

Инструкция по установке и настройке компонентов для работы с сертификатом ЭП

Сервис Личный кабинет клиента

ОГЛАВЛЕНИЕ

НЕОБХОДИМЫЕ КОМПОНЕНТЫ	3
ПОРЯДОК УСТАНОВКИ И НАСТРОЙКИ	4
УСТАНОВКА СКЗИ КРИПТОПРО CSP ВЕРСИИ 4.0.....	4
УСТАНОВКА КРИПТОПРО BROWSER PLUG-IN	10
Настройка КриптоПро ЭЦП Browser plug-in при использовании браузера IE	11
Настройка КриптоПро ЭЦП Browser plug-in при использовании браузера Chrome версии 45 и выше	12
УСТАНОВКА ДРАЙВЕРА КЛЮЧЕВОГО НОСИТЕЛЯ	13
Установка драйвера ключевого носителя Rutoken.....	13
Установка драйвера ключевого носителя ESMART Token	15
Установка драйвера ключевого носителя eToken	21
УСТАНОВКА СЕРТИФИКАТА КЛЮЧА ПОДПИСИ	24
УСТАНОВКА КОРНЕВОГО СЕРТИФИКАТА.....	28
НАСТРОЙКА БРАУЗЕРА INTERNET EXPLORER	31
ДОБАВЛЕНИЕ СЕРТИФИКАТА В КАРТОЧКУ ПОЛЬЗОВАТЕЛЯ СЕРВИСА.....	34
Экспорт сертификата с ключевого носителя	34
Загрузка сертификата пользователю системы	41

НЕОБХОДИМЫЕ КОМПОНЕНТЫ

Для корректной работы системы необходимо, чтобы на рабочем месте пользователя было установлено следующее программное обеспечение:

1. Лицензионная операционная система (с последними пакетами обновлений):
 - Windows XP SP3;
 - Windows Vista SP2 и выше;
 - Windows Server 2003 и выше;
 - Windows Server 2008 и выше;
 - Windows 7;
 - Windows 8;
 - Windows 8.1;
 - Windows Server 2012 и выше;
 - Windows 10.
2. .NET Framework 3.5 Service Pack 1 (для работы с Компонентом Сфера).
3. Интернет браузер:
 - Internet Explorer версии 9.0 и выше;
 - Mozilla Firefox версии 30 и выше;
 - Google Chrome версии 35 и выше.

Примечание: Корректная работа в других браузерах возможна, но не гарантирована.

4. СКЗИ КриптоПро CSP версии 3.6 и выше;

Примечание: Для корректной установки и работы СКЗИ КриптоПро CSP необходимо использовать версию и разрядность программы, совместимую с операционной системой, установленной на рабочем месте пользователя.

Подробнее с информацией о совместимости версий можно ознакомиться, перейдя по ссылке: <https://www.cryptopro.ru/products/csp/compare>.

Сертификация СКЗИ КриптоПро CSP версии 4.0 в настоящий момент не распространяется на ОС Windows 10.

5. КриптоПро ЭЦП Browser plug-in версии 1.5 и выше.

Примечание: Для корректной работы в браузере Google Chrome версии 45 и выше необходимо использовать КриптоПро ЭЦП Browser plug-in версии 2.0.

6. Драйвер для защищенного носителя ЭП (если таковой используется):

- Рутокен;
- eToken;
- ESMART Token и другие.

Также необходимо наличие USB-порта и доступа в Интернет.

Компоненты 1-3 должны быть установлены на компьютер пользователя самостоятельно, в настоящем руководстве рассматривается только установка компонентов 4-6 и настройка браузера Internet Explorer.

Все необходимые для установки дистрибутивы можно скачать с [сайта](#) в разделе «Поддержка» -> «Скачать» -> «Удостоверяющий центр» или по ссылкам, указанным в инструкции.

ПОРЯДОК УСТАНОВКИ И НАСТРОЙКИ

Установка и настройка компонентов осуществляется в следующем порядке:

1. Установка СКЗИ КриптоПро CSP версии 3.6 и выше (в руководстве рассмотрена установка КриптоПро CSP версии 4.0).
2. Установка и настройка КриптоПро ЭЦП Browser plug-in.
3. Установка драйвера ключевого носителя.
4. Установка сертификата ключа подписи.
5. Установка корневого сертификата Удостоверяющего центра.
6. Настройка браузера (в руководстве рассмотрена настройка Internet Explorer).
7. Добавление сертификата в карточку пользователя системы СФЕРА Курьер.

