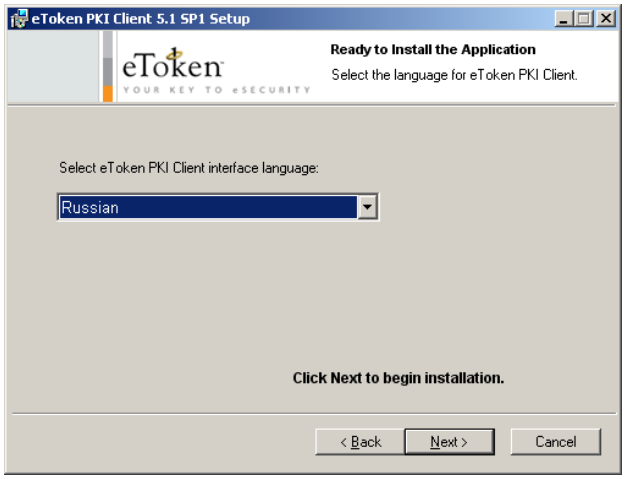
Электронный идентификатор - персональное средство аутентификации и защищенного хранения пользовательских данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронно-цифровой подписью (ЭП)

Новые версии драйверов eToken доступны по адресу: http://www.aladdin-rd.ru/support/downloads/etoken/

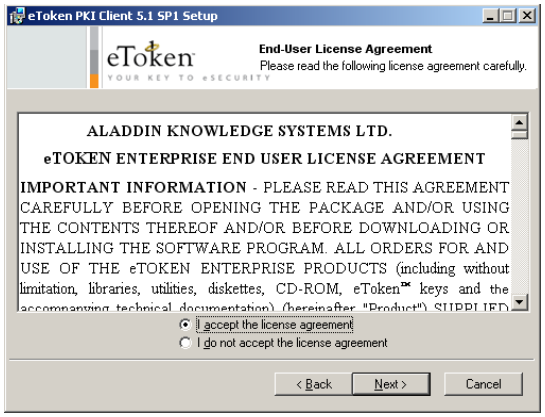
3.2.1) Скачайте и распакуйте файл eToken PKI Client 5.1 SP1 для Microsoft Windows. Войдите в архив, выберите установочный файл, соответствующий установленной на Вашем компьютере операционной системе, и запустите установку, дважды щёлкнув мышью по файлу PKIClient-x32-5.1-SP1.msi или PKIClient-x64-5.1-SP1.msi. Начнётся процесс установки.



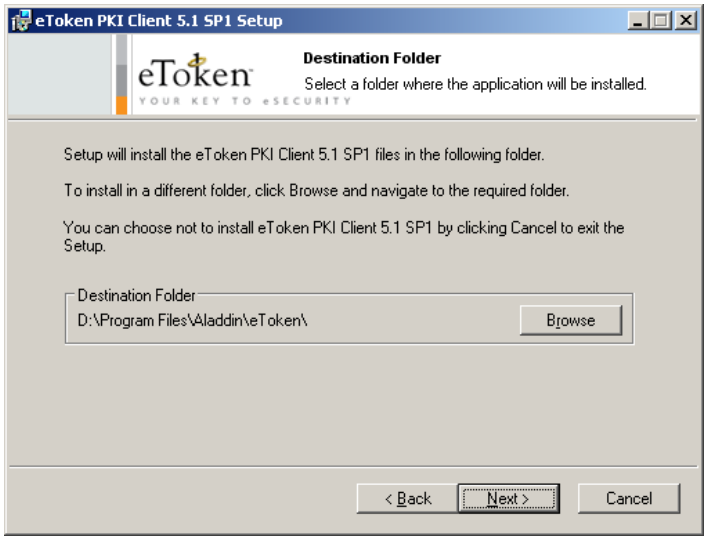
3.2.2) Выберите язык интерфейса пользователя.

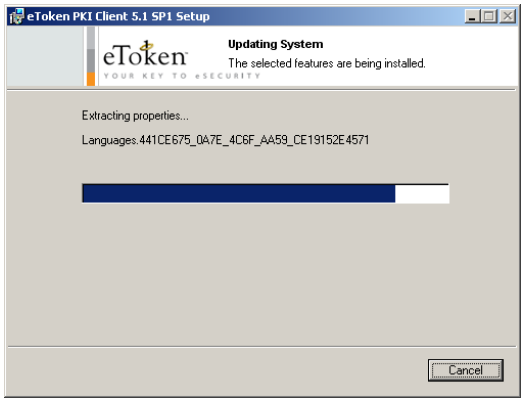


3.2.3) Ознакомьтесь с лицензионным соглашением и подтвердите свое согласие принять его условия, выбрав "I accept the license agreement".

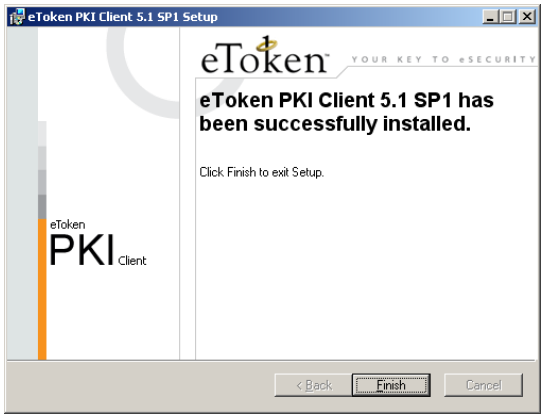


3.2.4) При необходимости Вы можете изменить путь установки программы.





3.2.5) После этого начнется процесс установки программы.



3.2.6) Во время установки программы могут появляться сообщения о необходимости закрыть программы, в которые интегрируется PKI Client - выполните эти указания.

В некоторых случаях программа установки может предложить перезагрузить компьютер.

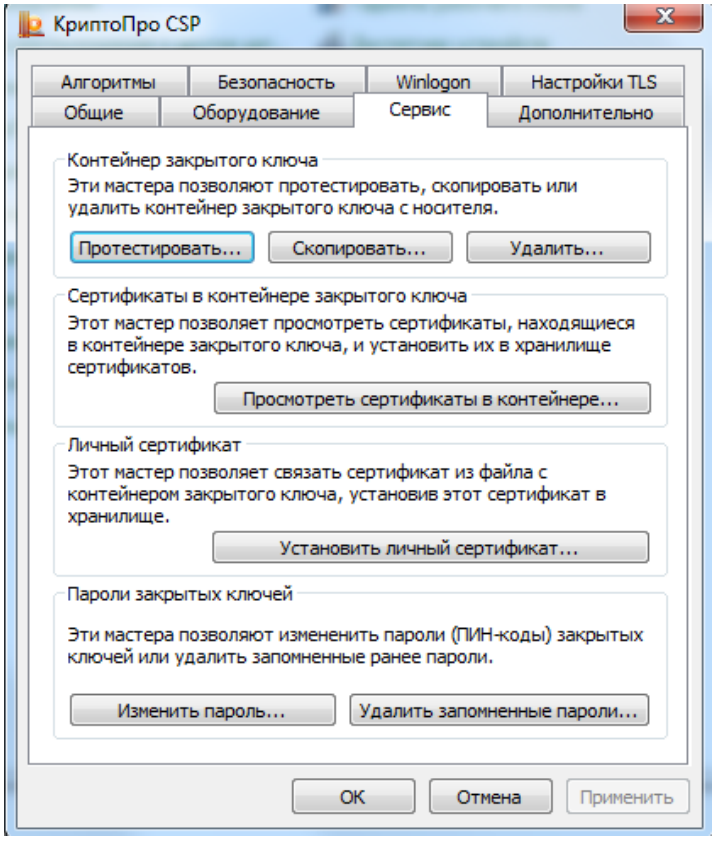
4. Установка личного сертификата пользователя

В этой главе описано, как установить личный сертификат на Ваш компьютер. После установки личного сертификата криптографическое программное обеспечение получает необходимые данные в электронном виде, которые используются при создании ЭП. Без наличия этих данных, невозможно будет подписывать никакие документы Вашей личной Электронной Цифровой Подписью.

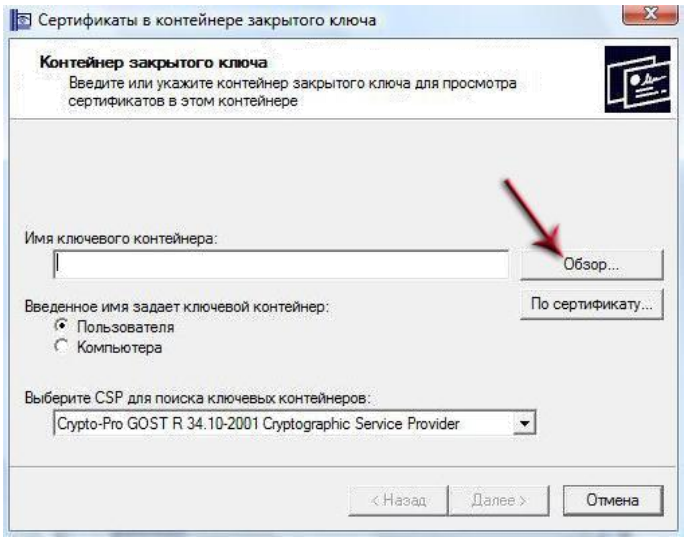
Предполагается, что программное обеспечение (ПО) средства криптографической защиты информации (СКЗИ) уже установлено на Вашем компьютере с диска, полученного Вами в Удостоверяющем центре.

Для установки личного сертификата необходимо иметь полученный в Удостоверяющем центре ключевой носитель, выполненный в виде брелока и подключаемый к разъему USB, т.к. при установке личного сертификата выполняется привязка открытого ключа (размещен в сертификате) к секретному ключу, (размещен на Вашем ключевом носителе).

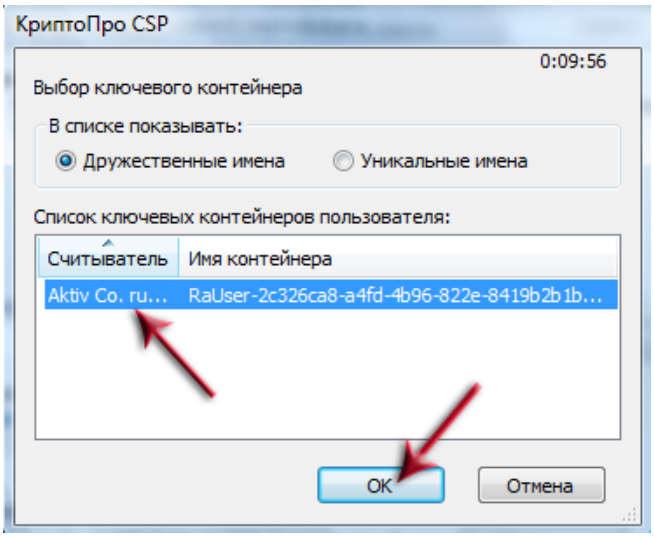
4.1) Процесс установки личного сертификата пользователя выглядит следующим образом: Выберите пункт меню Пуск – Программы – КриптоПро - КриптоПро CSP.



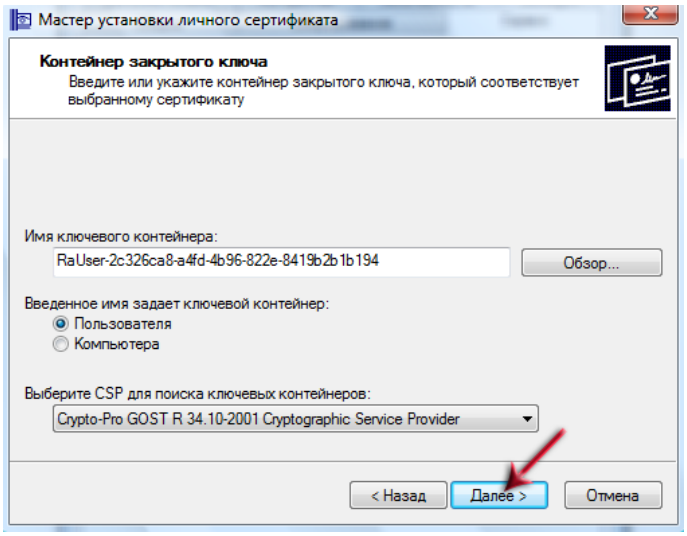
4.2) В окне свойств “КриптоПро CSP” перейдите на вкладку “Сервис” и нажмите кнопку “Просмотреть сертификаты в контейнере”.



