Инструкция
по установке средств криптографической защиты информации для подачи электронных документов на государственную регистрацию

Содержание:

Начальные условия.

1. Windows XP SP3 или выше (например, Windows 7);
2. Internet Explorer 8.0 или выше (при отсутствии Вы можете загрузить с сайта компании Microsoft: http://windows.microsoft.com/ru-RU/internet-explorer/download-ie);
3. Квалифицированный сертификат ключа проверки электронной подписи (далее – КСКПЭП) и соответствующий ему ключ электронной подписи, являющиеся действительными на момент подписания электронного документа и на день направления указанных документов в налоговый орган;

   Примечание: КСКПЭП должен быть выдан аккредитованным удостоверяющим центром Минкомсвязи России (далее АУЦ), аккредитация которого действительна на день выдачи сертификата. Перечень АУЦ размещен на Портале государственных услуг Российской Федерации (http://e-trust.gosuslugi.ru/CA).

Установка.

Шаг 1. Установка драйвера ключевого носителя.

Установите для носителя, на котором размещён ключ электронной подписи, драйвер в соответствии с указаниями разработчика носителя.

Например, если Вы используете ключевой носитель eToken разработки компании «Алладин Р.Д.», скачайте драйвер (ПО eToken PKI Client) этого устройства с сайта компании по ссылке http://www.aladdin-rd.ru/support/downloads/26037/, извлеките ключевой носитель eToken из разъема USB компьютера, установите драйвер с настройками по умолчанию и выполните перезагрузку.

Шаг 2. Установка СКЗИ

Установите в соответствии с указаниями разработчика средство криптографической защиты информации (СКЗИ), реализующие следующие требования:

1) Авторизация и обеспечение юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки усиленной квалифицированной электронной подписи (ЭП) в соответствии с отечественным стандартом ГОСТ Р 34.10-2001;
2) Обеспечение конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
3) Обеспечение аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;
4) Контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;
5) Управление ключевыми элементами системы в соответствии с регламентом средств защиты.

Примечание: Вы можете использовать сертифицированное СКЗИ **КриптоПро CSP** версии 3.6 или выше. Порядок использования КриптоПро CSP приведен на официальном сайте разработчика: http://www.cryptopro.ru (см. также Приложение 2. Установка КриптоПро CSP.)

Шаг 3. Установка личного КСКПЭП.

Выполните настройку СКЗИ для использования КСКПЭП в соответствии с инструкциями разработчика СКЗИ.

Примечание: Если Вы используете КриптоПро CSP см. Приложение 3. Установка КСКПЭП с помощью КриптоПро CSP.

В результате КСКПЭП должен быть установлен в папку «Личные» хранилища сертификатов текущего пользователя и связан с контейнером ключа электронной подписи.

Шаг 4. Установка корневого сертификата УЦ ФНС России.

Скачайте сертификат Ведомственного УЦ ФНС России по следующей ссылке:

http://uc.nalog.ru/crt/ca_fns_russia.crt

и затем установите его в папку «Доверенные корневые центры сертификации» текущего пользователя. См. Приложение 1. Установка сертификата в заданную папку

Шаг 5. Установка корневого сертификата УЦ ФГУП ГНИЦ ФНС России.

Скачайте сертификат УЦ ФГУП ГНИВЦ ФНС России по следующей ссылке:

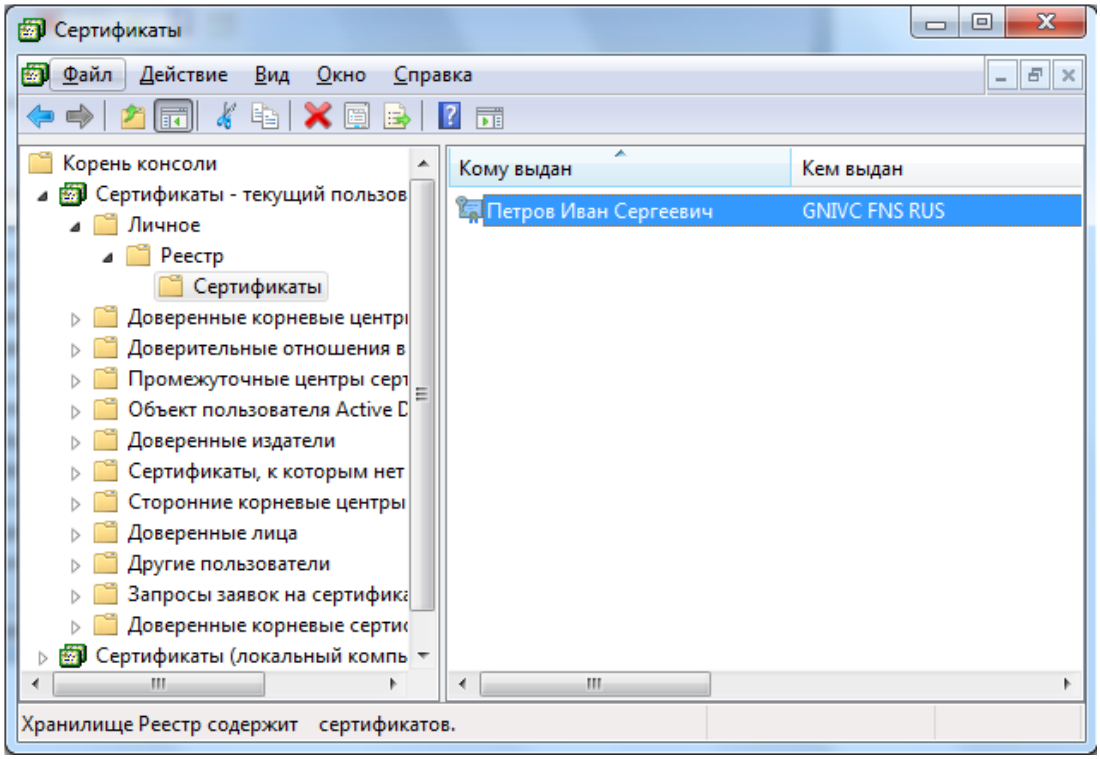
http://www.gnivc.ru/uc/gnivc63-2012.crt

и затем установите его в папку «Доверенные корневые центры сертификации» текущего пользователя. См. Приложение 1. Установка сертификата в заданную папку

Шаг 6. Выстраивание цепочки доверия к личному КСКПЭП

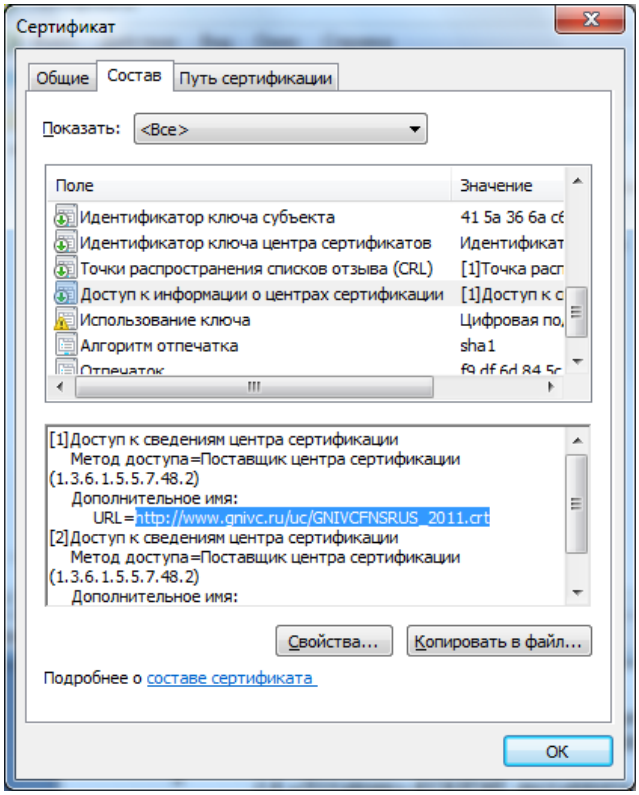
Для выстраивания цепочки доверия к личному КСКПЭП, установка которого была осуществлена в соответствии с 3 шагом настоящей инструкции, необходимо установить корневой сертификат Аккредитованного удостоверяющего центра Минкомсвязи России, издавшего личный КСКПЭП.

Корневой сертификат АУЦ, издавшего личный КСКПЭП, Вы можете получить в обратившись в данный АУЦ. Также Вы можете найти сведения о корневом сертификате АУЦ в личном КСКПЭП. Для этого, если Вы используете КриптоПро CSP, в меню «Пуск» выберите Программы -> Крипто-Про -> Сертификаты. Откройте папку «Сертификаты – текущий пользователь» -> Личные -> Реестр -> Сертификаты:



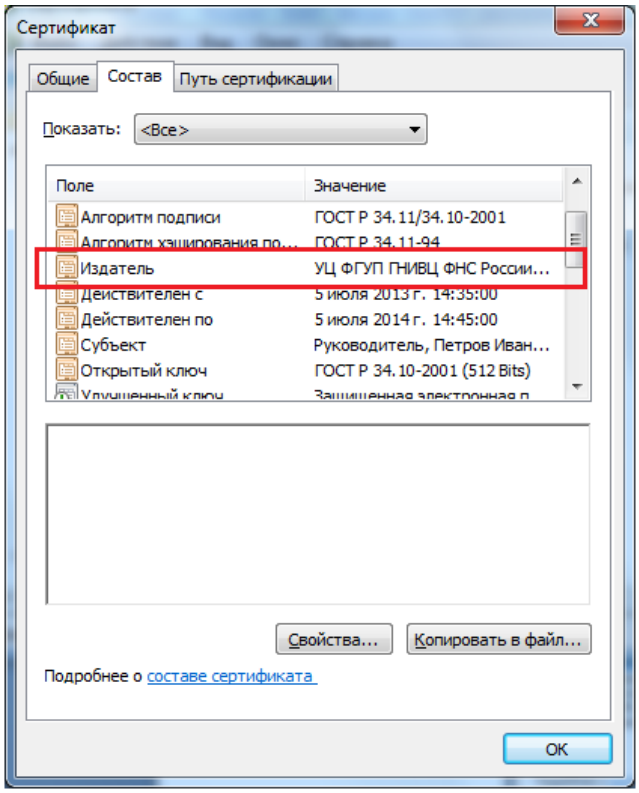
Примечание: Для просмотра сертификатов в хранилище Вы также можете запустить консоль MMC и открыть оснастку сертификаты.

Выберите установленный сертификат, кликнув по нему два раза левой кнопкой мыши. Перейдите на вкладку «Состав»:



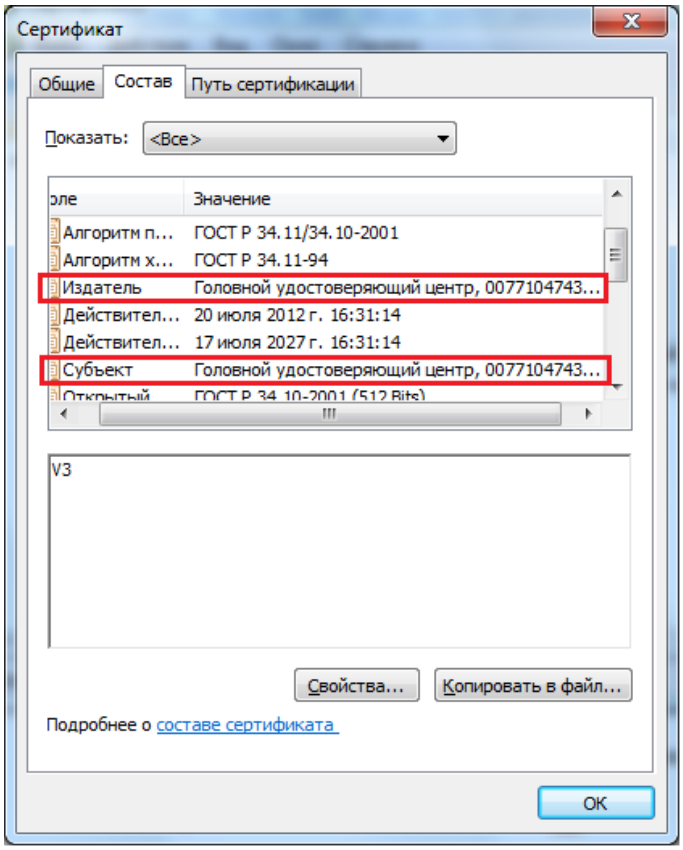
Выберите в верхнем окне строку «Доступ к информации о центрах сертификации» и нижнем окне отобразится ссылка на корневой сертификат по протоколу http. По данной ссылке можно скачать корневой сертификат АУЦ.

В случае отсутствия строки «Доступ к информации о центрах сертификации», можно посмотреть издателя личного КСКПЭП на вкладке «Состав», значение в поле «Издатель». В соответствии с указанной в поле «Издатель» информацией Вам следует связаться с АУЦ и получить корневой сертификат АУЦ.



Перед установкой сертификата, откройте его (кликнув по нему два раза левой кнопкой мыши), чтобы узнать какой это сертификат: корневой (самоподписанный) или нет. Перейдите на вкладку «Состав».

У корневого (самоподписанного) сертификата поля «Издатель» и «Субъект» на вкладке «Состав» имеют одинаковые значения.