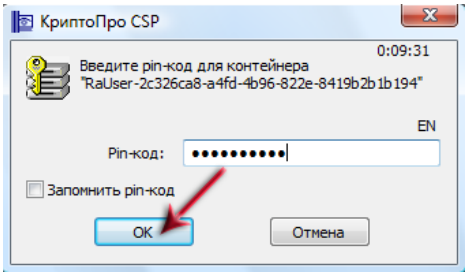
4.3) В окне “Сертификаты в контейнере закрытого ключа” выберите “Обзор”.



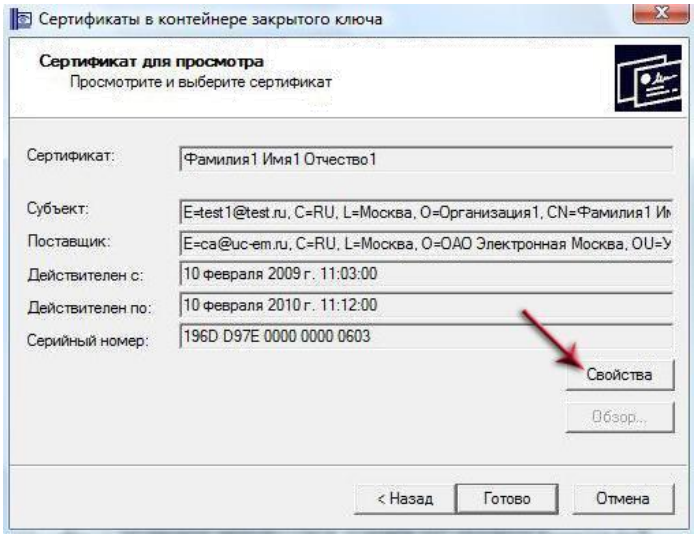
4.4) Выберите идентификатор из списка (в большинстве случаев в списке будет присутствовать один ключевой контейнер) и нажмите “OK”.



Нажмите кнопку “Далее”.

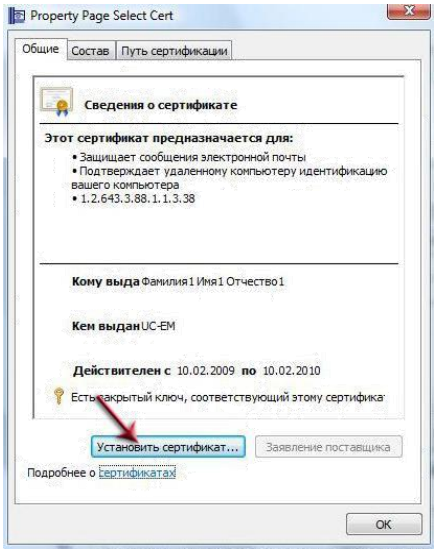


4.5) Введите *pin-код* ключа, не ставьте флажок возле надписи “Запомнить пароль”. Нажмите кнопку “OK”.

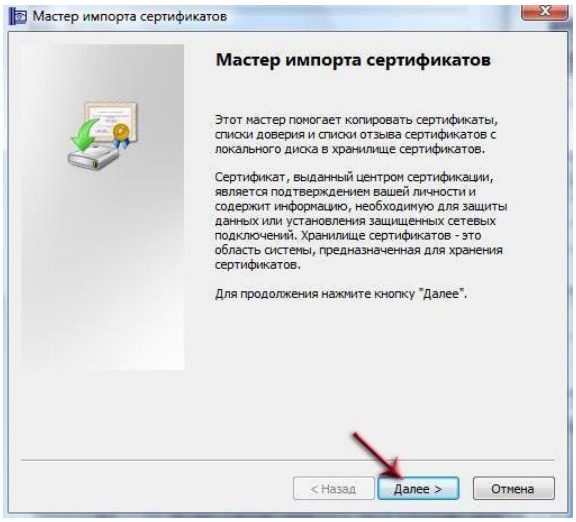


Если *pin-код* введен правильно, то появится окно с информацией о сертификате.

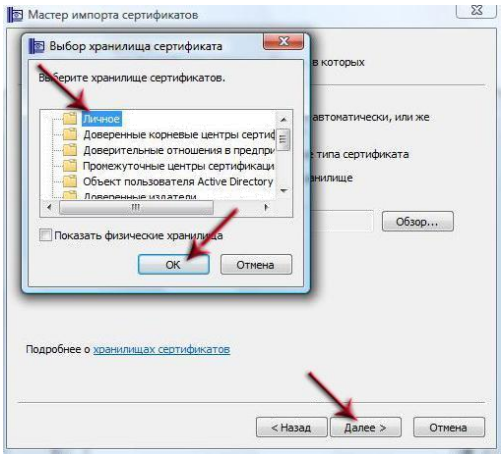
4.6) В открывшемся окне нажмите кнопку “Свойства”. В окне свойств сертификата на вкладке “Общие” нажмите кнопку «Установить сертификат…».



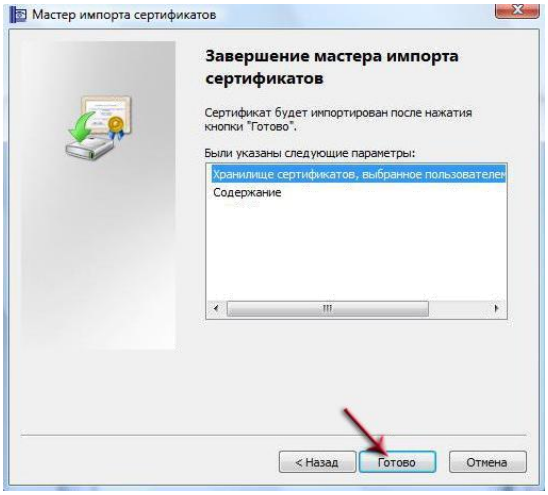
Запустится мастер импорта сертификатов. В окне “Мастера импорта сертификатов” нажмите кнопку “Далее”.



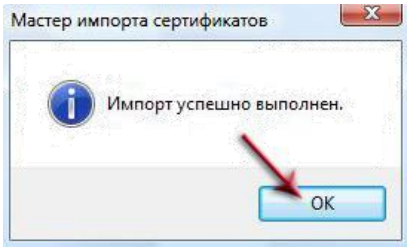
4.7) Переставьте флаг в состояние “Поместить все сертификаты в следующее хранилище”. Нажмите “Обзор”, в списке хранилищ выберите “Личное” и нажмите “ОК”, а потом “Далее ”.



4.8) Нажмите кнопку “Готово”.



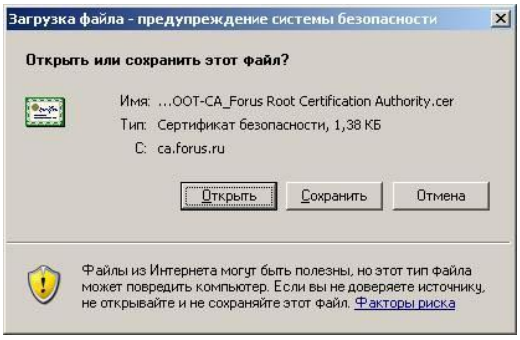
4.9) Вы получите сообщение о том, что импорт сертификата успешно завершен.



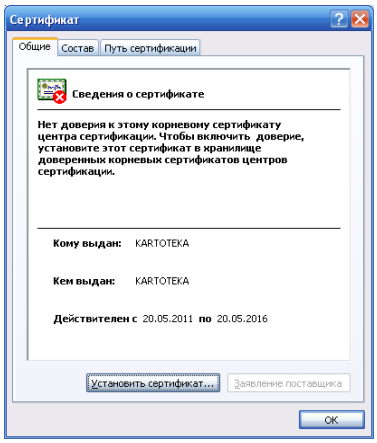
5. Инструкция по установке корневого сертификата

В этой части инструкции описаны шаги по установке сертификатов на Ваш компьютер. Без наличия на компьютере сертификатов Удостоверяющего центра программное обеспечение не сможет подтвердить достоверность Электронной Цифровой Подписи, и Вы не сможете подписывать никакие документы.
Предполагается, что программное обеспечение (ПО) средства криптографической защиты информации (СКЗИ) уже установлено на Вашем компьютере с диска, полученного Вами в Удостоверяющем центре.

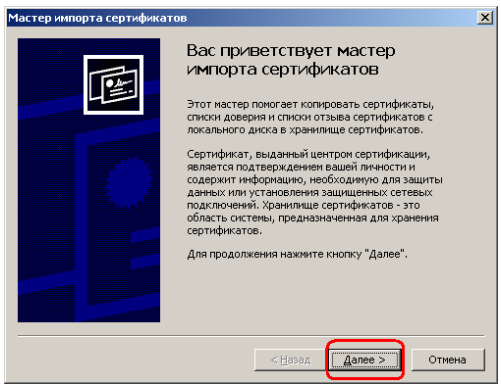
5.1) Исходя из того каким удостоверяющим центром была выдана ваша электронная подпись, вы можете найти корневые сертификаты на официальном сайте вашего удостоверяющего центра.
5.2) Для того, чтобы скачать сертификаты, нужно нажать дважды на изображении сертификата, после чего отобразится предупреждение системы безопасности, в окне которого нужно выбрать «Открыть».



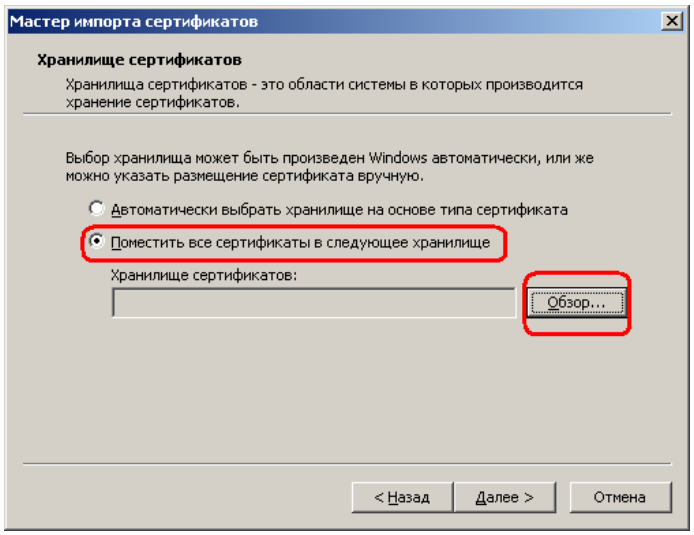
5.3) Нажмите кнопку "Установить Сертификат". Запустится "Мастер импорта сертификатов".



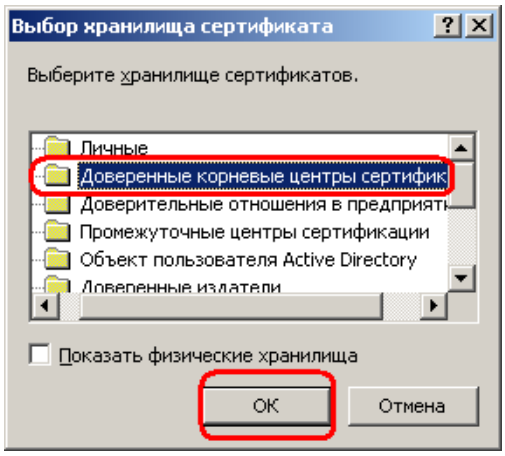
5.4) В окне приветствия Мастера импорта сертификатов нажмите кнопку «Далее».



5.5) В окне выбора Хранилища сертификатов выберите пункт «Поместить все сертификаты в следующее хранилище» и нажмите кнопку «Обзор…».

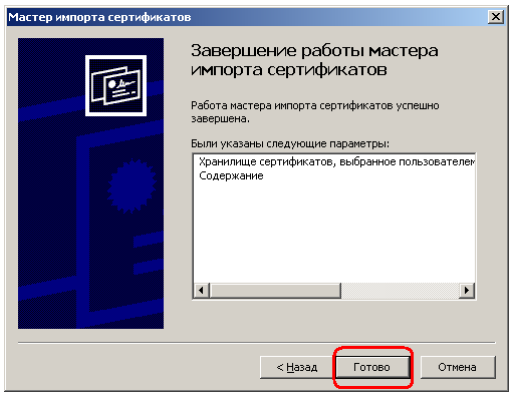


5.6) В указанном списке выберите пункт «Доверенные корневые центры сертификации» и нажмите кнопку «ОК».

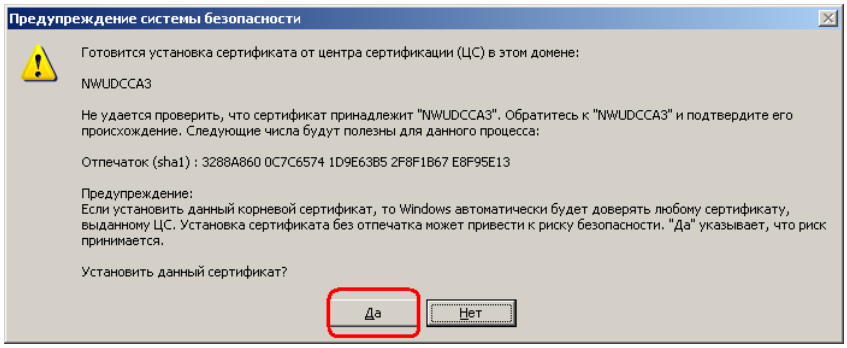


После этого автоматически откроется предыдущее окно, но в поле «Хранилище сертификатов» теперь будет указано «Доверенные корневые центры сертификации». Нажмите кнопку «Далее».

5.7) В окне «Завершение работы мастера импорта сертификатов» нажмите кнопку «Готово».



5.8) На экране появится предупреждение системы безопасности. Ознакомьтесь с выведенной информацией и нажмите кнопку «Да», подтверждая тем самым свое согласие на установку корневого сертификата.



5.9) При успешной установке сертификата появится сообщение «Импорт успешно выполнен». Нажмите кнопку «ОК».

Установка корневого сертификата УЦ завершена.

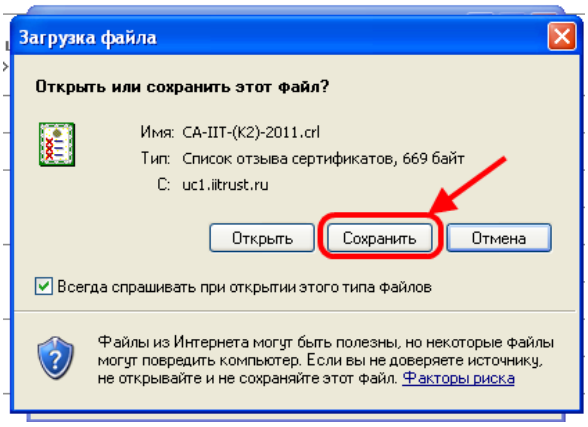
6. Загрузка и установка списка отзыва сертификатов УЦ

В этой части инструкции описаны шаги по установке списка отозванных сертификатов на ваш компьютер.

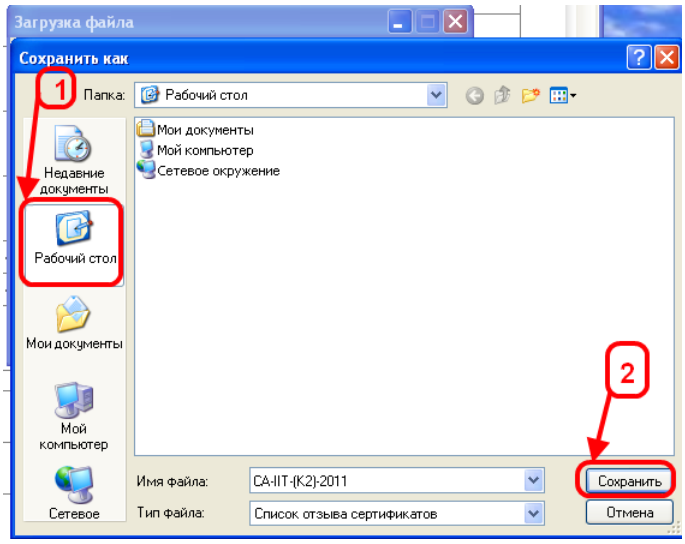
Список отозванных сертификатов (СОС) - файл, подписанный УЦ, содержащий серийные номера СКП, прекративших свое действие (отозванных) раньше установленного срока, причину прекращения действия, информацию об УЦ, отозвавшем сертификаты, и другую служебную информацию.

Исходя из того каким удостоверяющим центром была выдана ваша электронная подпись, вы можете найти список отозванных сертификатов на официальном сайте вашего удостоверяющего центра.

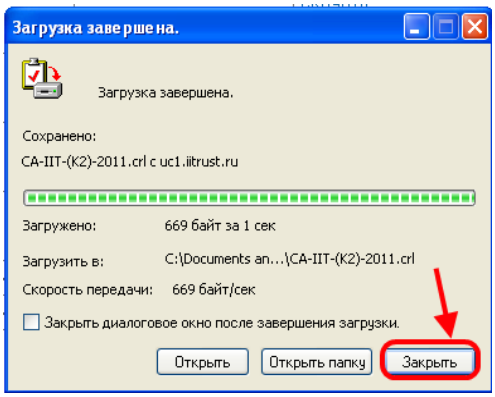
6.1) Загружайте необходимые вам файлы и сохраняйте их на рабочий стол.



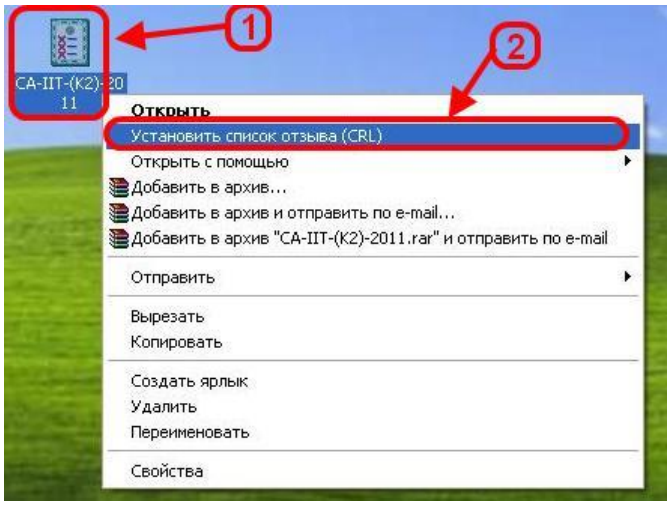
6.2) Сохраните список отзыва сертификатов, например, на рабочем столе. (Рисунок – позиции 1-2)



6.3) Закройте окно по завершению загрузки.

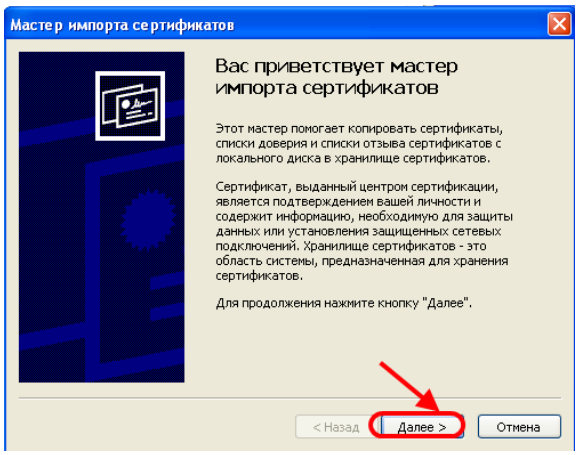


6.4) На иконке списка отзыва сертификатов, сохраненного на рабочем столе, нажмите правой кнопкой мышки (позиция 1) и из выпадающего меню выберите «Установить список отзыва (CRL)» (позиция 2).

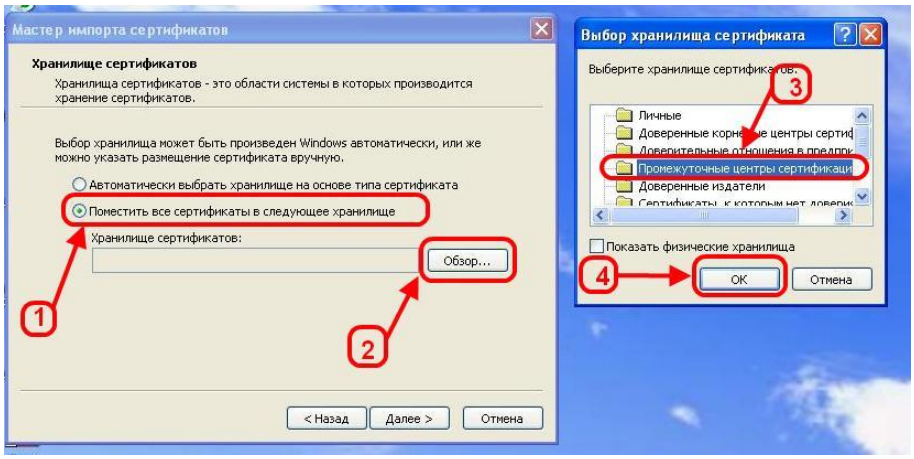


6.5) После того, как откроется мастер импорта сертификатов Windows, нажмите

«Далее».



В окне выбора Хранилища сертификатов выберите пункт «Поместить все сертификаты в следующее хранилище» и нажмите кнопку «Обзор…». В указанном списке выберите пункт «Промежуточные центры сертификации» и нажмите кнопку «ОК».



6.6) При успешной установке списка отозванных сертификатов появится сообщение «Импорт успешно выполнен». Нажмите кнопку «ОК».

Установка списка отозванных сертификатов УЦ завершена.