Вариант 1

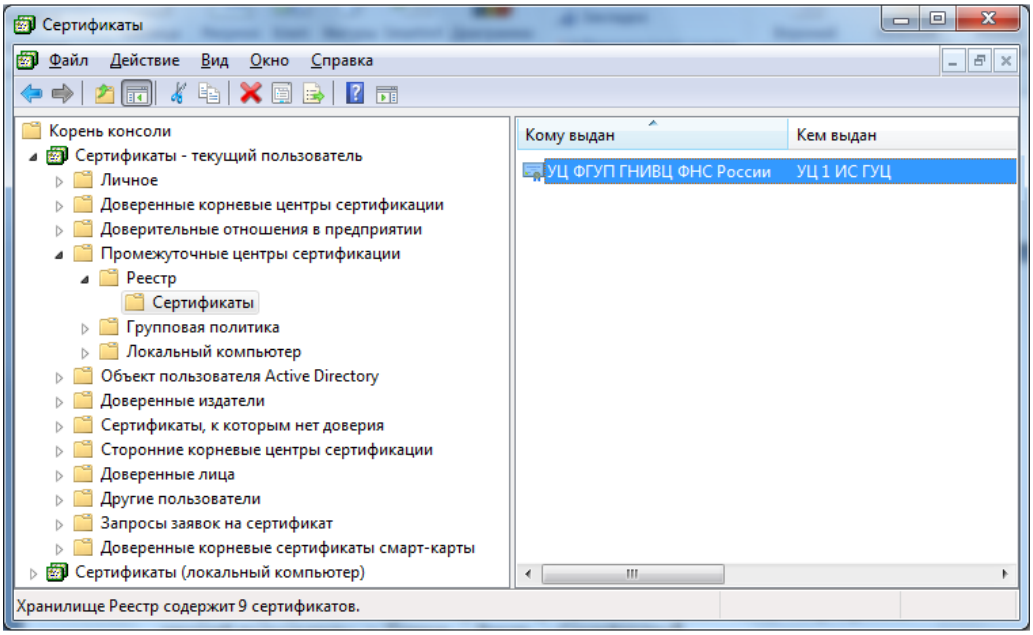
Если сертификат корневой, то его нужно устанавливать в папку ***«Доверенные корневые центры сертификации»***. См. Приложение 1. Установка сертификата в заданную папку.

После установки корневого сертификата цепочка доверия к личному КСКПЭП будет выстроена.

Вариант 2

Если у сертификата поля «Издатель» и «Субъект» на вкладке «Состав» имеют различные значения, то данный сертификат необходимо устанавливать в папку ***«Промежуточные центры сертификации»***. См. Приложение 1. Установка сертификата в заданную папку.

Далее смотрим сведения о следующем сертификате в цепочке. Для этого в хранилище сертификатов откройте папку «Сертификаты – текущий пользователь» -> Промежуточные центры сертификации -> Реестр -> Сертификаты:



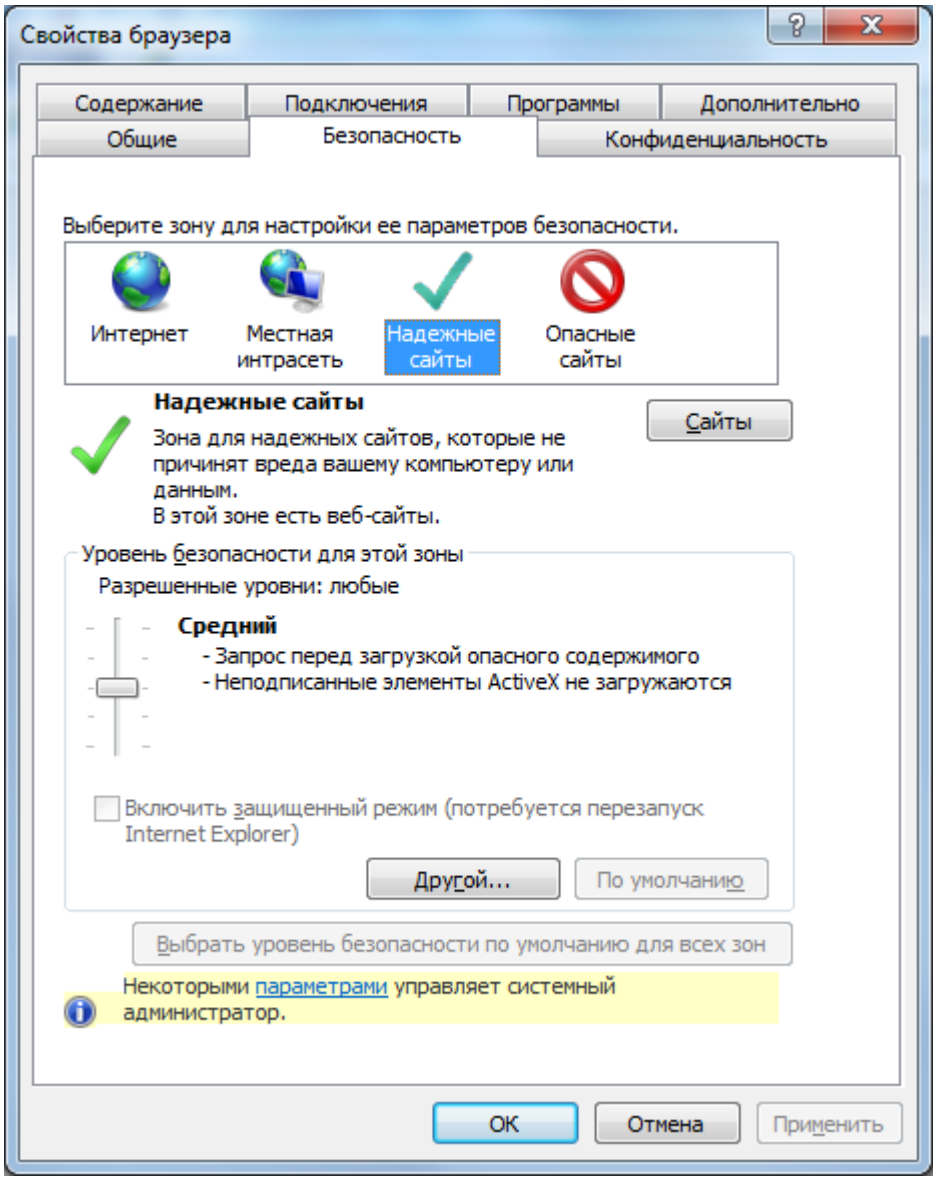
Выберите установленный сертификат, кликнув по нему два раза левой кнопкой мыши. Перейдите на вкладку «Состав», где в строке «Доступ к информации о центрах сертификации» и нижнем окне отобразится ссылка на следующий сертификат в цепочке.

Таким образом, необходимо установить все сертификаты, пока не дойдете до корневого сертификата АУЦ. После установки корневого сертификата будет выстроена цепочка доверия к личному КСКПЭП.

Для проверки установки сертификатов см. Приложение 4. Проверка установки сертификатов.

Шаг 7. Установка узлов https://*.nalog.ru в зону надежных узлов.

Зайдите в меню «Сервис» и выберите пункт «Свойства обозревателя». В появившемся окне перейдите на вкладку «Безопасность», выберите «Надежные узлы» и нажмите кнопку «Узлы».



Нажмите «Сайты» и добавьте https://*.nalog.ru в список.

Проверка установки СКЗИ

Для проверки установки и настройки СКЗИ воспользуйтесь сервисом

https://service.nalog.ru/static/gost-test.html?svc=regin

В случае успешной установки СКЗИ все проверки должны быть успешно пройдены (см. Рис.1)

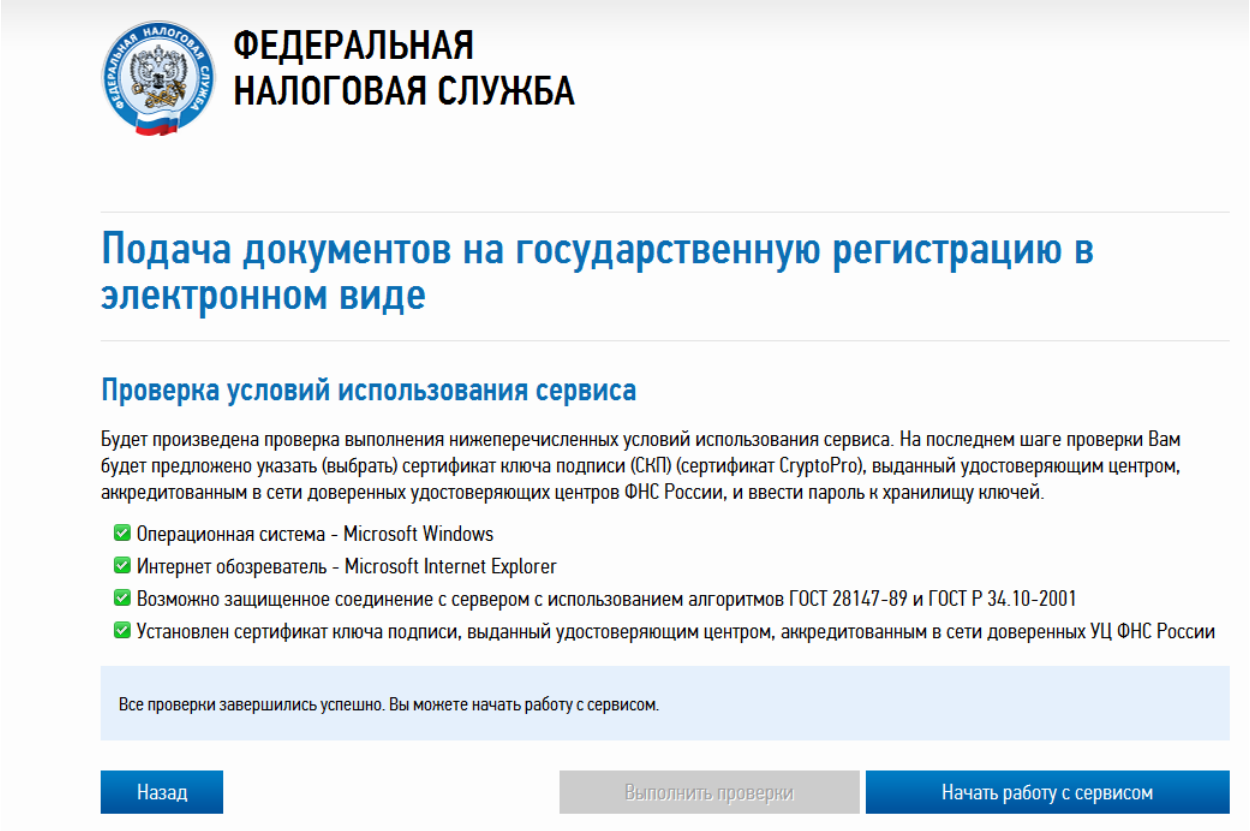


Рис.1

В случае если средства СКЗИ не установлены или установленные средства СКЗИ не удовлетворяют требованиям к СКЗИ, указанными на Шаге 2, то проверка не будет пройдена (см. Рис. 2).

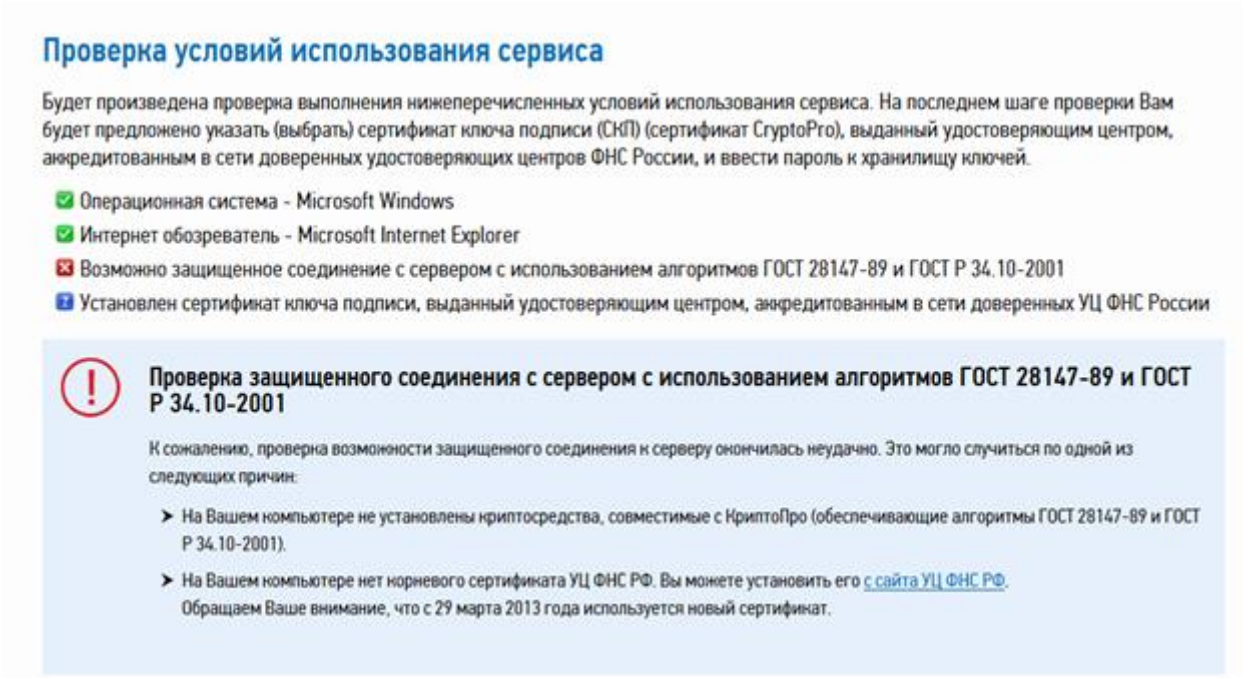


Рис. 2

Для устранения этой ошибки выполните Шаг 2. Установка СКЗИ

В случае если КСКПЭП не установлен или КСКПЭП не удовлетворяет установленным требованиям или не удается выстроить цепочку доверия к КСКПЭП, то проверка не будет пройдена (см. Рис. 3).