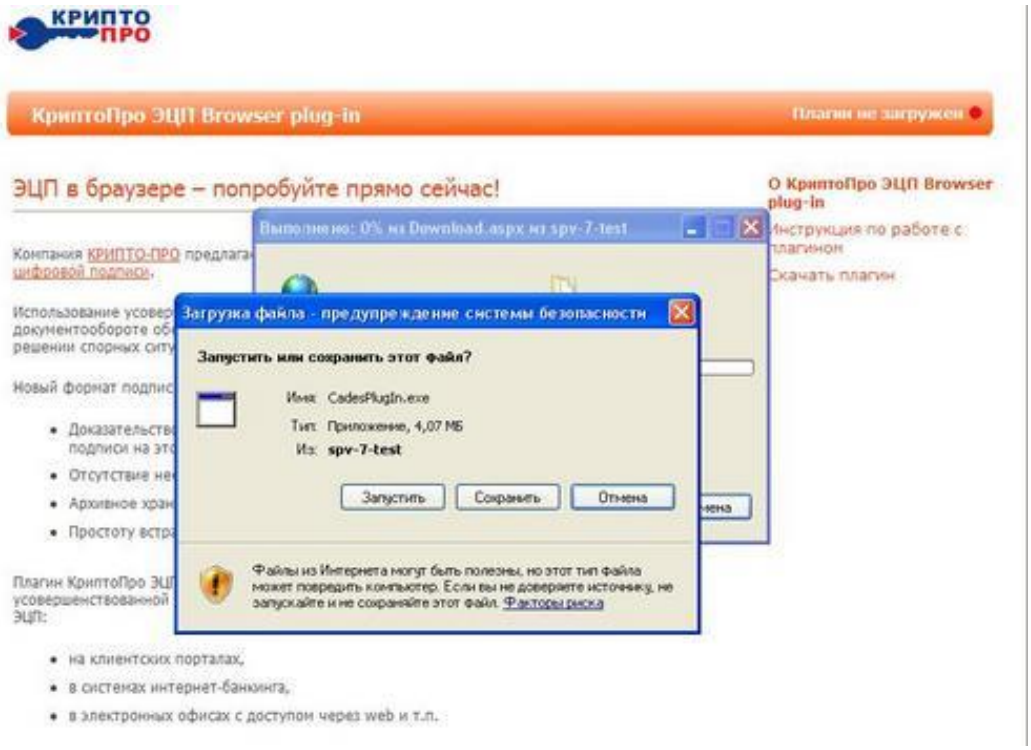
7. Установка ЭП Browser Plug - In

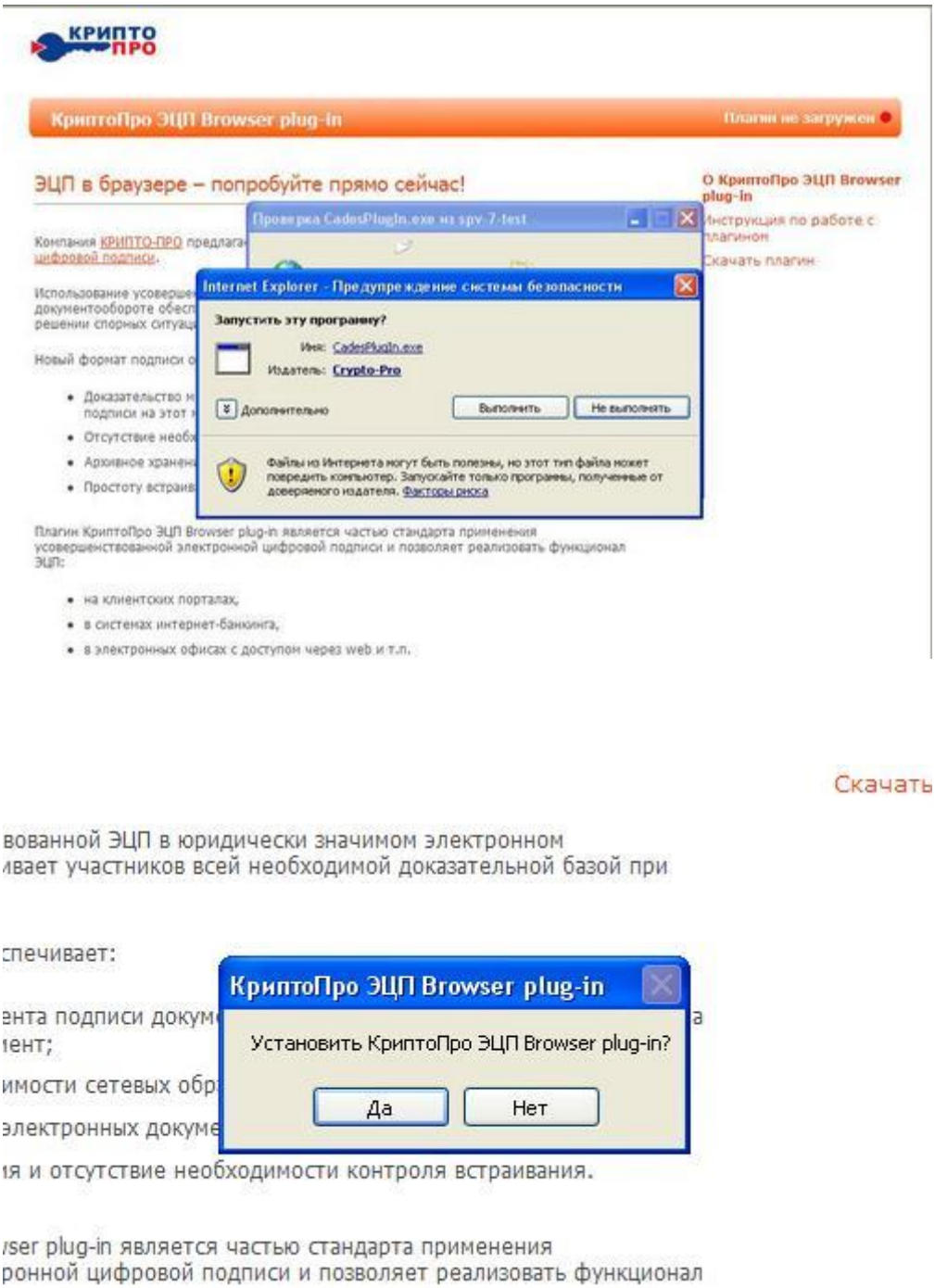
Для корректной работы программы Крипто Про при использовании различных браузеров требуется загрузка дополнительного плагина ЭП Browser plug-in. **КриптоПро ЭП browser plug-in** - это программное обеспечение, предназначено для работы с электронной цифровой подписью (в том числе и с усовершенствованной ЭП) на веб-страницах в сети Интернет.

Внимание! Убедитесь, что все условия для использования КриптоПро ЭП Browser plug-in соблюдены!

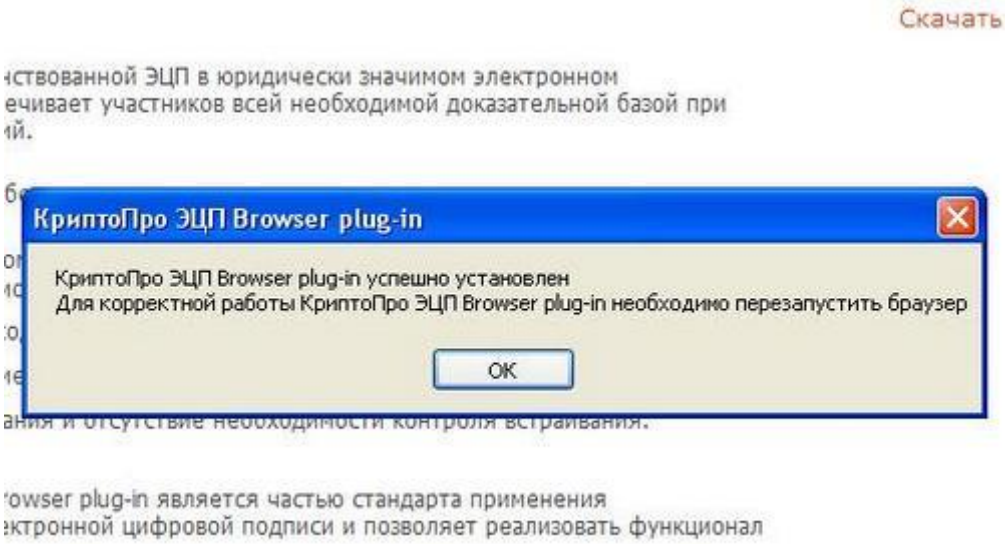
Установка плагина на Windows-платформы

Скачайте программу установки с сайта Крипто ПРО и запустите исполняемый файл CadesPlugIn.exe.





Перезапустите браузер. Если установка прошла корректно, на странице появится информация о том, что плагин загружен.



Установка плагина на Unix-платформы

1. Для работы плагина требуется установленный КриптоПро CSP версии 3.6 и выше. Дистрибутив и инструкцию по установке можно получить по ссылке http://www.cryptopro.ru/products/cades/plugin/downloads.
2. Скачайте и распакуйте архив npcades_linux_ia32.zip или npcades_linux_amd64.zip.
3. Установите пакеты lsb-cprocsp-tsp-util, lsb-cprocsp-ocsp-util, lsb-cprocsp-cades, cprocsp-npcades, cprocsp-cadescapilite из архива. В дистрибутивах семейства Debian необходимо конвертировать пакеты из формата rpm в deb. Для этого можно использовать утилиту alien.
4. Скопируйте файлы libnpcades.so* из /opt/cprocsp/lib/<ia32/amd64>/ в /usr/lib(<32/64>)/mozilla/plugins/ для 32-битных или 64-битных платформ соответственно.

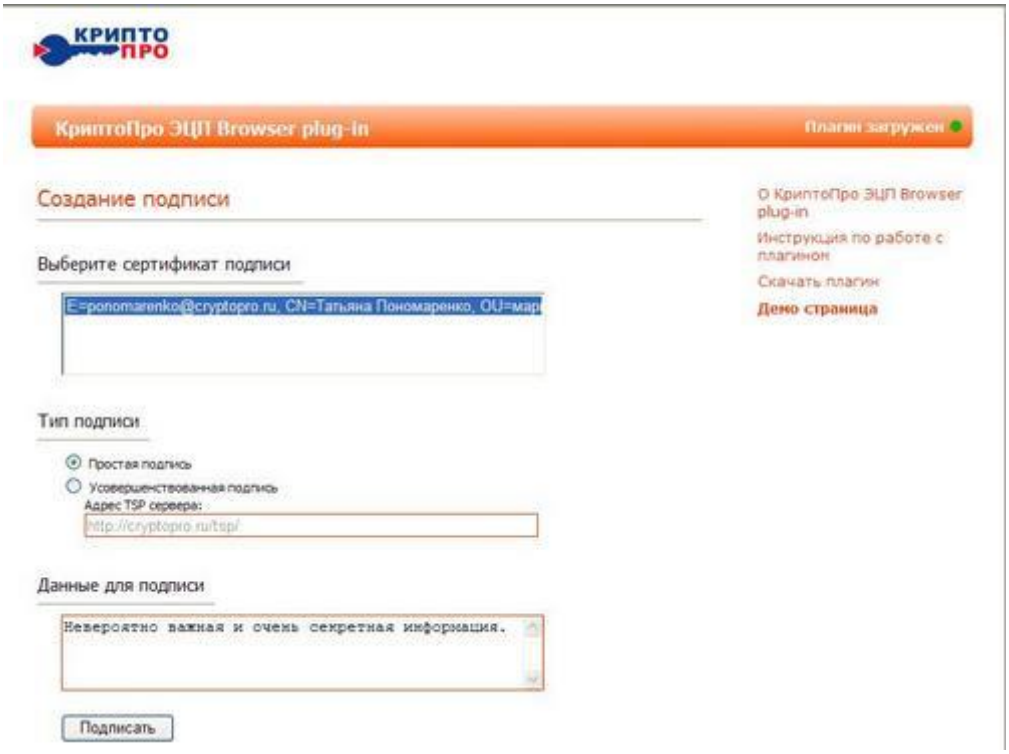
5. Выполните от пользователя root команду /sbin/ldconfig.
6. Перезапустите браузер.

Поддерживаемые браузеры: FireFox версии 3.6 и выше, Opera версии 11.x, Google Chrome.

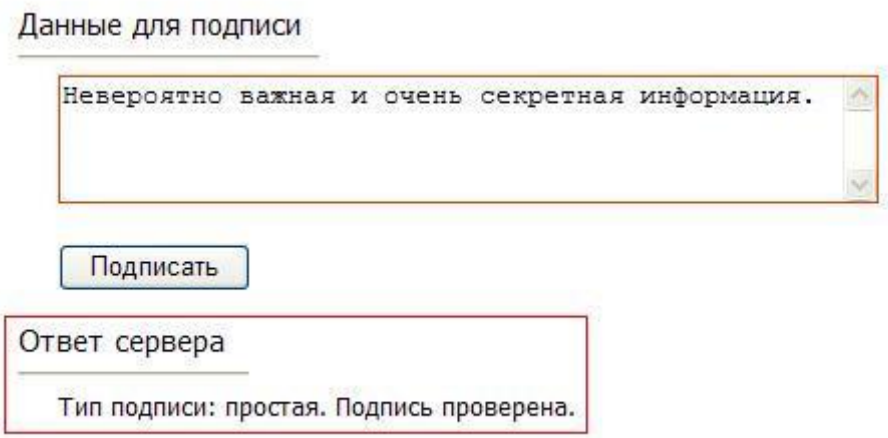
Обратите внимание, что если вы используете как 64-битный, так и 32-битный браузер, то вам необходимо установить и 64-битную и 32-битную версию плагина.

Работа с плагином

Перейдите на демо-страницу.



Следуя указаниям демо-страницы, выберите сертификат подписи, укажите тип подписи, введите текстовые данные для проверки работы плагина и нажмите "Подписать".

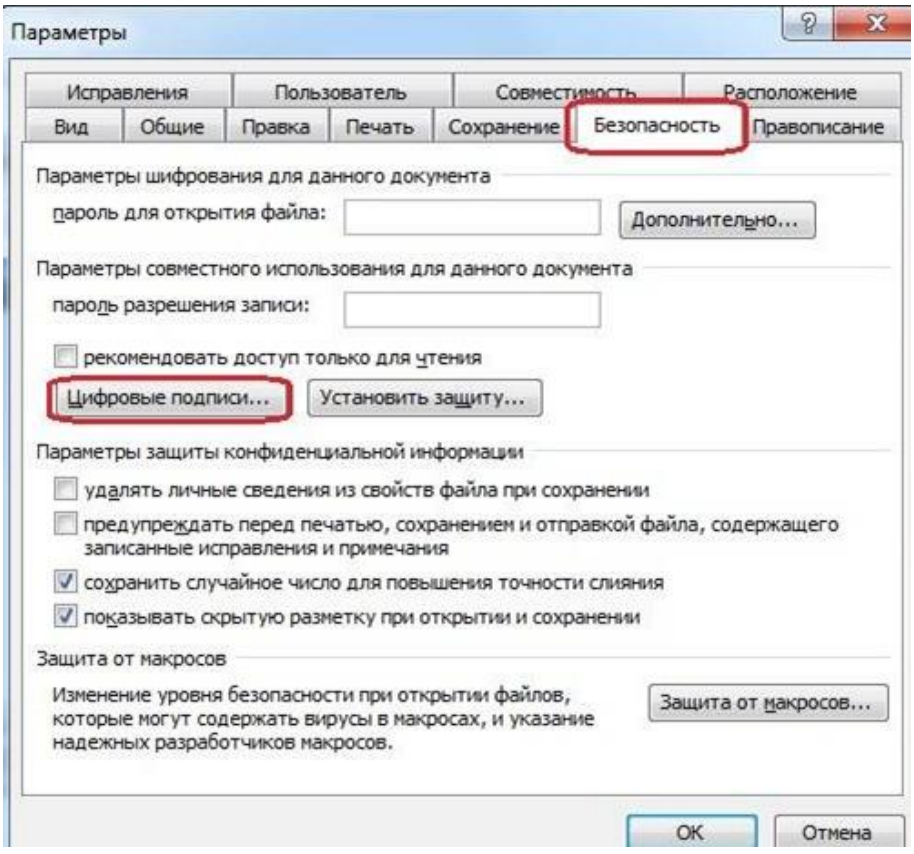

Данные для подписи
Невероятно важная и очень секретная информация.
Подписать
Ответ сервера
Тип подписи: простая. Подпись проверена.

8. Инструкция по добавлению электронной подписи в документе Microsoft Word.

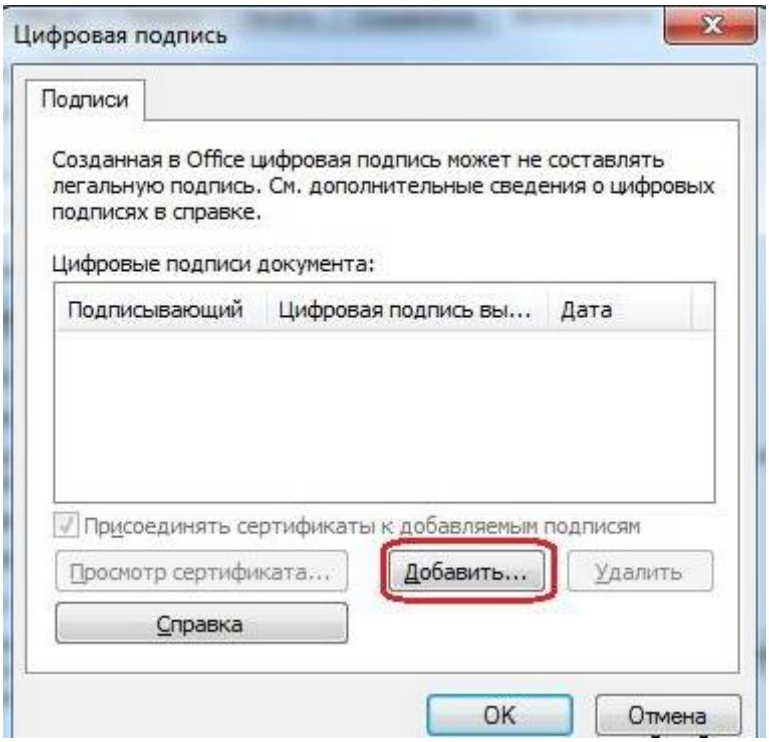
Как подписать документ Word в версии Office 2003 с помощью ЭП

Как только вы создали Word файл и завершили его редактирование необходимо сохранить его и только потом начинать добавление ЭП к документу. Нужно помнить, что после подписания документ станет доступен только для чтения, и если требуется редактирование документа, то сначала следует удалить созданные ЭП, отредактировать и заново подписать, иначе документ будет содержать недействительную подпись. Отмечаем, что на рабочем месте должен быть установлен КриптоПро версии не ранее 3.0, а так же установлен сертификат ЭП в папке "Личные".

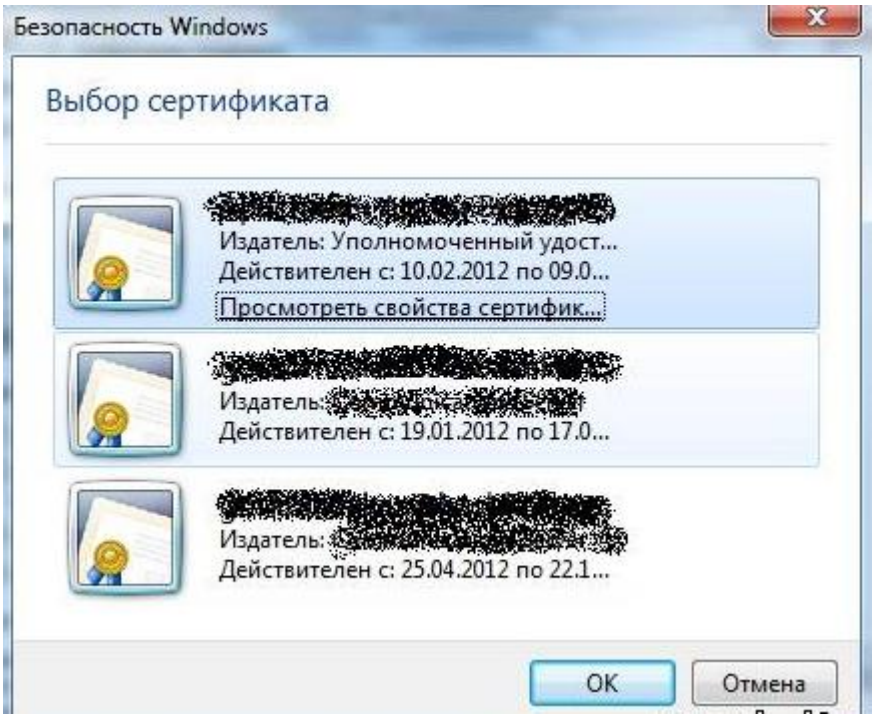
После сохранения документа, который нам нужно подписать, в нашем случае это "Тест.doc", в верхнем меню выбираем "Сервис", "Параметры", и в открывшемся окне нажимаем на вкладку "Безопасность":



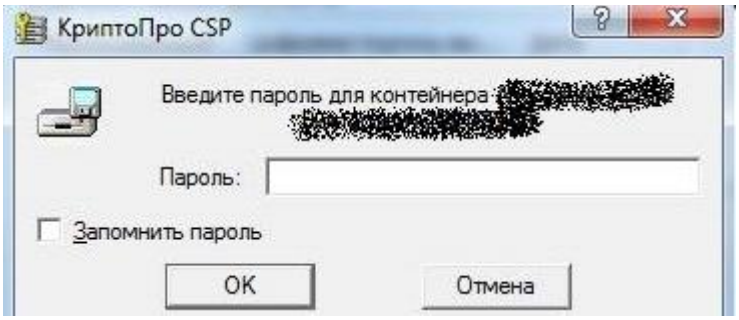
Нажимаем кнопку "Цифровые подписи" и в открытом окне жмем "Добавить":



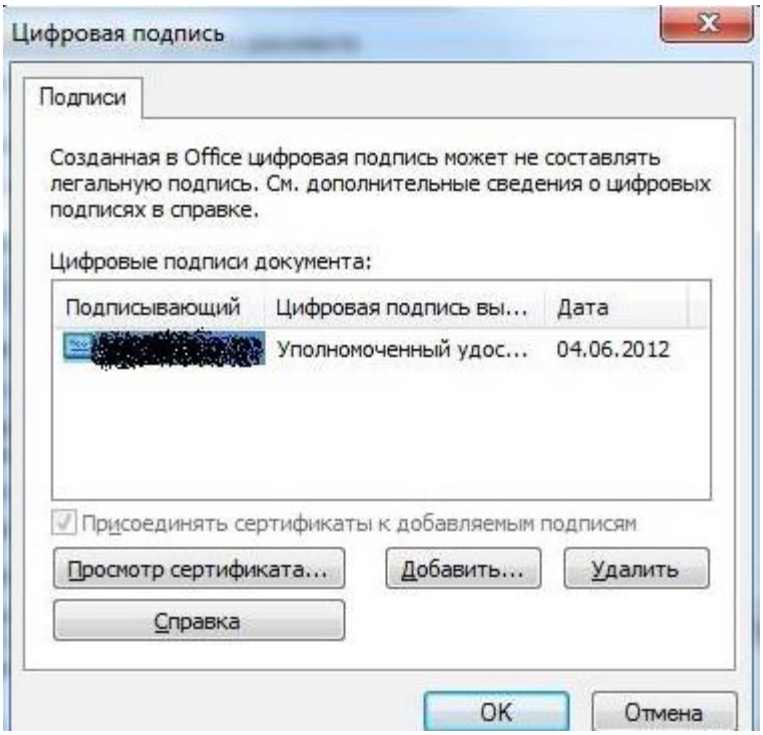
Открывается окно выбора сертификата, выбираем необходимого пользователя, ЭП которого планируется подписать документ:



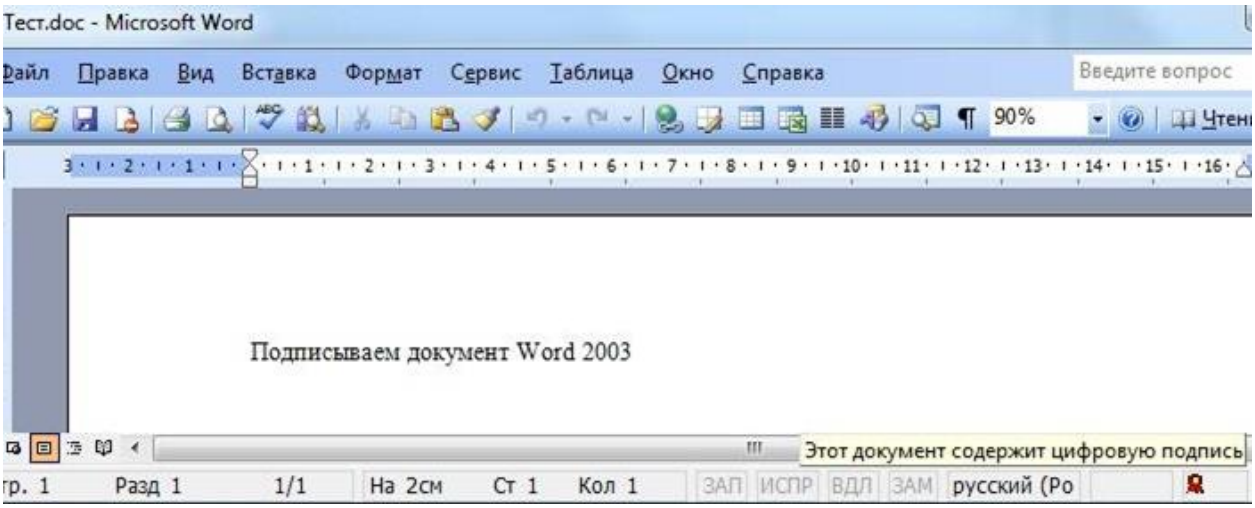
Жмем "ОК", вводим пароль на ЭП: (если ранее на рабочем месте с данным ЭП работали и сохранили пароль, то этого окна у вас не будет)



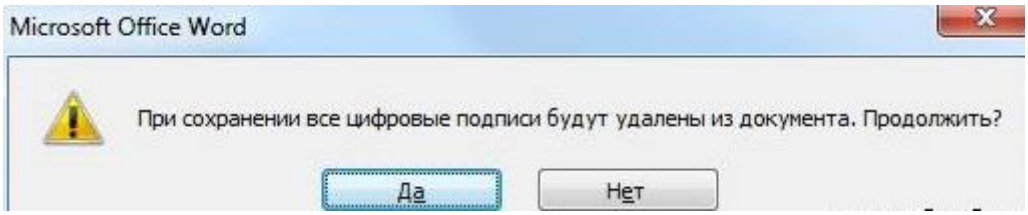
Как видим, в окне Цифровые подписи появился Подписывающий. Кстати, таким же образом можно добавить второго, третьего и т.д. подписанта