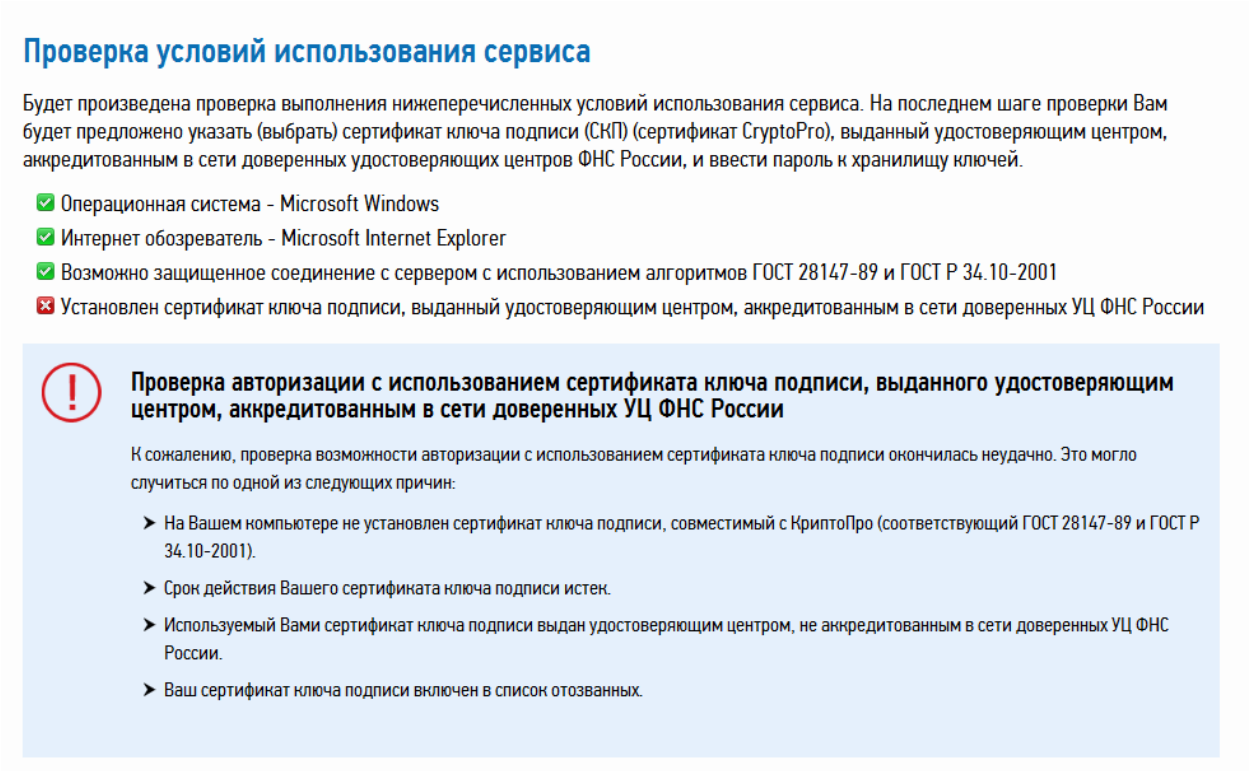
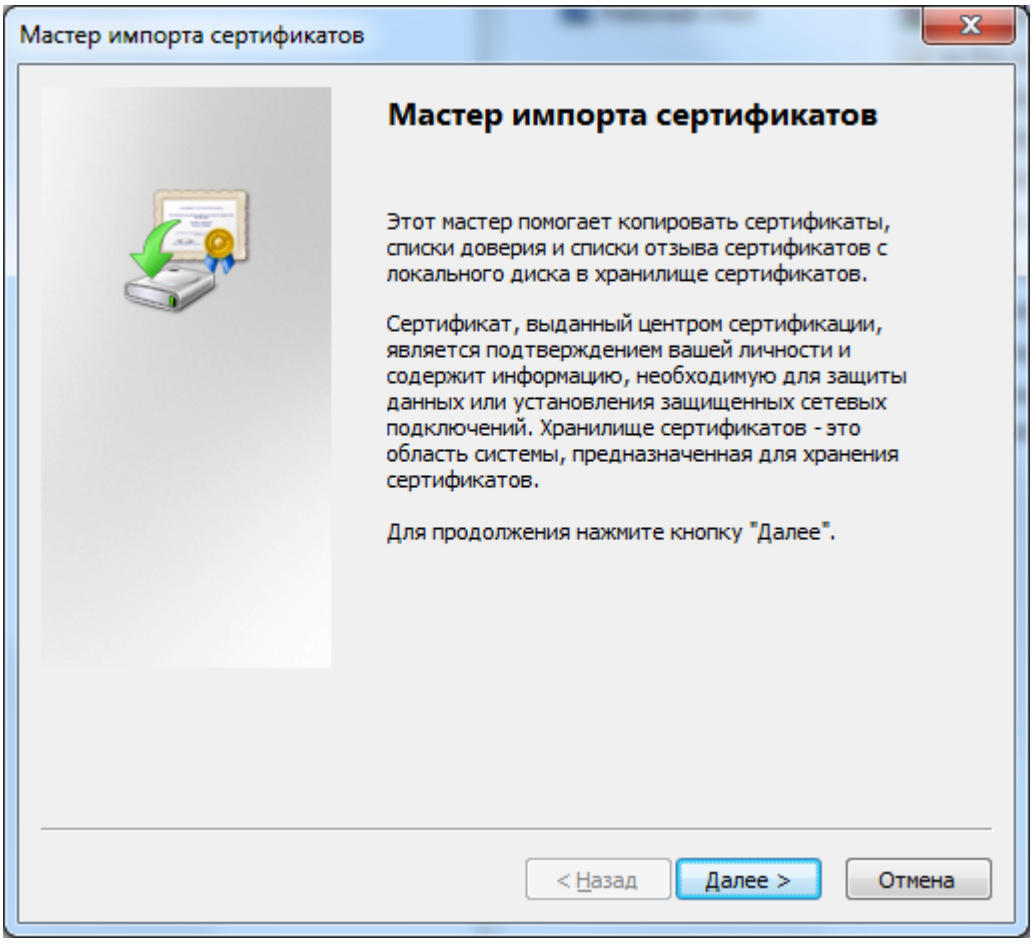


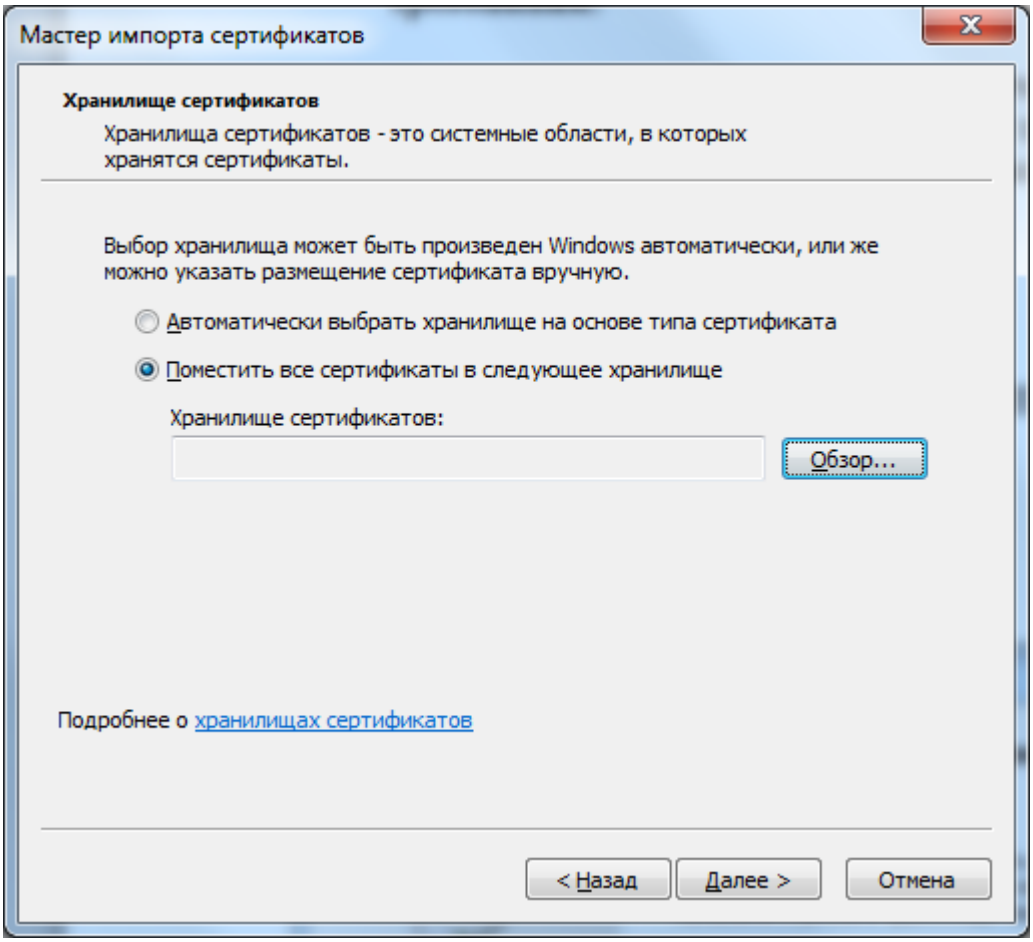
Рис. 3

Для устранения этой ошибки выполните Шаги 3-6 установки.

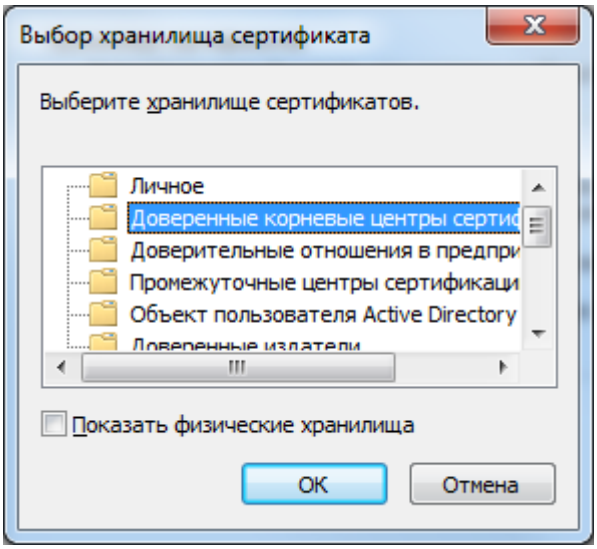
Приложение 1. Установка сертификата в заданную папку

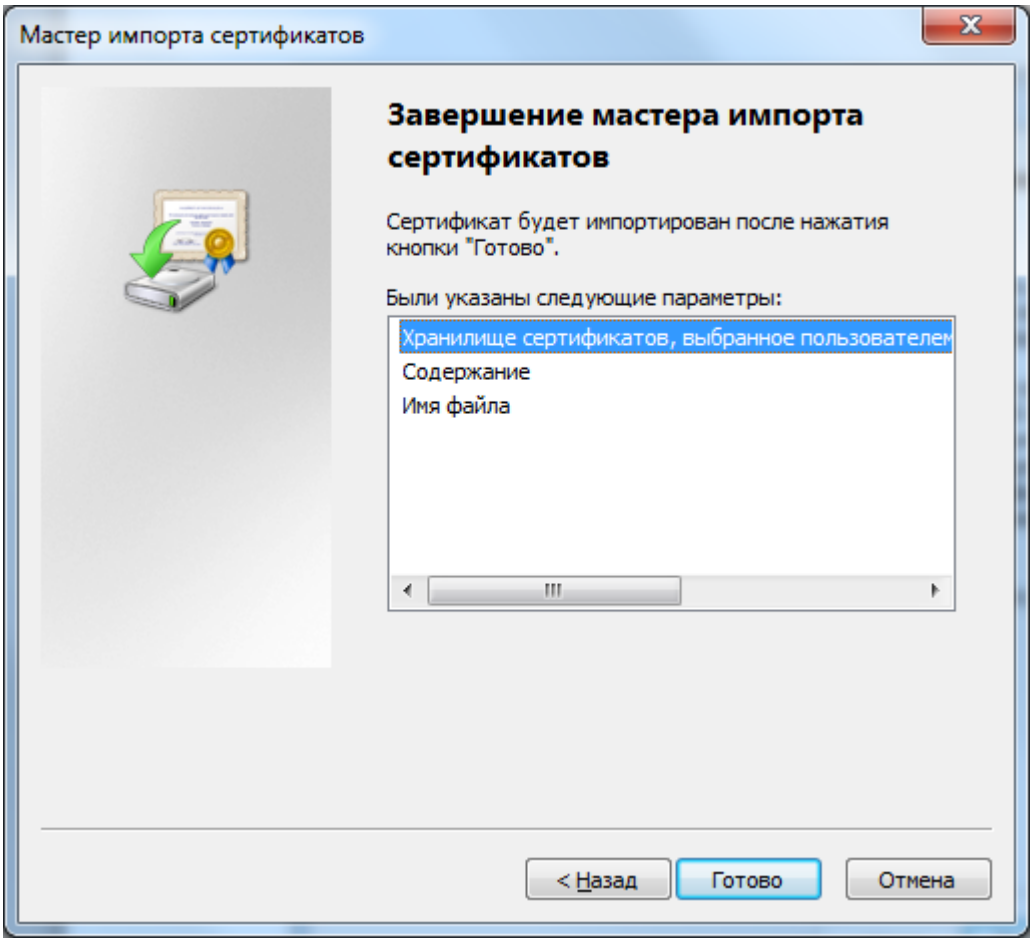


Нажмите «Далее».
В следующем окне выберите «Поместить все сертификаты в следующее хранилище»

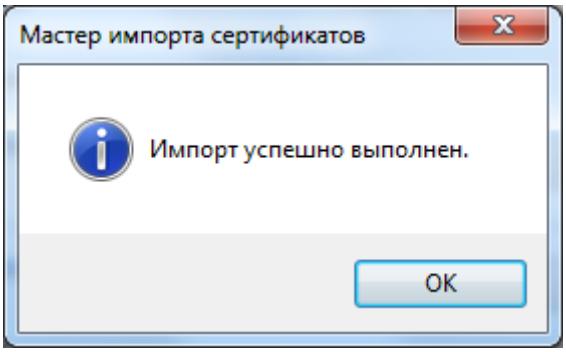


Выберите папку, в которую необходимо установить сертификат».
Например, в папку «Доверенные корневые центры сертификации» как показано на рисунке ниже





В случае предупреждения системы безопасности подтвердите установку сертификата в указанную папку.