Жмем "ОК" чтобы закрыть окна. Теперь word документ подписан с помощью ЭП, а в правой нижней части появился значок, при наведении на который появляется надпись: "Этот документ содержит цифровую подпись":



С этого момента, любые изменения вносимые в документ, удаляют цифровые подписи, о чем информирует нас Word при попытке сохранить изменения:

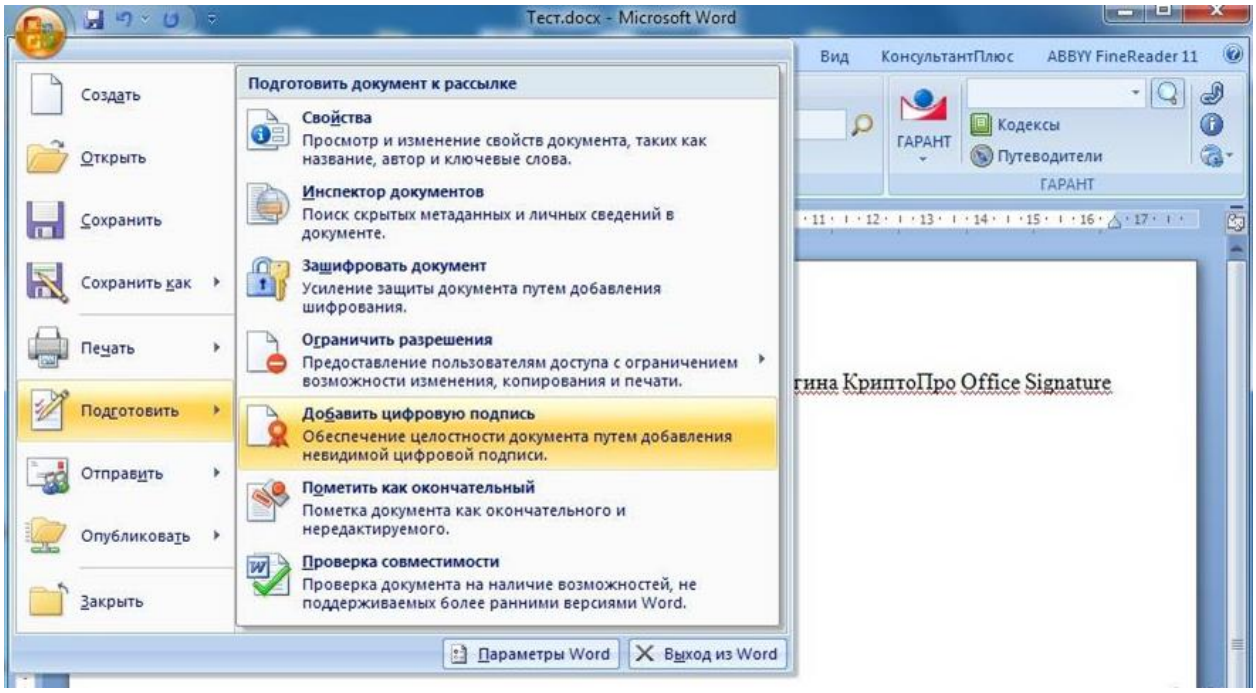


Как подписать файл Word 2007 и 2010 с помощью ЭП

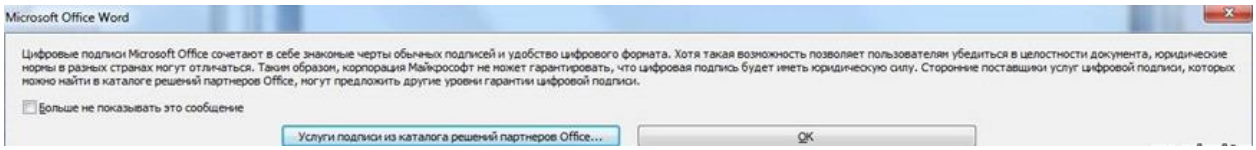
Первый вариант: Подписываем документ Word 2007 без использования плагина КриптоПро Office Signature.

После того как вы создали документ и он готов для подписи, сохраните его и не забудьте еще раз проверить текст, так как внесение изменений после добавления ЭП делает ее недействительной. Мы создали документ Тест.docx с заданным текстом и теперь будем подписывать его.

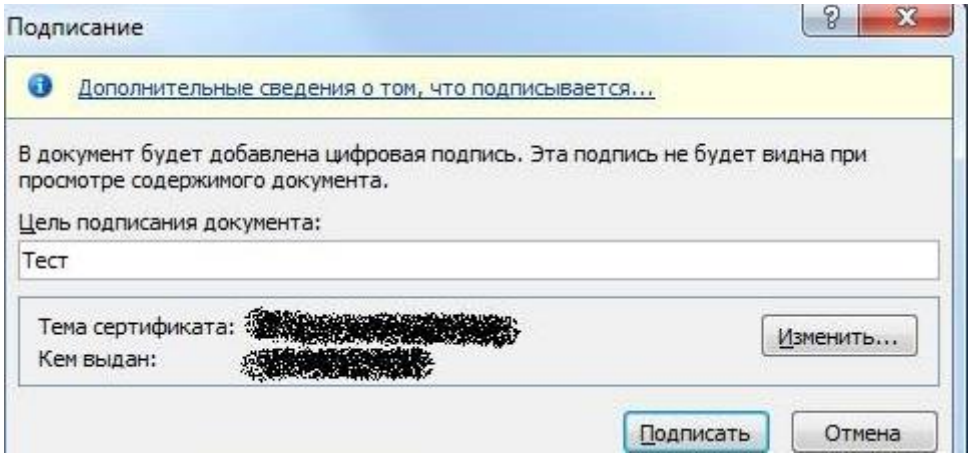
Далее нажимаем значок Office в левом верхнем углу, кнопку "Подготовить" и жмем "Добавить цифровую подпись"



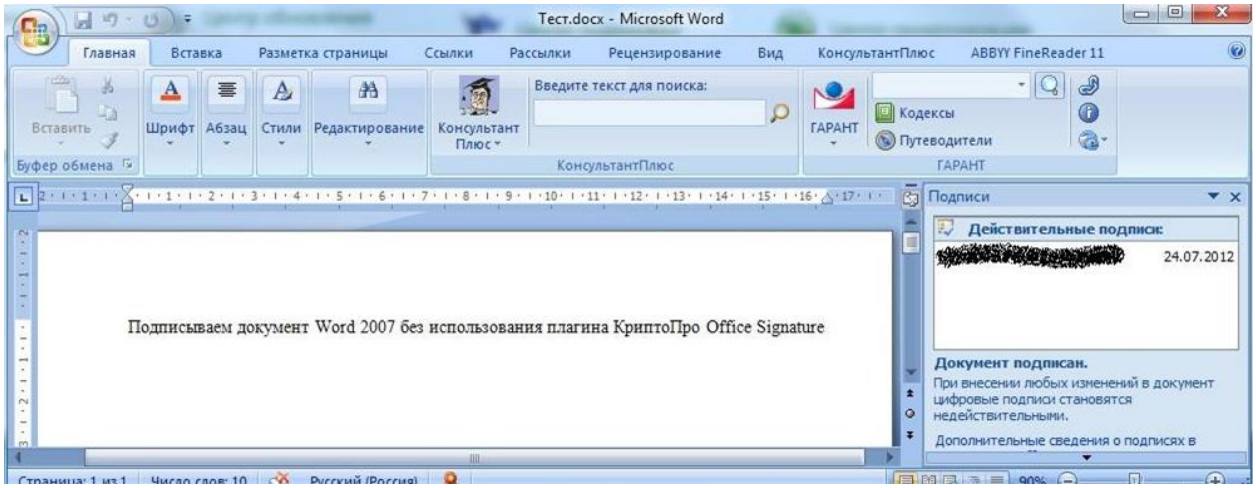
Возможно появление всплывающего окна Microsoft Office Word с информацией о цифровых подписях в документах Office. Данное окно можно закрыть, поставив галочку в поле "Больше не показывать это сообщение" и нажав "ОК".



Далее Вам будет предложено ввести цель подписания документа, но это поле не является обязательным. Если ниже в "Теме сертификата" Вы увидите свое ФИО, это означает что выбран сертификат Вашей подписи и теперь необходимо нажать "Подписать". В ином случае, следует нажать на кнопку "Изменить" и выбрать необходимого пользователя (такое может произойти, если за одним компьютером работает несколько пользователей и у каждого есть собственная ЭП).



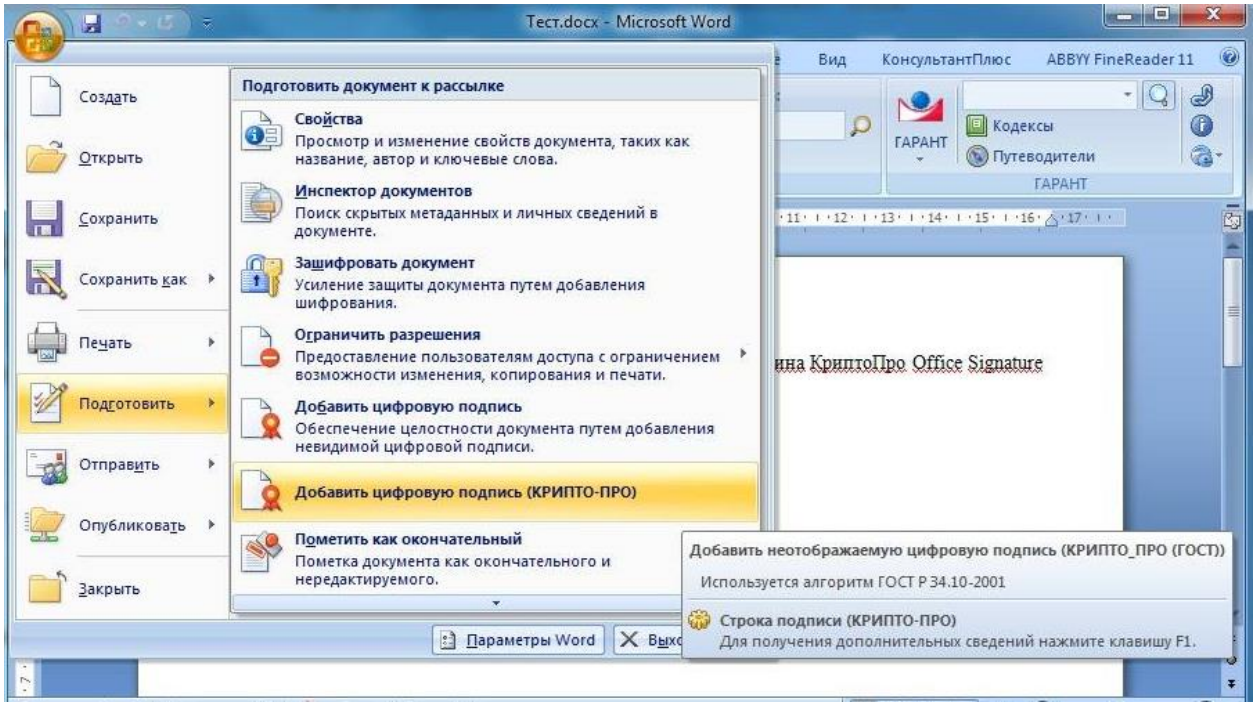
На этом работа по созданию подписи в документе Word 2007 закончена. Как видно на следующем рисунке, справа будут отражены действительные подписи данного документа. Таким же образом можно накладывать на файл дополнительные подписи. При любом изменении файла подписи станут недействительными, и документ утратит свою целостность.



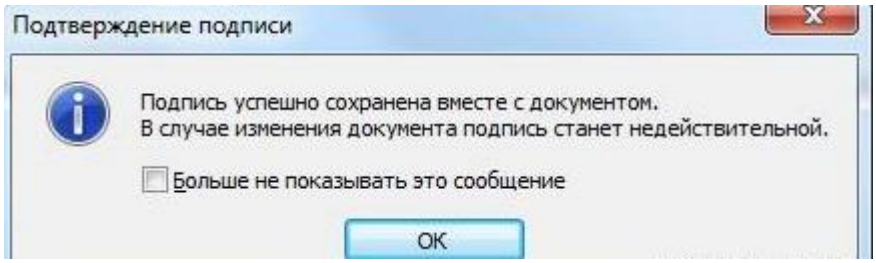
Теперь рассмотрим вариант подписи этого же файла, но уже с помощью плагина КриптоПро Office Signature. Следует отметить, что принципиальных различий в механизме создания подписи нет - отсутствие или наличие этого плагина, а так же версия используемого пакета Office у подписывающей и проверяющей сторон определяют итог. Дело в том, что документы с ЭП созданные в разных версиях Word, что 2003, 2007 или 2010 по - разному могут быть восприняты у принимающей стороны. Для удобства представляем Вам следующую таблицу совместимости.

Документ сделан и подписан в:	Документ открывается в:				
	Office 2003	Office 2007	Office 2007 с плагином	Office 2010	Office 2010 с плагином
Office 2003	Подпись проверяется при наличии КриптоПро CSP 3.0 SP3, или 3.6	Подпись проверяется при наличии КриптоПро CSP 3.6. При наличии CSP 3.0 выводит сообщение «Документ содержит недействительные подписи»	Подпись проверяется при наличии КриптоПро CSP 3.6. При наличии CSP 3.0 выводит сообщение «Документ содержит недействительные подписи»	Выводит сообщение «Документ содержит недействительные подписи»	Выводит сообщение «Документ содержит недействительные подписи»
Office 2007	Подпись не будет показана	Подпись проверяется при наличии КриптоПро CSP 3.0 SP3, CSP 3.6	Подпись проверяется при наличии КриптоПро CSP 3.0 SP3, CSP 3.6	Подпись не будет показана	Подпись не будет показана
Office 2007 с плагином	Подпись не будет показана	При наличии КриптоПро CSP 3.0 SP3, CSP 3.6 выводит сообщение «Документ содержит недействительные подписи», но предлагает ссылку на сайт для установки плагина	Подпись проверяется при наличии КриптоПро CSP 3.0 SP3, CSP 3.6	Подпись не будет показана	Подпись проверяется при наличии КриптоПро CSP 3.0 SP3, CSP 3.6
Office 2010	-	-	-	-	-
Office 2010 с плагином	Подпись не будет показана	При наличии КриптоПро CSP 3.0 SP3, CSP 3.6 выводит сообщение «Документ содержит недействительные подписи», но предлагает ссылку на сайт для установки плагина	Подпись проверяется при наличии КриптоПро CSP 3.0 SP3, CSP 3.6	Подпись не будет показана	Подпись проверяется при наличии КриптоПро CSP 3.0 SP3, CSP 3.6

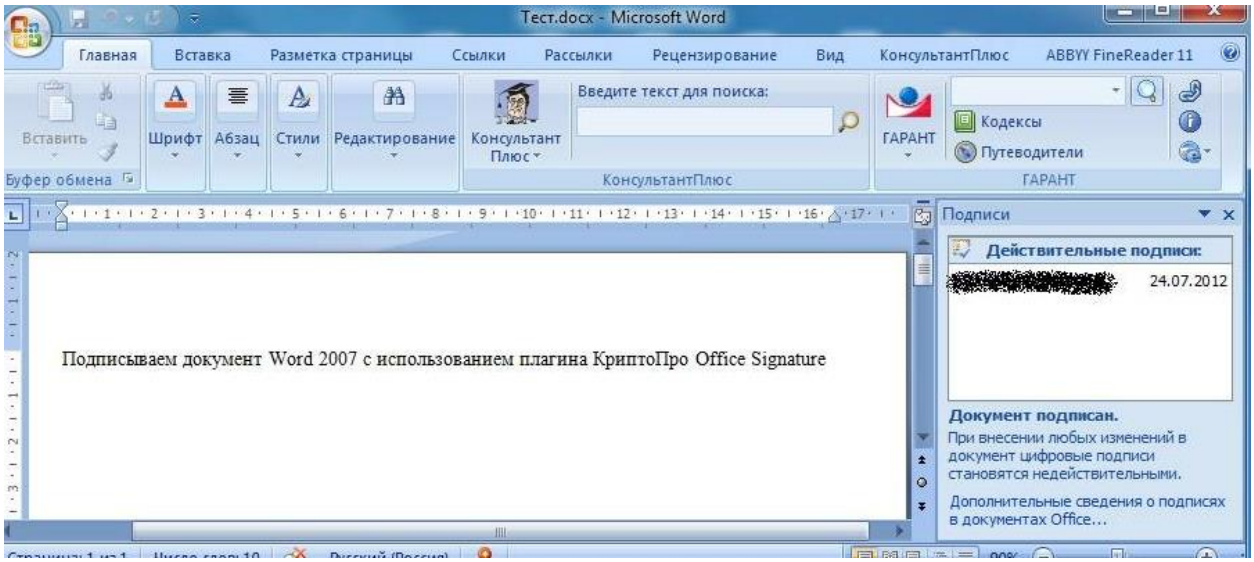
Вернемся к подписи документа с помощью плагина КриптоПро Office Signature. После того как вы скачали и установили его к себе на компьютер появится новая строчка: "Добавить цифровую подпись (КРИПТО-ПРО)", которая открывается через кнопку Office в левом углу и кнопку "Подготовить". Как видите, возможность добавления подписи стандартными средствами тоже осталась.



Аналогично следует выбрать цель подписания, саму подпись, при необходимости ввести пароль на ЭП (если он заранее нее сохранен) и подтвердить подпись:



Результатом является подписанный документ Word 2007.

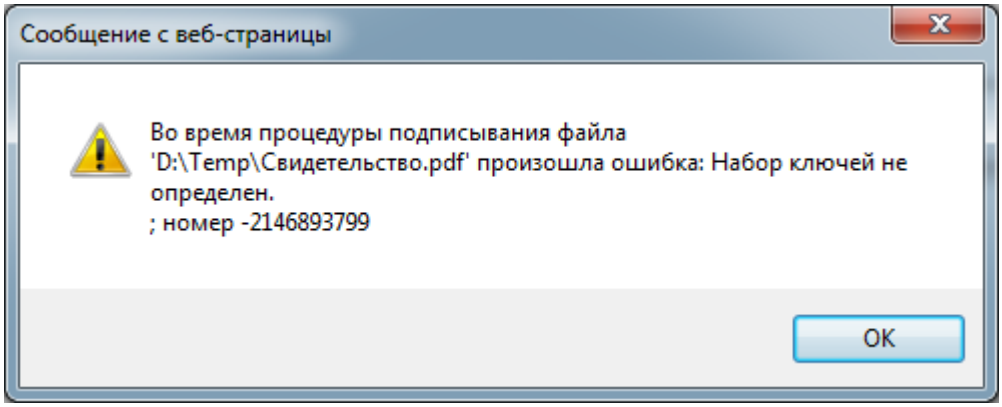


Посмотреть подписи, существующие в документе при повторном открытии, можно через меню (это круглая кнопка - значок Office) - "Подготовить" - "Просмотр подписей".

9. Часто возникающие ошибки

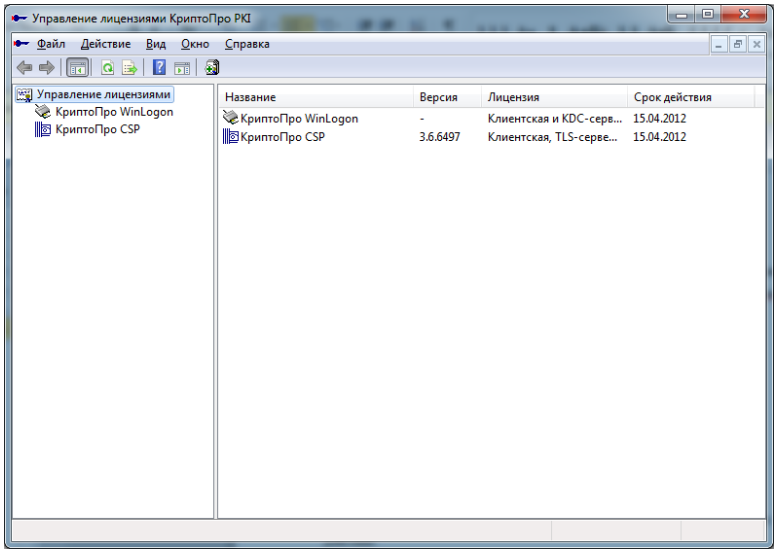
Ошибки установки и настройки Крипто-Про

В случае, если проблема возникла в связи с неправильной установкой и настройкой программного обеспечения «Крипто Про» при попытке подписать документ возникает следующая ошибка.



При возникновении подобной ошибки необходимо проделать следующие действия:

1. Убедиться, что на компьютере установлено ПО «Крипто Про» версии не ниже 3.0 (для Windows XP допустима установка как версии 3.0, так и версии 3.6, для Windows Vista/Windows 7 допустима только версия 3.6). При необходимости установить данное программное обеспечение.
2. Убедиться, что не закончилась лицензия на использование ПО «Крипто Про». Для этого войдите в меню Пуск, найдите папку с «КриптоПро», запустите «Управление лицензиями КриптоПро PKI». Убедитесь, что срок действия компонентов превышает текущую дату.

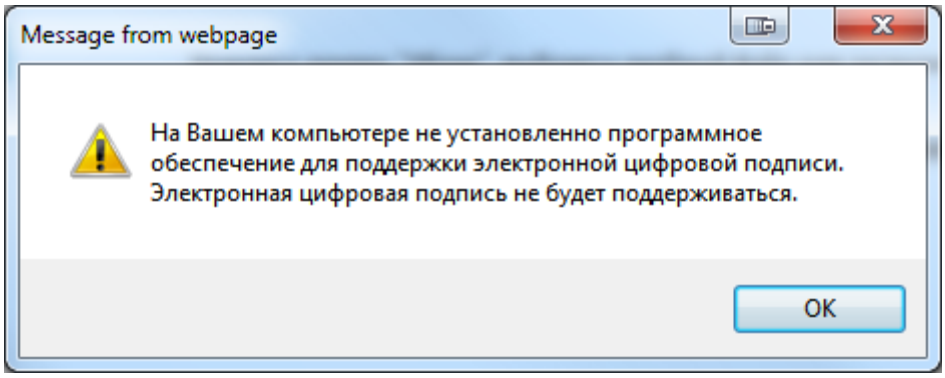


3. Попробуйте переустановить КриптоПро и настроить программу заново.

4. Возможно проблема с флеш устройством, на которой хранится ключ, либо ключ поврежден. Обратитесь в Удостоверяющий Центр

Ошибки настройки системного ПО

В случае если при попытке подписать документ возникает ошибка «На Вашем компьютере не установлено программное обеспечение для поддержки цифровой подписи» необходимо выполнить описанные ниже действия.



1. Убедитесь, что используется правильный браузер. Рекомендуется использовать браузеры Internet Explorer версии 8.0 и выше, FireFox версии 3.6 и выше, Opera версии 11.x, Google Chrome.

2. Убедитесь, что используется 32-битная версия браузера Internet Explorer. Для этого зайдите в меню «Справка» - «О программе». Убедитесь, что рядом с версией нет надписи «64-Bit Edition» (подробнее см. раздел 2.2.1 Руководства).

3. Возможно, требуется установка библиотеки CAPICOM (в зависимости от используемого Вами браузера). Проделайте следующие шаги:

Скачайте последнюю версию CAPICOM на сайте Microsoft.

Для Windows 7 64 bit

Скачайте файл Capicom for Windows 7 64 bit.exe, запустите и далее действуйте по инструкции.

(Установка должна быть произведена в папку “C:\windows\syswow64”)

В 64-разрядной операционной системе (Windows 7), как правило, установлено две версии браузера Internet Explorer: 64 и 32 – битные версии.