Приложение 2. Установка КриптоПро CSP.

На рабочее место пользователя должно быть установлено сертифицированное средство ЭП КриптоПро версии 3.6 или выше с действующей лицензией.

Если на рабочее место пользователя еще не было установлено программное обеспечение КриптоПро, то рекомендуется установить последнюю сертифицированную версию ПО КриптоПро. Установка аналогична установке версии 3.6.

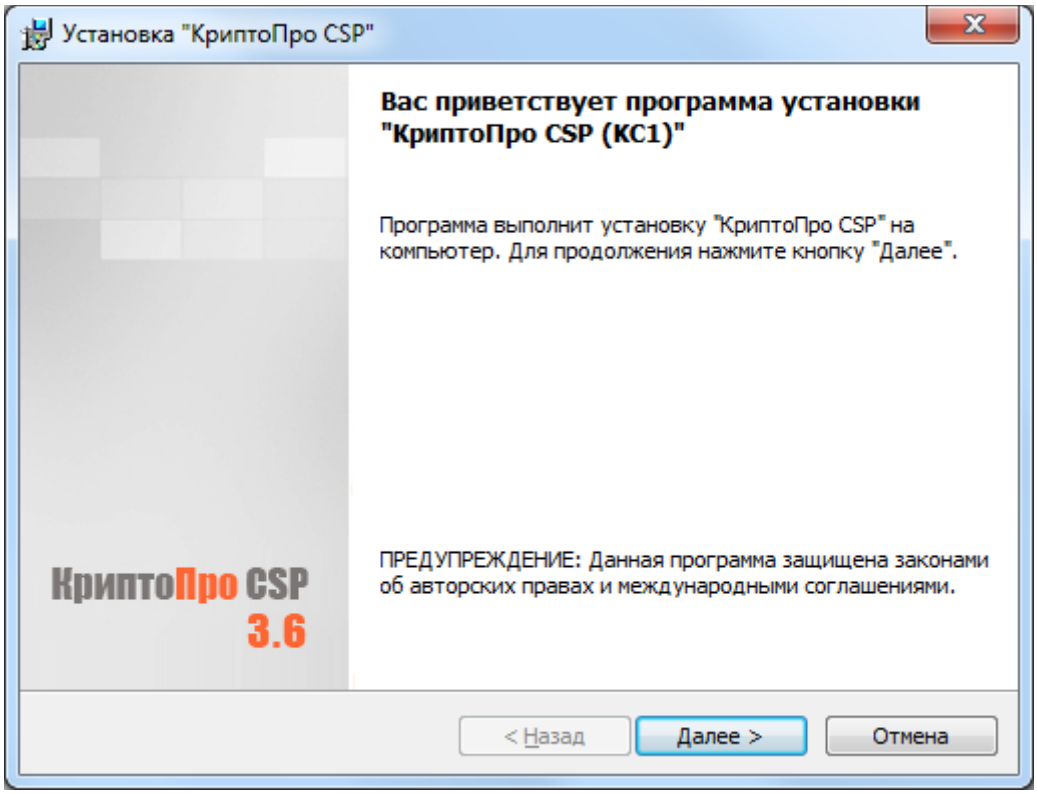
Если на рабочее место пользователя установлено программное обеспечение КриптоПро 3.6, то рекомендуется обновить до последней сертифицированной версии (http://cryptopro.ru/downloads).

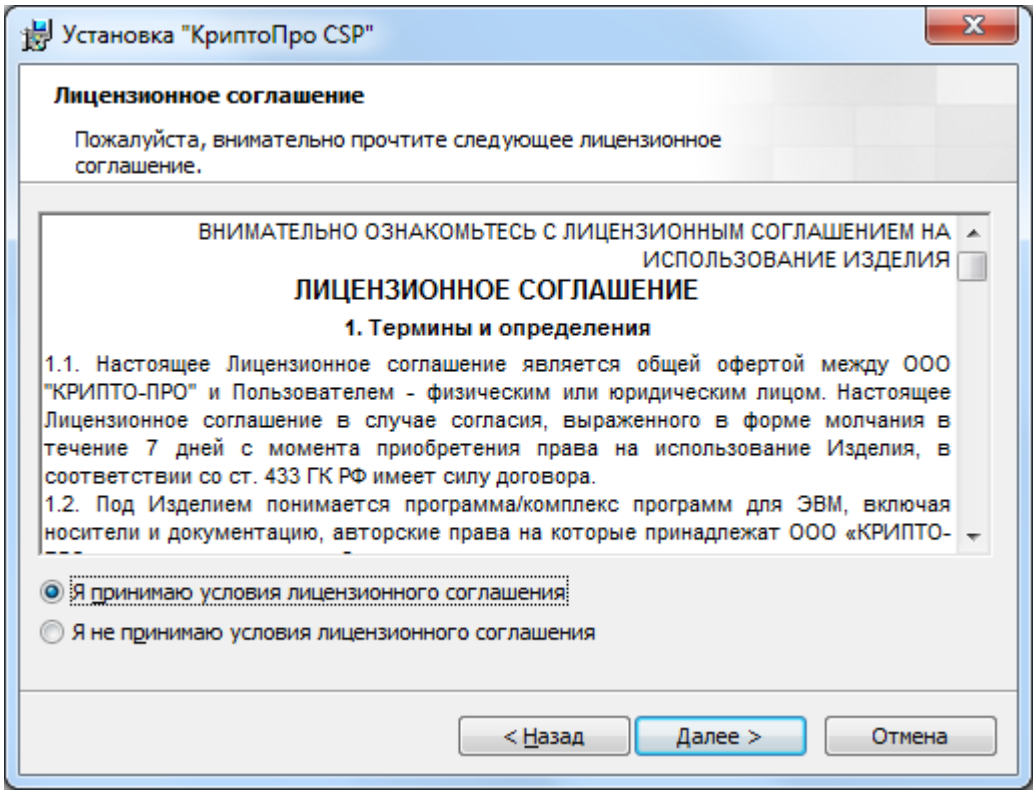
Внимание! Если на рабочее место пользователя установлен несертифицированный криптопровайдер, то рекомендуется его удалить.

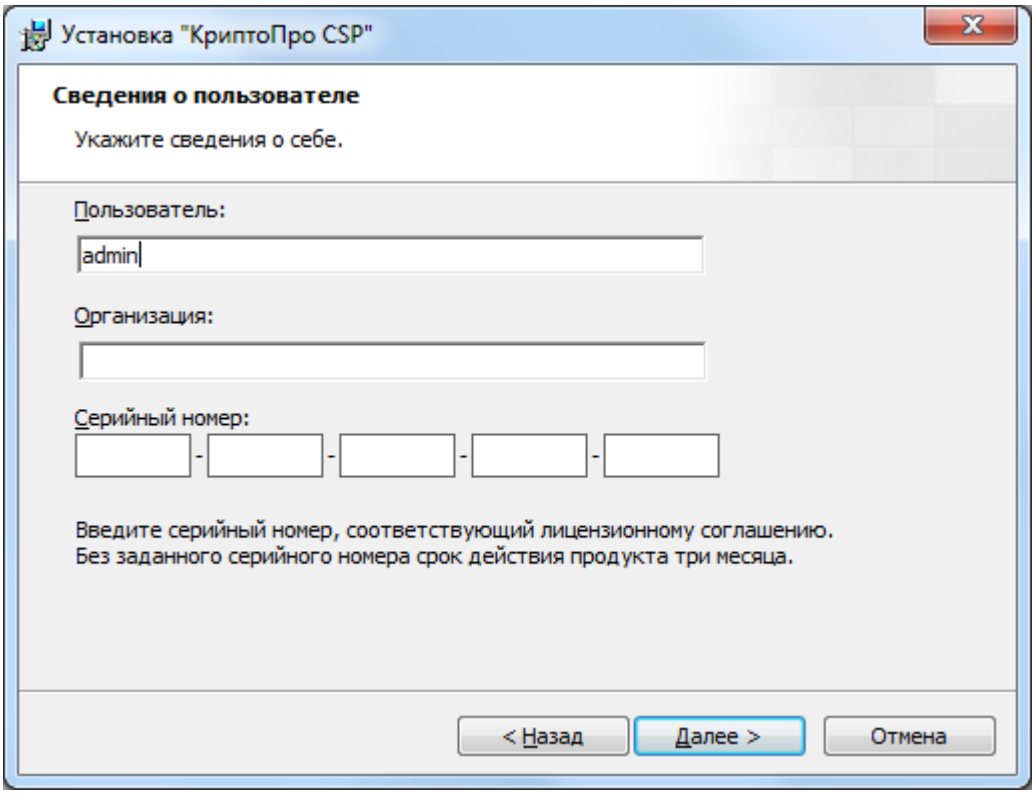
Если на рабочее место пользователя установлено программное обеспечение КриптоПро CSP версии 3.0, его необходимо удалить.

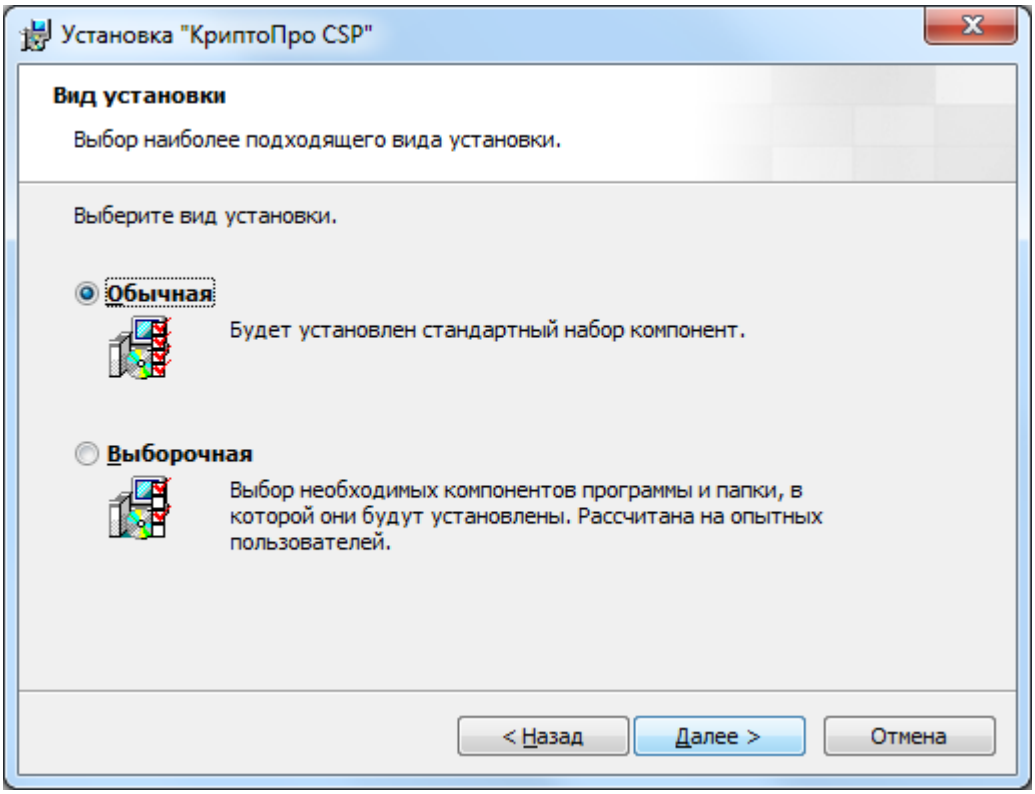
Загрузите дистрибутив КриптоПро CSP 3.6 с официального сайта по ссылке http://www.cryptopro.ru/products/csp/overview.

При установке КриптоПро CSP 3.6 следуйте инструкциям мастера установки:

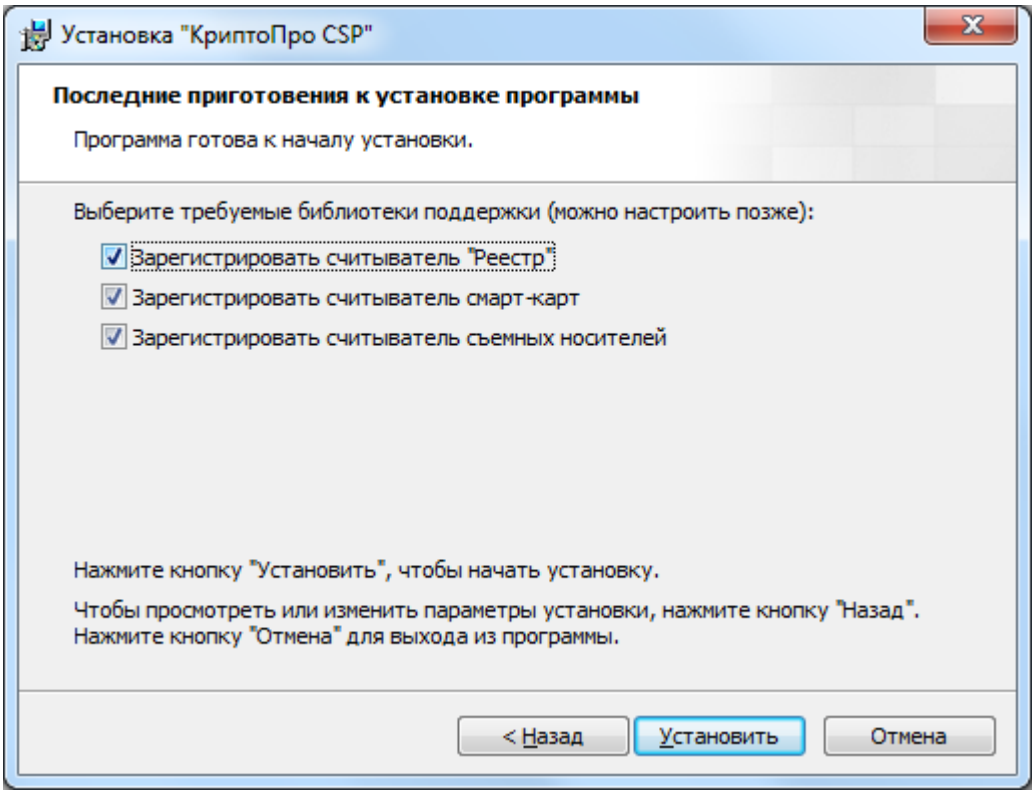


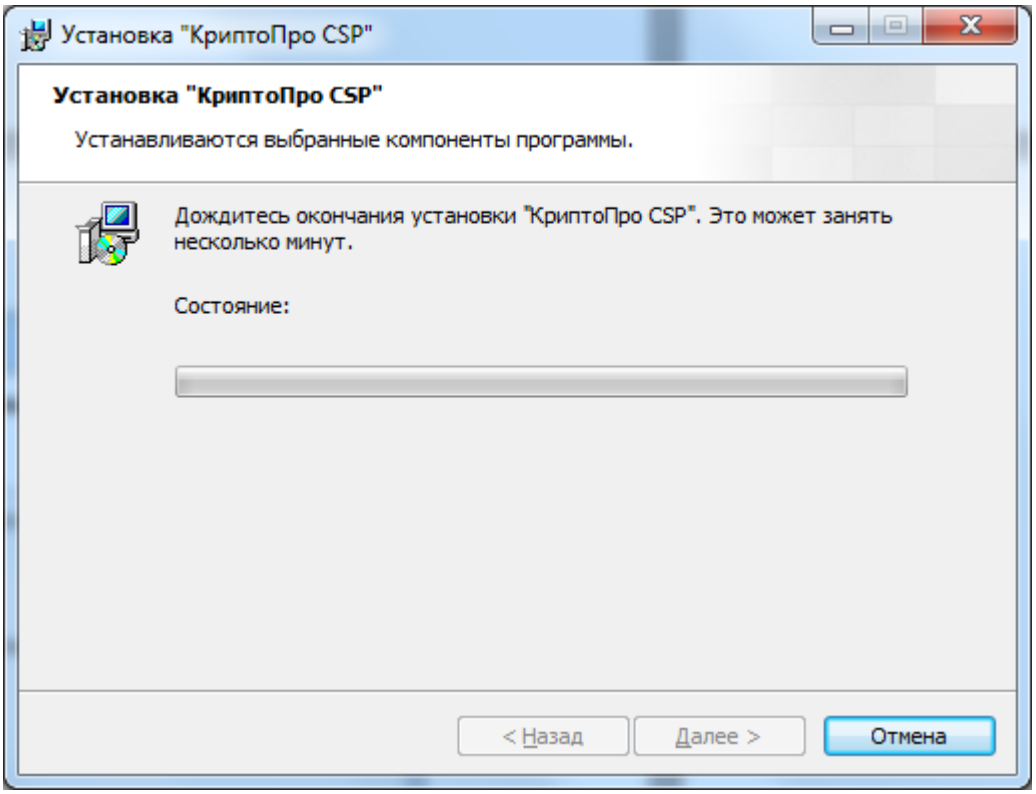

Установка "КриптоПро CSP"
Лицензионное соглашение
Пожалуйста, внимательно прочтите следующее лицензионное соглашение.
ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ С ЛИЦЕНЗИОННЫМ СОГЛАШЕНИЕМ НА ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ
ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ
1. Термины и определения
1.1. Настоящее Лицензионное соглашение является общей офертой между ООО "КРИПТО-ПРО" и Пользователем - физическим или юридическим лицом. Настоящее Лицензионное соглашение в случае согласия, выраженного в форме молчания в течение 7 дней с момента приобретения права на использование Изделия, в соответствии со ст. 433 ГК РФ имеет силу договора.
1.2. Под Изделием понимается программа/комплекс программ для ЭВМ, включая носители и документацию, авторские права на которые принадлежат ООО «КРИПТО-
Я принимаю условия лицензионного соглашения
Я не принимаю условия лицензионного соглашения
< Назад
Далее >
Отмена

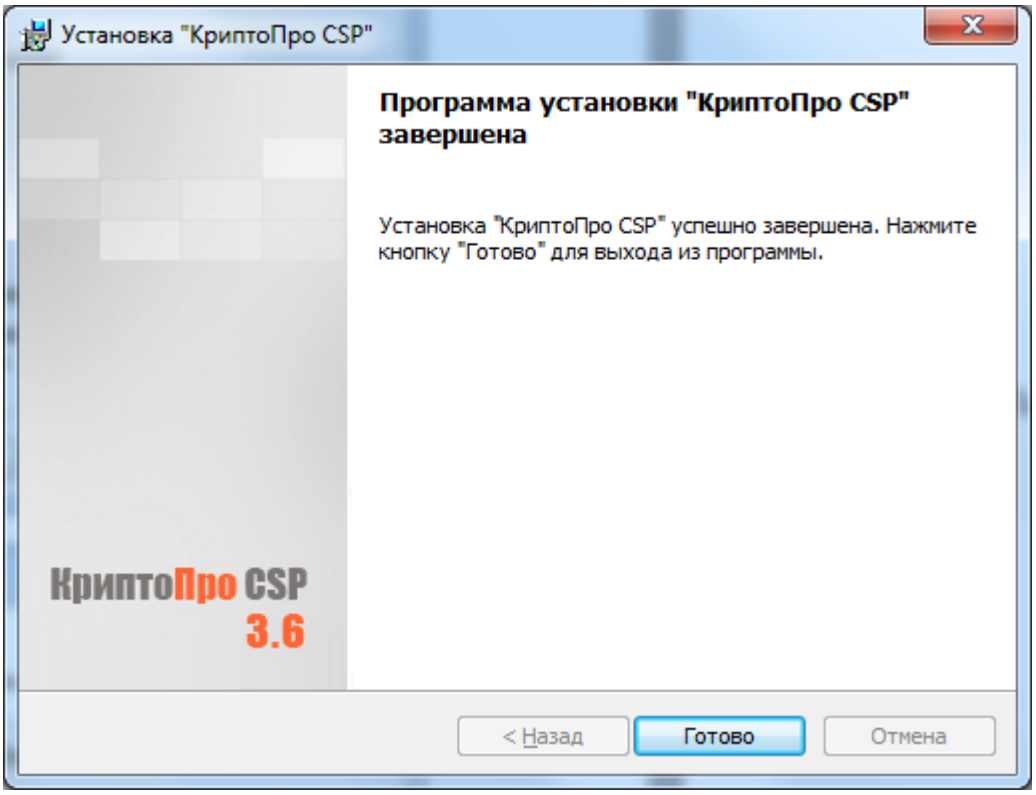

Установка "КриптоПро CSP"
Сведения о пользователе
Укажите сведения о себе.
Пользователь:
admin
Организация:
Серийный номер:
Введите серийный номер, соответствующий лицензионному соглашению.
Без заданного серийного номера срок действия продукта три месяца.
< Назад
Далее >
Отмена



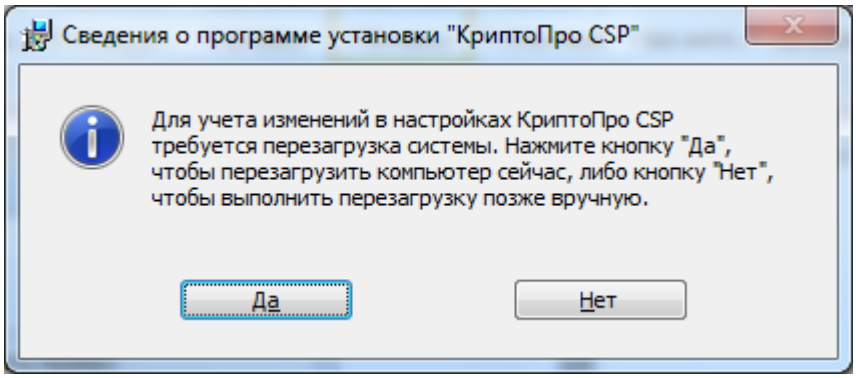
В блоке «Требуемые библиотеки поддержки» необходимо выбрать все опции:







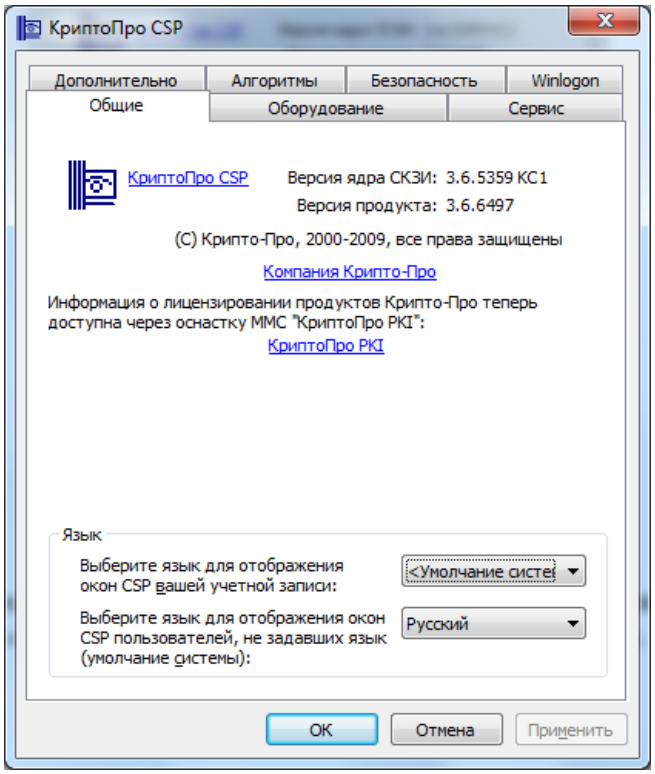
После завершения установки обязательно перезагрузите компьютер.



Приложение 3. Установка личного КСКПЭП с помощью КриптоПро CSP.

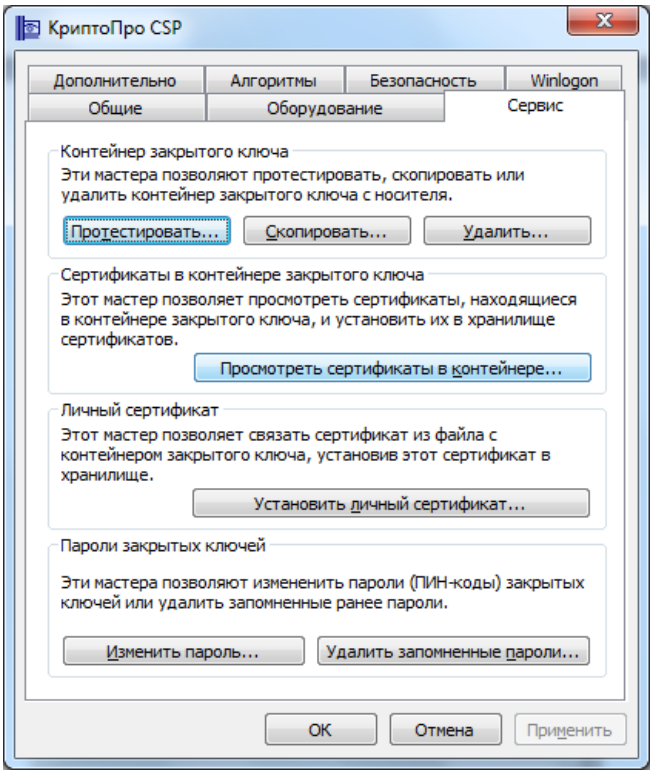
Подключите ключевой носитель с личным КСКПЭП и ключем ЭП (дискету, eToken или т.п.) к компьютеру.