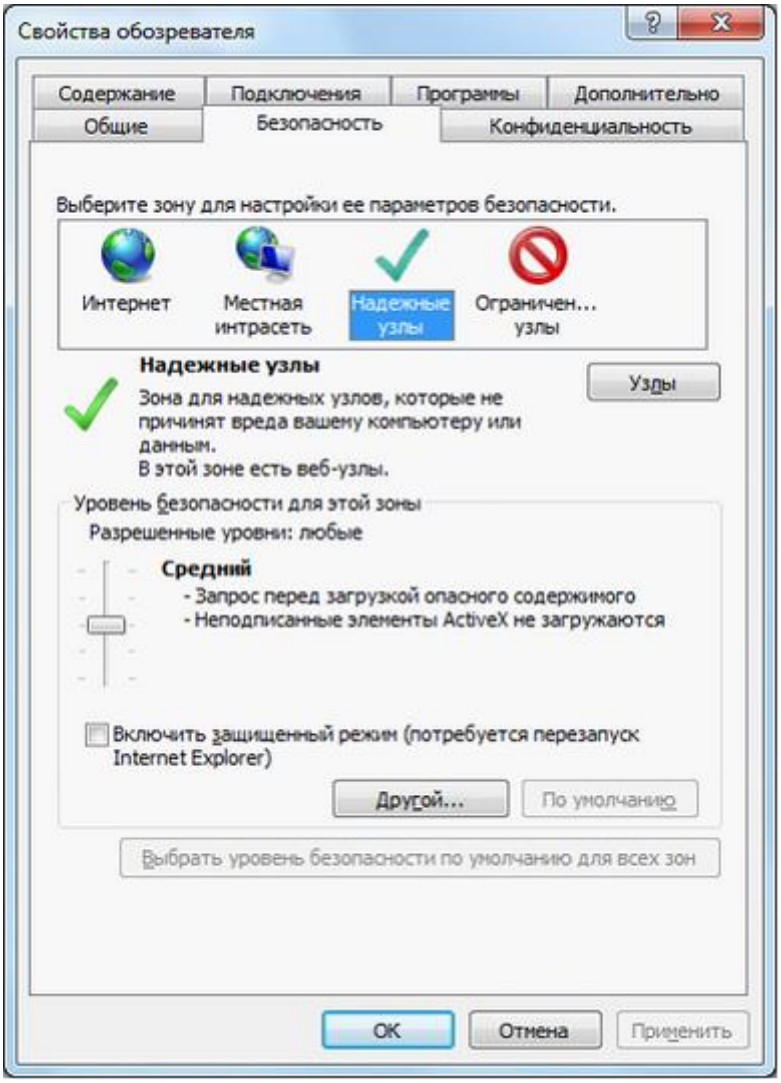
Для работы с ЭЦП на электронной площадке необходимо использовать только 32-битную версию браузера Internet Explorer

Для запуска 32-битной версии Internet Explorer необходимо войти в **«Мой компьютер» → «Диск С» → «Program Files x86» → «Internet Explorer».**

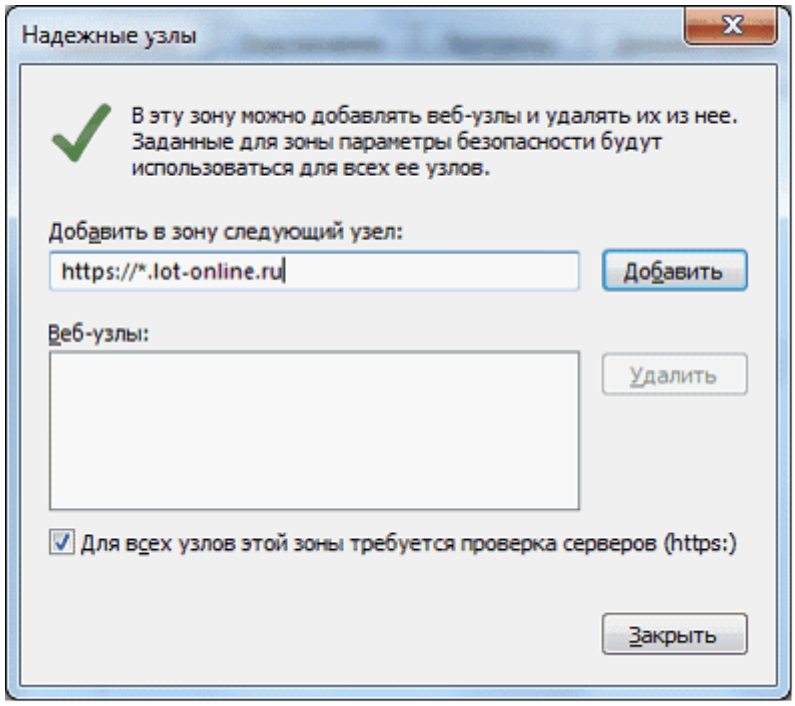
В этой папке необходимо найти и запустить ярлык с именем «iexplore.exe»

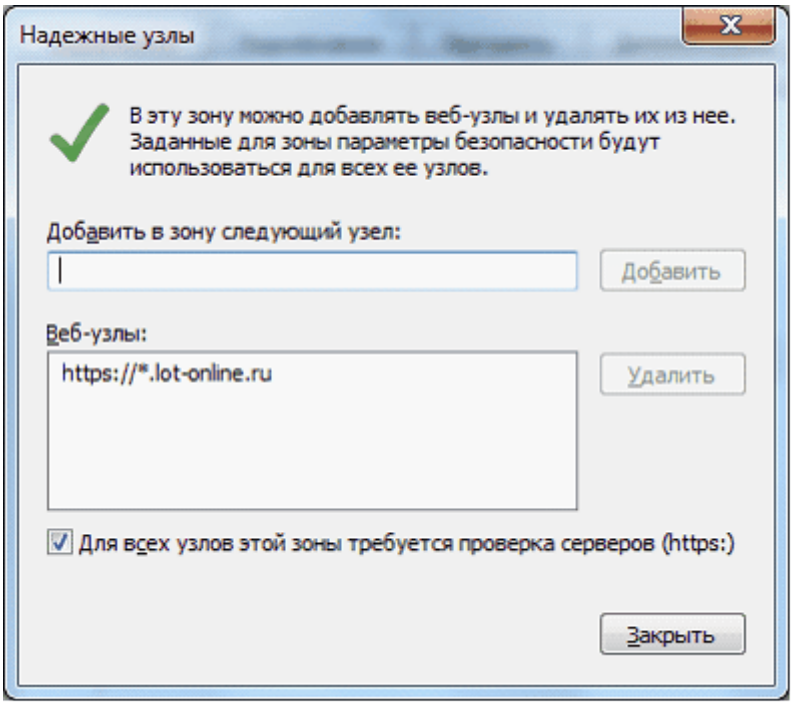
Настройка Internet Explorer для работы на площадке:

Для этого надо зайти в браузере “Сервис” -> “Свойства обозревателя” -> Вкладка “Безопасность”.



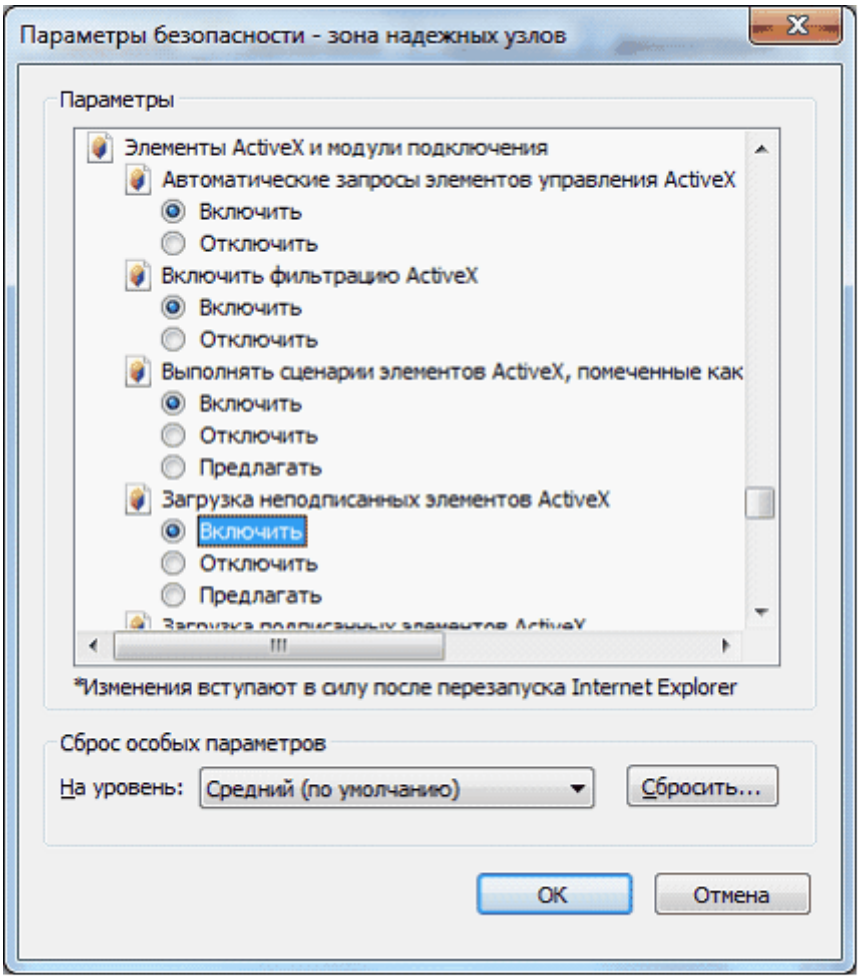
Выбрать “Надежные узлы” -> Нажать кнопку “Узлы”, в открывшемся окне ввести “ https://*.lot-online.ru ” и нажать кнопку “Добавить”





После этого нажать кнопку “Закрыть”

Во вкладке “Безопасность” нажать на кнопку “Другой”



В разделе “Элементы ActiveX и модули подключения” во всех полях выбрать “Включить”.

Если все действия Вами произведены согласно данной инструкции, то вы сможете подписывать документы на нашей площадке.

Ошибки, связанные с использованием некорректных сертификатов.

Ошибка «Некорректный корневой сертификат! Для создания ЭП используйте сертификат, выданный уполномоченным Удостоверяющим Центром»

Данная ошибка возникает, если УЦ, выдавший сертификат, отсутствует в списке доверенных корневых центров сертификации на сервере. Если УЦ состоит в АЭТП, необходимо написать письмо на адрес технической поддержки ЭТП и приложить сертификат пользователя.

Чтобы получить сертификат пользователя надо сделать следующее:

- В Internet Explorer перейти в меню "Сервис" - "Свойства обозревателя", выбрать вкладку "Содержание", нажать кнопку "Сертификаты" (для других браузеров требуются аналогичные действия).
- В открывшемся окне выбрать используемый сертификат, нажать "Экспорт", 3 раза нажать "Далее", ввести путь, куда сохранить открытую часть сертификата, нажать "Далее".
- После того как файл по указанному пути создастся переслать его на адрес технической поддержки ЭТП.

Другие возможные случаи возникновения ошибок при использовании сертификатов на ЭТП и рекомендации по их устранению.

- ***«Сертификат отозван удостоверяющим центром».***

В случае, если сертификат был отозван удостоверяющим центром, следует обратиться в удостоверяющий центр с запросом на выпуск нового сертификата.

- ***«Сертификат выпущен неизвестным удостоверяющим центром».***

Корневой сертификат Вашего Удостоверяющего Центра не поддерживается площадкой. Обратитесь в службу поддержки.

- ***«Сертификат просрочен или ещё не активен».***

Для решения данной проблемы рекомендуется обратиться в удостоверяющий центр, предоставивший ЭП.

- ***«Не удалось расшифровать подпись».***

При возникновении данной ошибки рекомендуется обратиться в службу поддержки.

- ***«Переданные данные не соответствуют подписи».***

Для решения проблемы рекомендуется обратиться в службу технической поддержки.

- ***«Ошибка создания цифровой подписи».***

Возможно, не установлен корневой сертификат (выполните повторно действия из раздела 5 данного руководства) или не установлен сертификат в систему CryptoPro (повторите действия из раздела 4 данного руководства).

- ***«Ошибка инициализации цифровой подписи»,***
  «Ошибка загрузки сертификатов для цифровой подписи».

Данные ошибки возникают при наличии проблем с плагином CryptoPro. Рекомендуется повторить действия, описанные для решения проблемы «Ошибки установки и настройки Крипто-Про».