В меню «Пуск» выберите Программы -> Крипто-Про -> КриптоПро CSP:

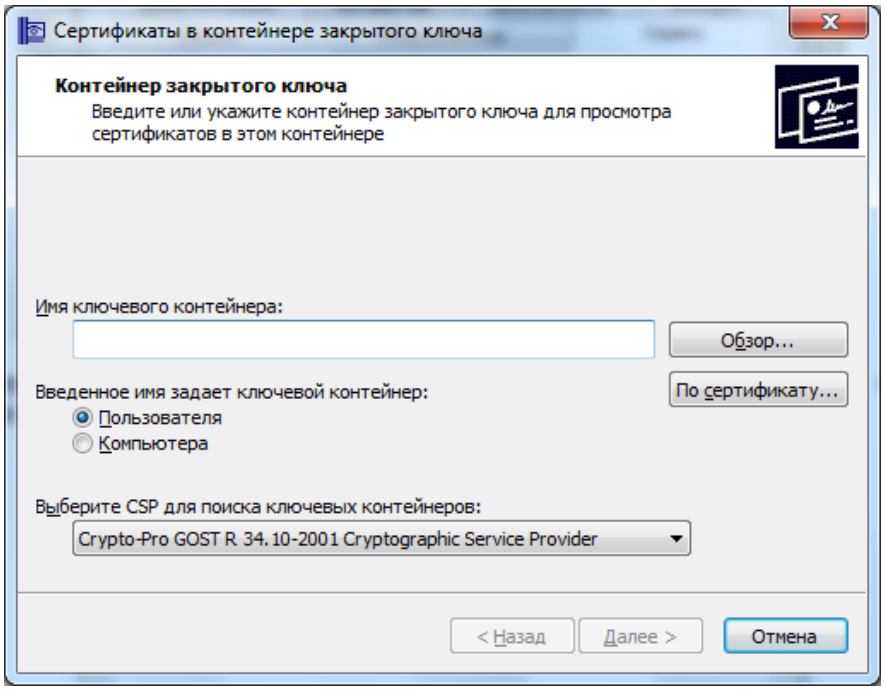


Вариант установки 1 (с носителя КСКПЭП):

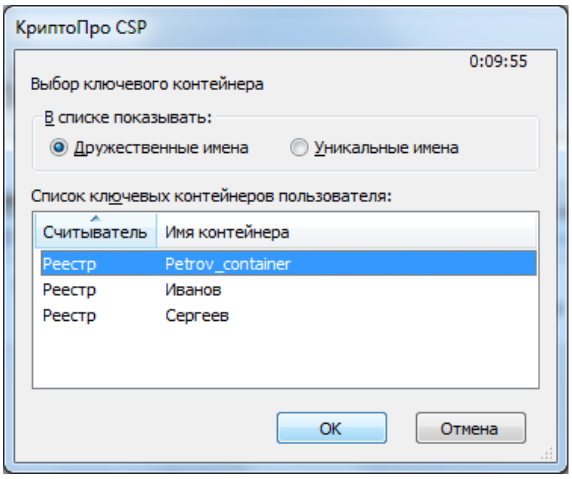
На вкладке «Сервис» нажмите «Посмотреть сертификаты в контейнере…»:



Нажмите «Обзор…» рядом с полем «Имя ключевого контейнера»:



Выберите ключевой контейнер, соответствующий подключенному носителю электронной подписи:

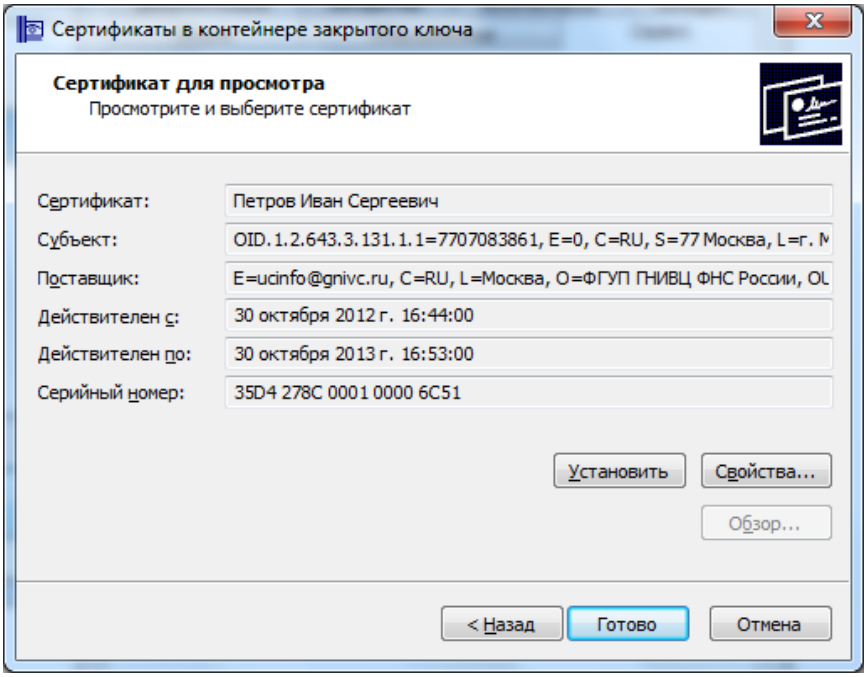


Нажмите «ОК».

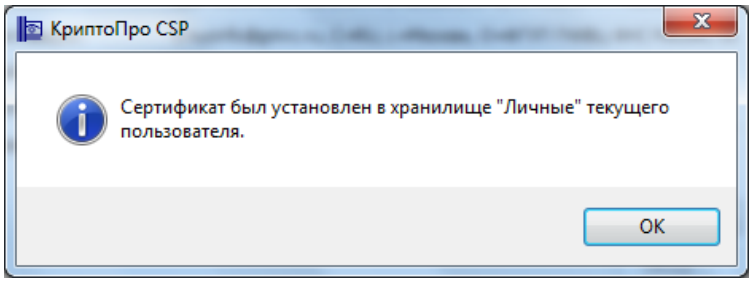
После того, как имя контейнера отобразится в поле «Имя ключевого контейнера», нажмите «Далее».

Внимание! Если при выборе ключевого контейнера появляется окно с предупреждением о том, что истек срок действия лицензии КриптоПро CSP, то необходимо обновить лицензию, иначе работа с сервисом будет невозможна.

Нажмите «Установить»:



Нажмите «ОК»:

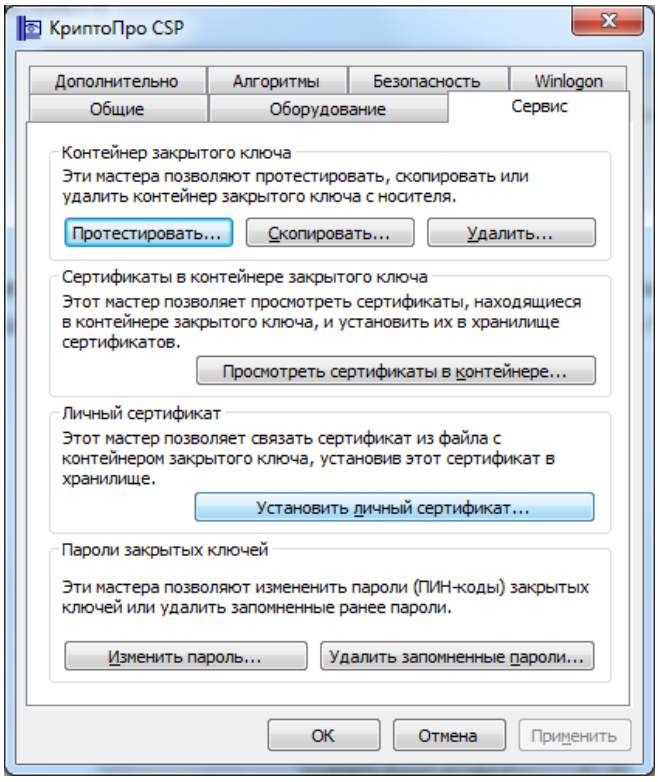


При необходимости введите пароль/пин-код, заданный для доступа к ключу ЭП на ключевом носителе.

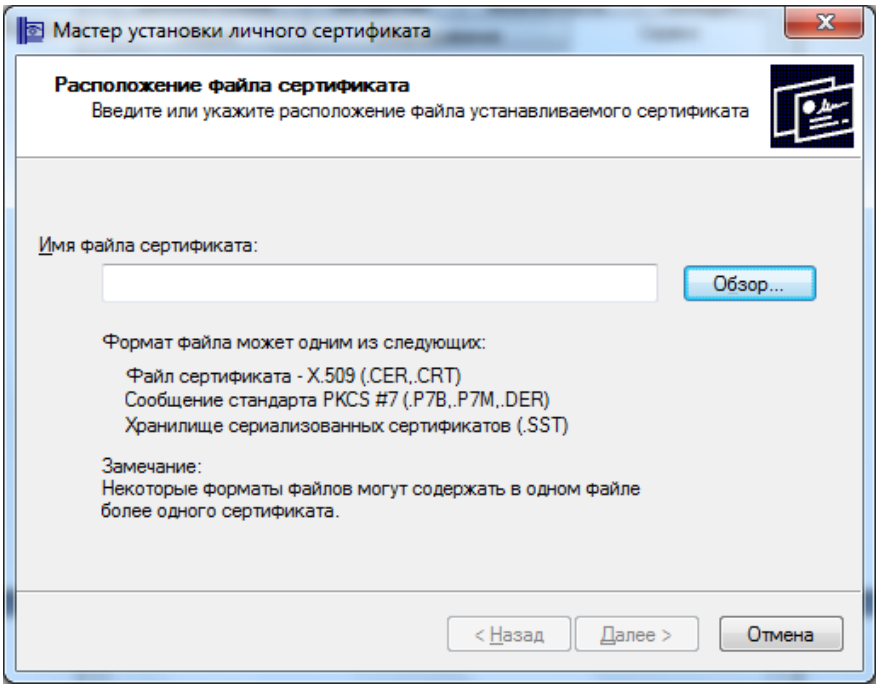
Вариант установки 2 (из файла сертификата):

Для установки понадобится файл сертификата (файл с расширением .cer). Он может находиться, например, на дискете или на жестком диске компьютера (если Вы делали копию сертификата или Вам присылали его по электронной почте). Также файл сертификата можно экспортировать из хранилища Личные.

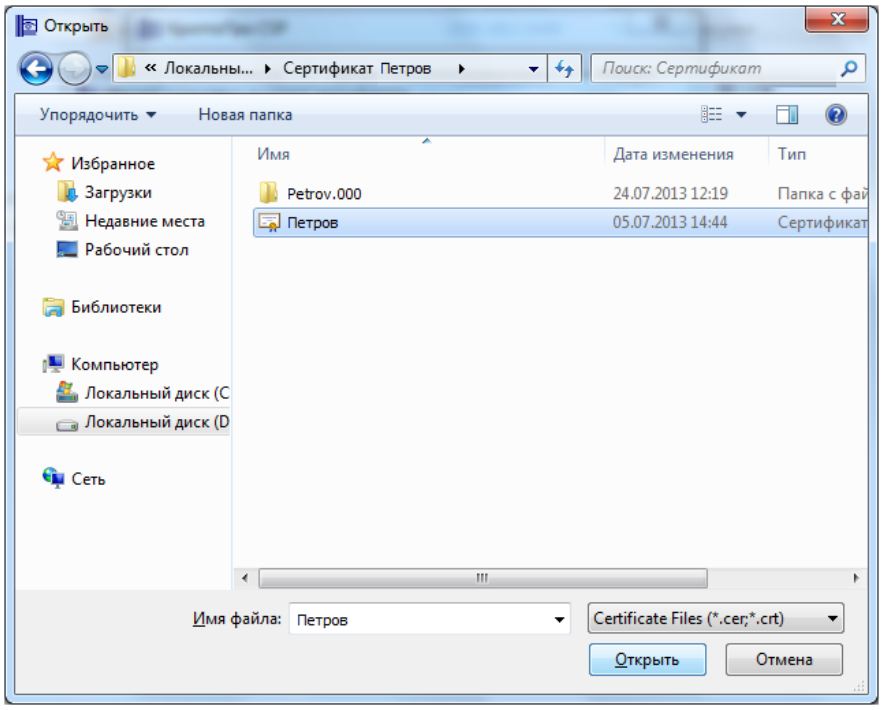
На вкладке «Сервис» нажмите кнопку «Установить личный сертификат…»:



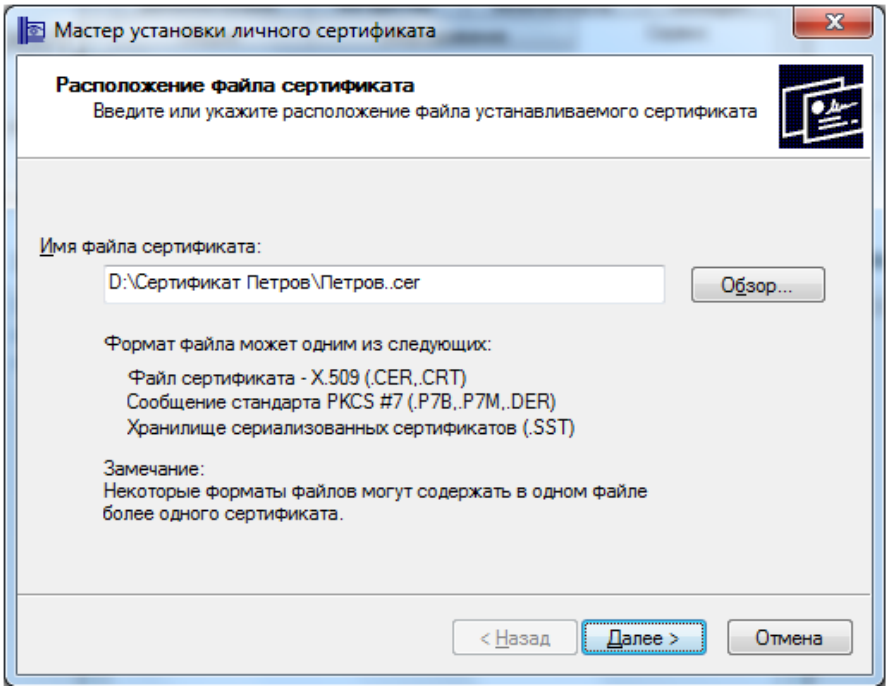
В окне «Мастер установки личного сертификата» нажмите кнопку «Обзор» рядом с полем «Имя файла сертификата», чтобы выбрать файл сертификата:



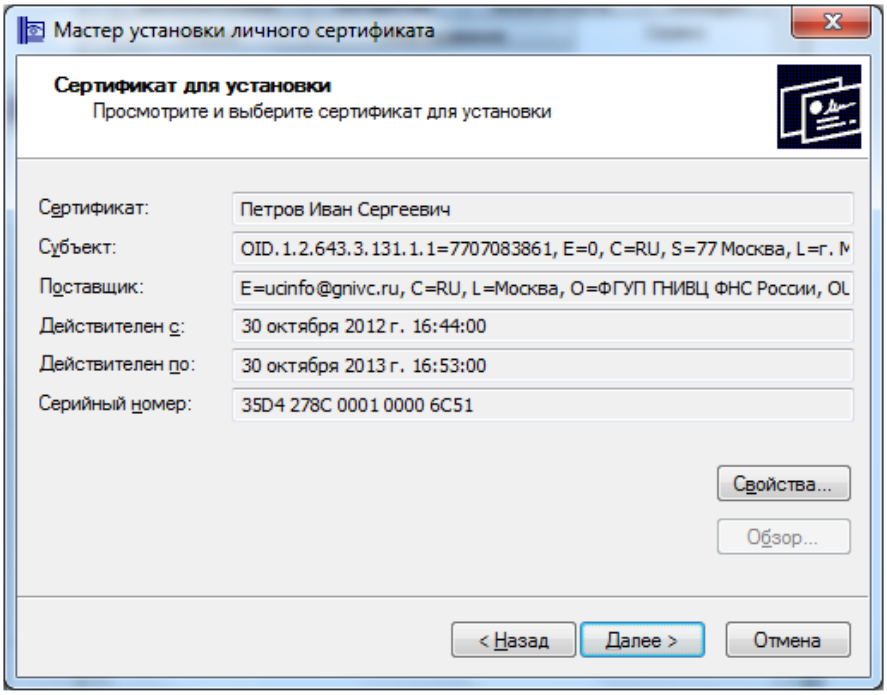
Укажите путь к сертификату (файл с расширением .cer) и нажмите на кнопку «Открыть»:



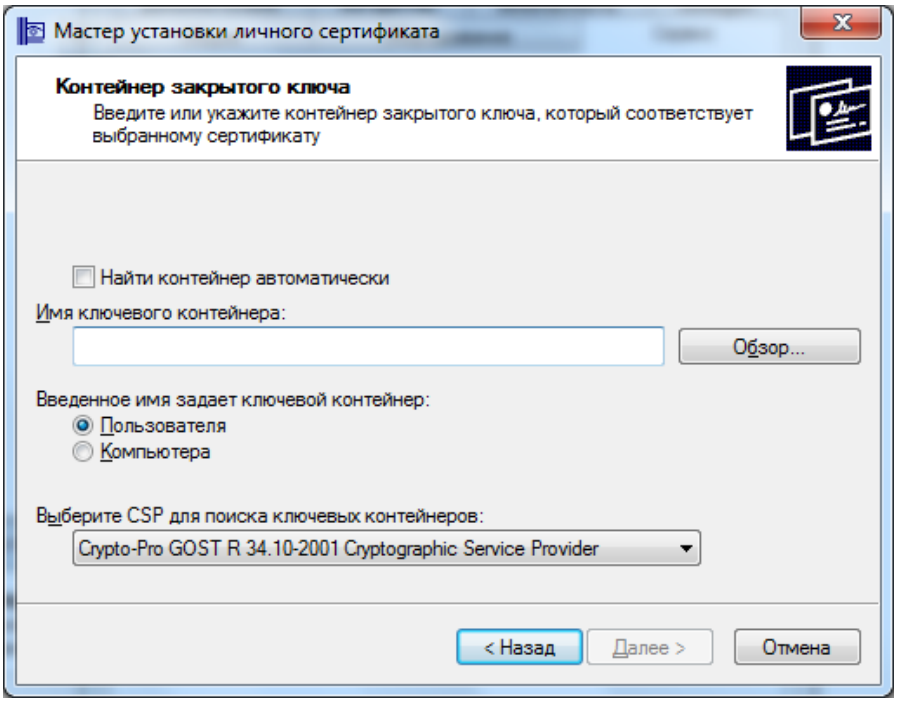
В поле «Имя файла сертификата» отобразится выбранный сертификат, нажмите «Далее».



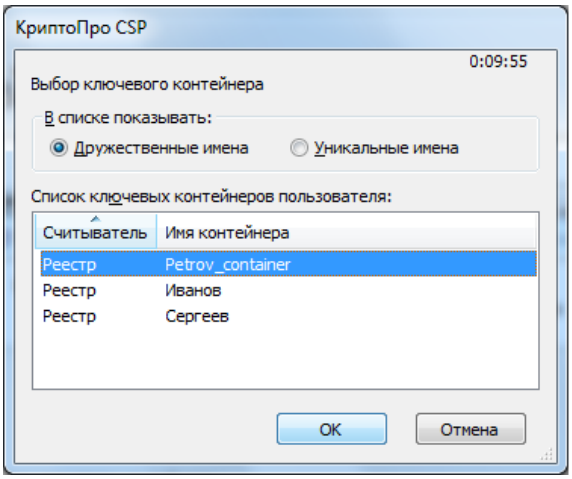
В окне «Сертификат для установки» кликните по кнопке «Далее».



Выберите «Обзор», чтобы указать соответствующий контейнер закрытого ключа.

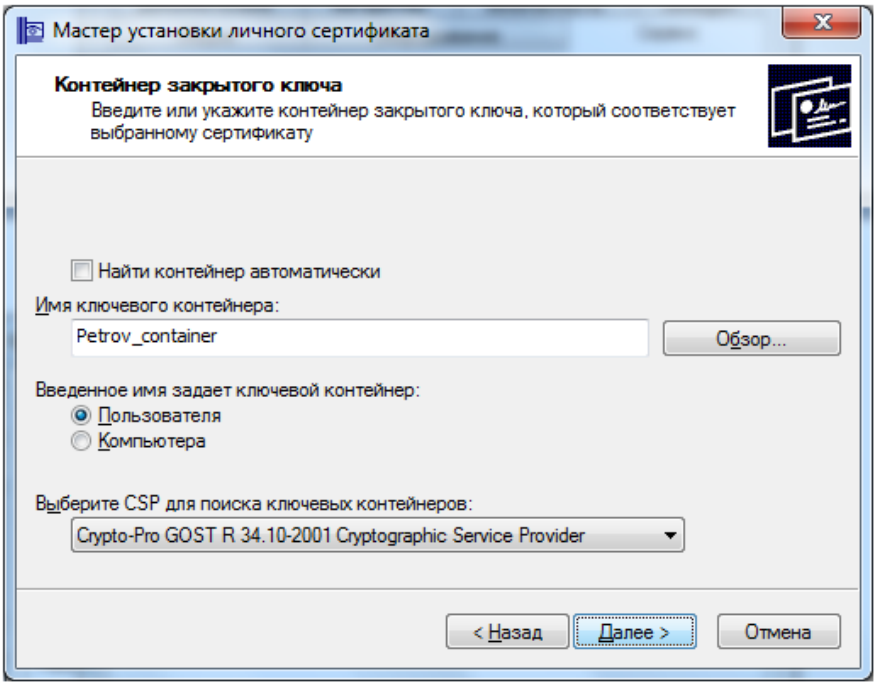


Установите опцию «Найти контейнер автоматически» или выберите нужный ключевой контейнер через кнопку «Обзор». Нажмите «ОК».

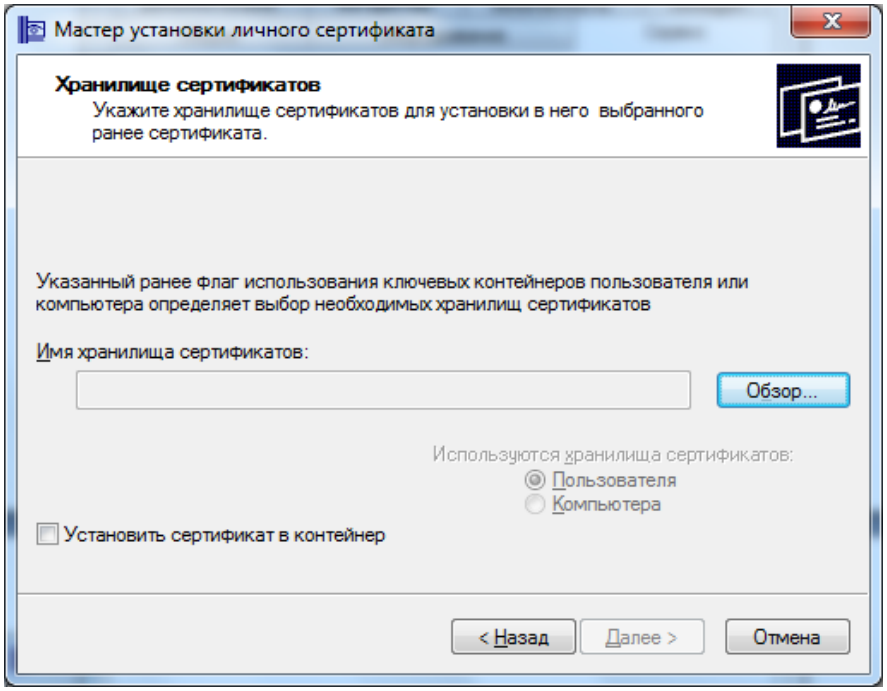


После того, как имя контейнера отобразится в поле «Имя ключевого контейнера», нажмите «Далее».

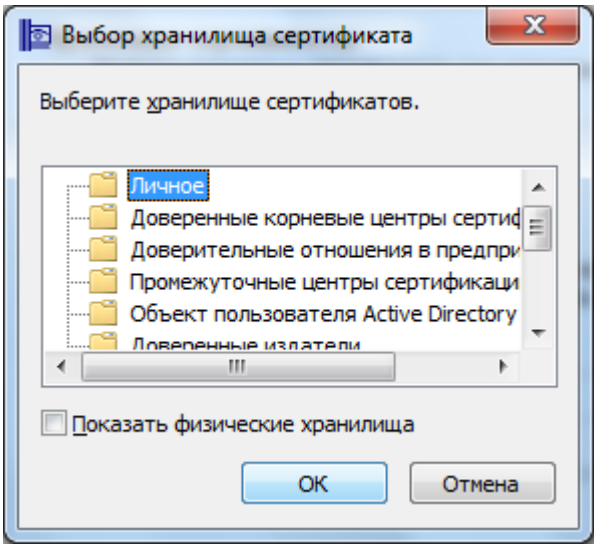
Примечание: Если в списке нет Вашего ключевого контейнера, например, если Вы используете eToken, то выполните Шаг 1. Установка драйвера носителя КСКПЭП.



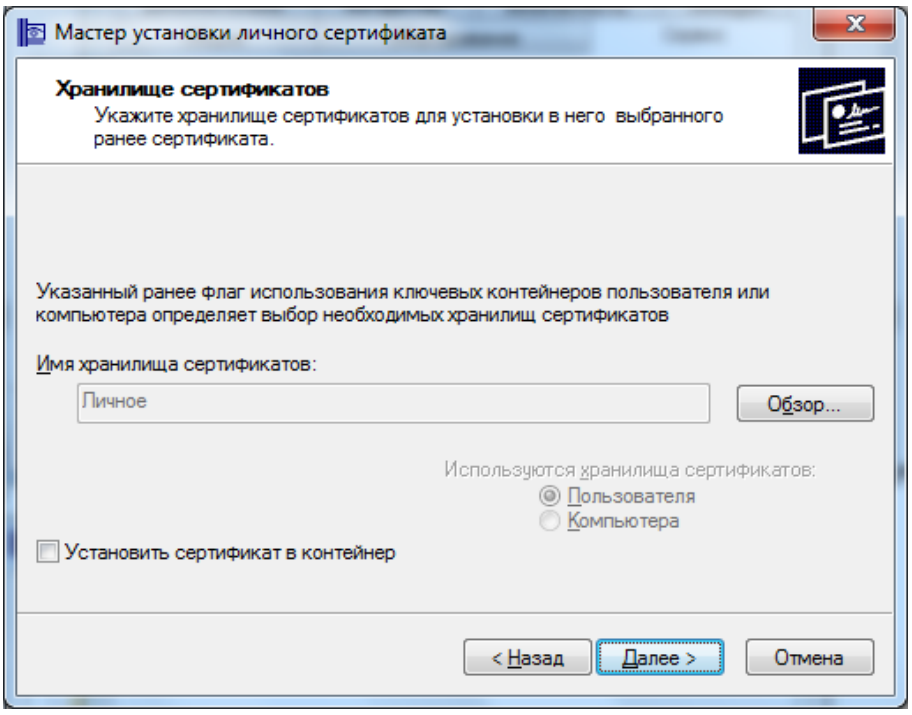
В окне «Выбор хранилища сертификатов» кликните по кнопке «Обзор».



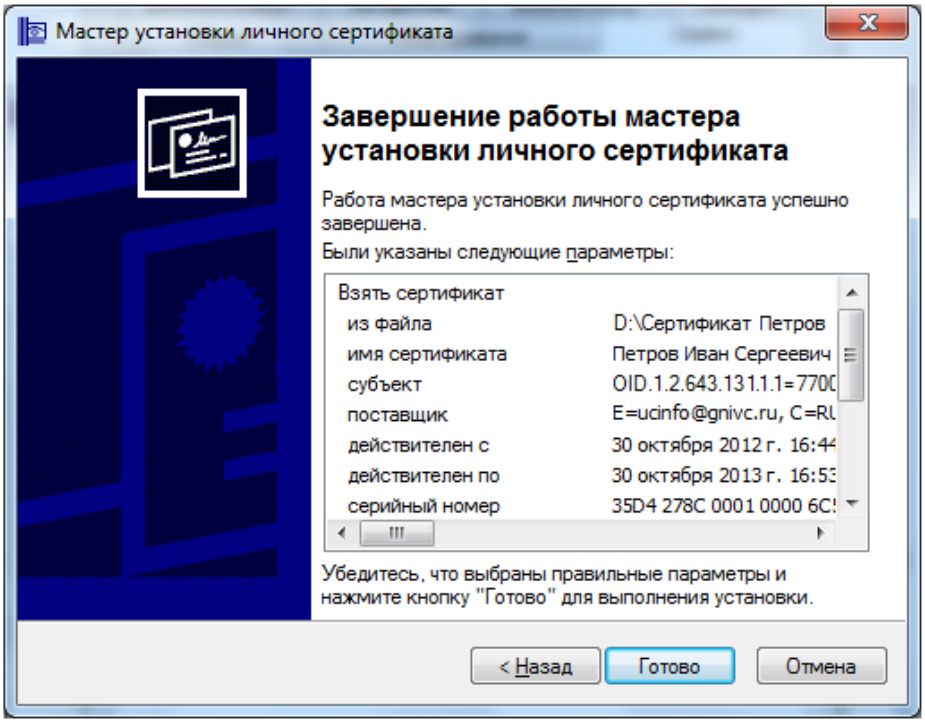
Выберите хранилище «Личное» и нажмите «ОК».



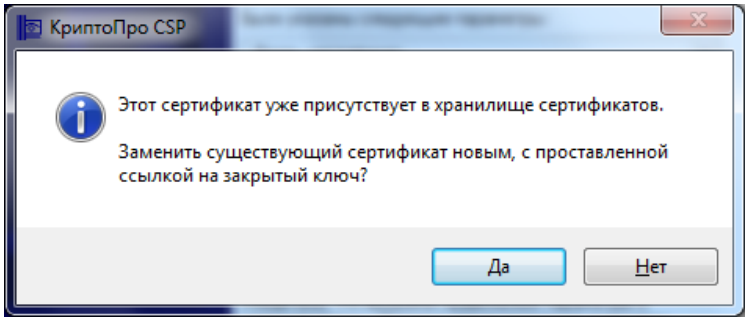
После выбора хранилища нажмите на кнопку «Далее».



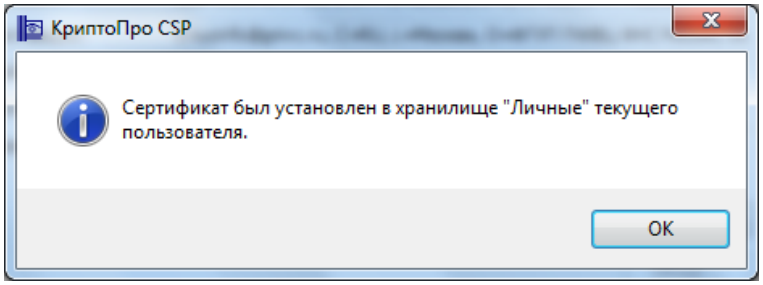
Затем нажмите на кнопку «Готово».



После нажатия на кнопку «Готово» может появиться такое сообщение: «Этот сертификат уже присутствует в хранилище сертификатов. Заменить существующий сертификат новым, с проставленной ссылкой на закрытый ключ?». В таком случае необходимо выбрать «Да».



В сообщении об успешной установке нажмите «ОК». Если у Вас отобразилось сообщение «Этот сертификат уже присутствует в хранилище сертификатов. Заменить существующий сертификат новым, с проставленной ссылкой на закрытый ключ?», то сообщение «Сертификат был установлен в хранилище «Личные» текущего пользователя» может не появиться.



Внимание! Если при установке личного КСКПЭП в хранилище сертификатов «Личные» появляется сообщение «Закрытый ключ на указанном контейнере не

соответствует открытому ключу в сертификате. Выберите другой ключевой контейнер», или выберите опцию «Найти контейнер автоматически». При повторном появлении сообщения Вам потребуется перейти в закладку «Сервис» и нажать кнопку «Удалить запомненные пароли…», в появившемся окне «Удаление запомненных паролей» проставить галки для пунктов «Удалить все запомненные пароли закрытых ключей:», «Удалить информацию об использованных съемных носителях:» и нажать «ОК». Далее повторить действия по установке личного КСКПЭП.

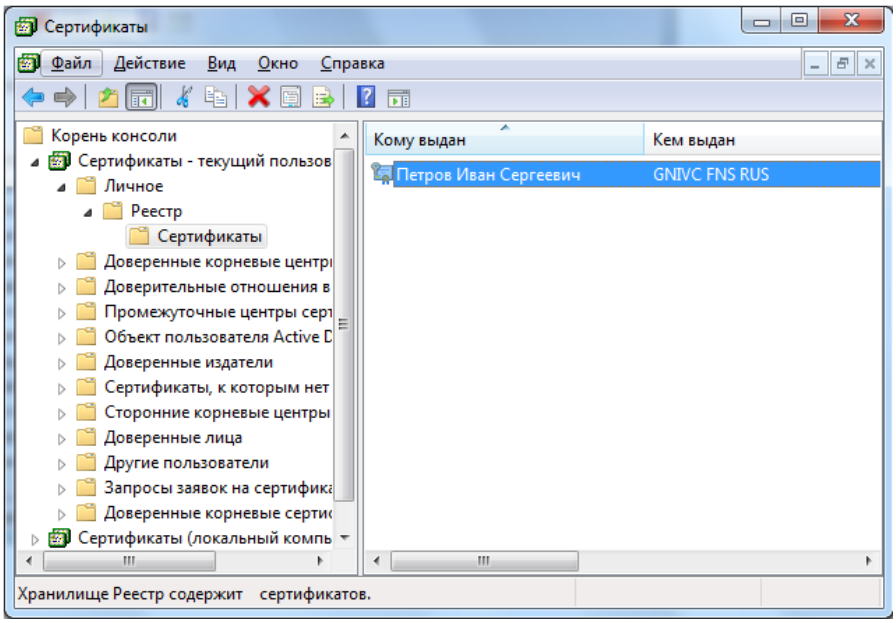
1. Запустите редактор реестра (Пуск/ввести в поисковую строку "regedit"/ ввод).
2. Перейдите в следующую ветвь редактора реестра: HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\USERS, найдите ветку с названием S-1-5-21-887842899-779666540-1964827887-17186 (где S-1-5-21-887842899-779666540-1964827887-17186- SID пользователя).
3. Зайдите в KeyDevices и удалите там passwords.
4. Удалите содержимое папки C:\Documents and Settings\имя пользователя \Application Data\Microsoft\SystemCertificates\My\Keys.
5. Установите заново сертификат.

Если выполнение описанных выше действий, не решило Вашу проблему, обратитесь в Аккредитованный удостоверяющий центр, издавший личный КСКПЭП.

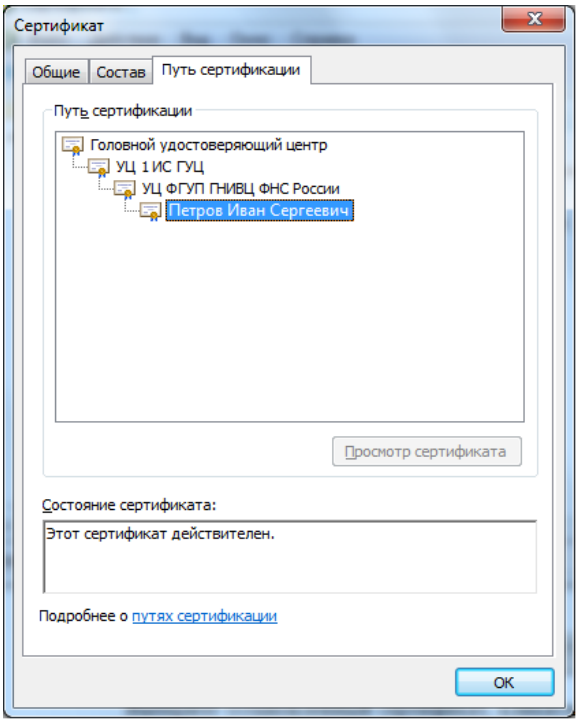
Приложение 4. Проверка установки сертификатов

Откройте хранилище сертификатов. Для этого если Вы используете КриптоПро CSP в меню «Пуск» выберите Программы -> Крипто-Про -> Сертификаты или запустите консоль Пуск->Выполнить MMC и откройте оснастку «Сертификаты».

Далее откройте папку «Сертификаты – текущий пользователь» -> Личные -> Реестр -> Сертификаты:



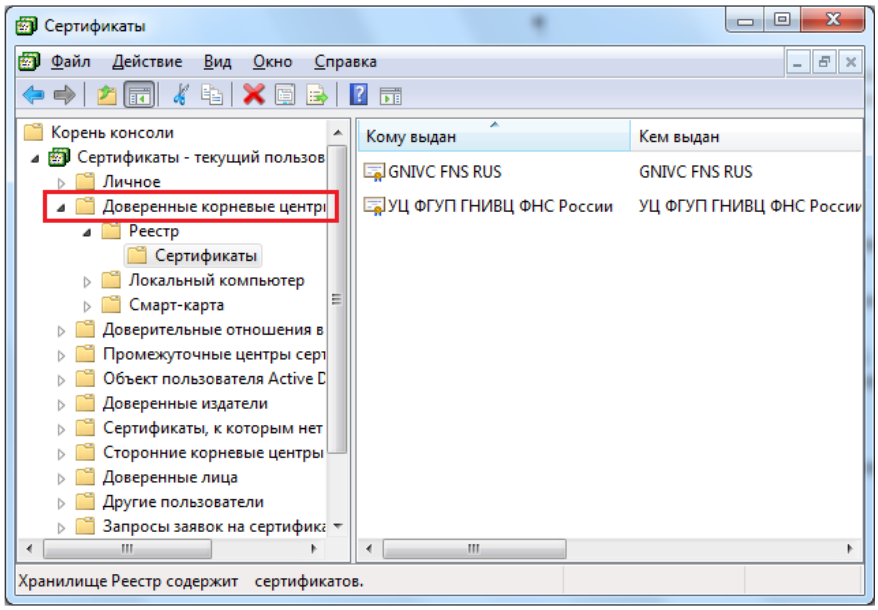
Выберите установленный сертификат, кликнув по нему два раза левой кнопкой мыши. Перейдите на вкладку «Путь сертификации»:



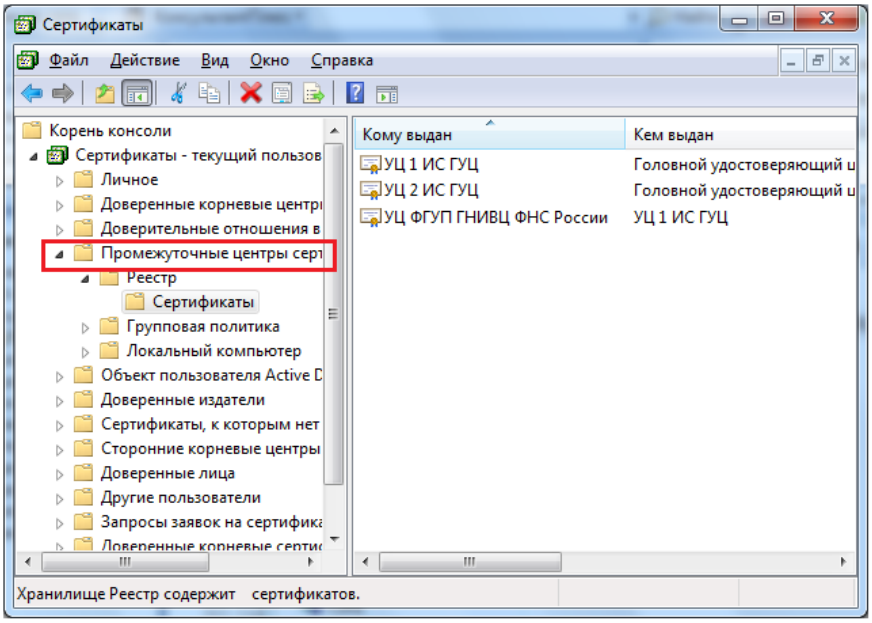
На вкладке «Путь сертификации» должна отображаться цепочка сертификатов, с помощью которых устанавливается доверие. Верхний сертификат должен быть корневым.

В поле **«Состояние сертификата»** должно отображаться сообщение о действительности сертификата.

Корневой сертификат «УЦ ФГУП ГНИВЦ ФНС России», корневой сертификат Ведомственного УЦ ФНС России и корневой сертификат АУЦ, выдавшего личный КСКПЭП, будут размещаться в хранилище сертификатов **«Доверенные корневые центры сертификации»**:



Остальные сертификаты цепочки будут размещаться в хранилище сертификатов **«Промежуточные центры сертификации»**:


Сертификаты
Файл Действие Вид Окно Справка
Корень консоли
Сертификаты - текущий пользов
Личное
Доверенные корневые центр
Доверительные отношения в
Промежуточные центры серт
Реестр
Сертификаты
Групповая политика
Локальный компьютер
Объект пользователя Active D
Доверенные издатели
Сертификаты, к которым нет
Сторонние корневые центры
Доверенные лица
Другие пользователи
Запросы заявок на сертифика
Кому выдан
Кем выдан
УЦ 1 ИС ГУЦ
Головной удостоверяющий ц
УЦ 2 ИС ГУЦ
Головной удостоверяющий ц
УЦ ФГУП ГНИВЦ ФНС России
УЦ 1 ИС ГУЦ
Хранилище Реестр содержит сертификатов.