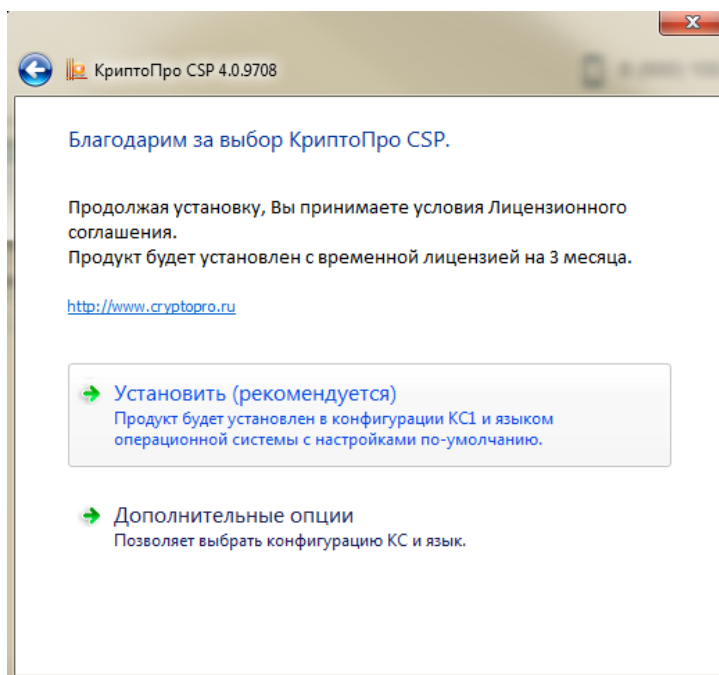
УСТАНОВКА СКЗИ КРИПТОПРО CSP ВЕРСИИ 4.0

Дистрибутив программы СКЗИ КриптоПро CSP можно скачать с сайта производителя, а также по ссылке в разделе «Дистрибутивы для КриптоПро CSP для Windows»:

[КриптоПро CSP 4.0 универсальный установщик \(Windows 10 не поддерживается\)](#)

Для установки программы запустите установочный файл и выберите вариант установки:

- Быстрая установка демо-версии продукта с временной лицензией на 3 месяца с последующим вводом серийного номера из бланка лицензии на использование программного продукта КриптоПро CSP версии 4.0;
- Установка полной версии продукта с вводом серийного номера из бланка лицензии на использование программного продукта КриптоПро CSP версии 4.0.



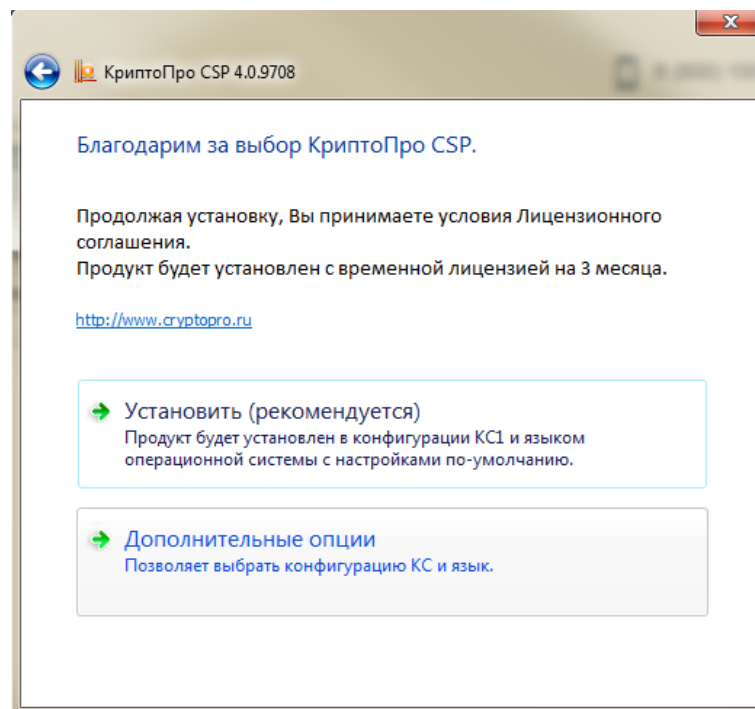
Для быстрой установки выполните следующие шаги:

1. Нажмите кнопку **Установить**.
2. Нажмите кнопку **ОК** в сообщении об успешной установке КриптоПро CSP.

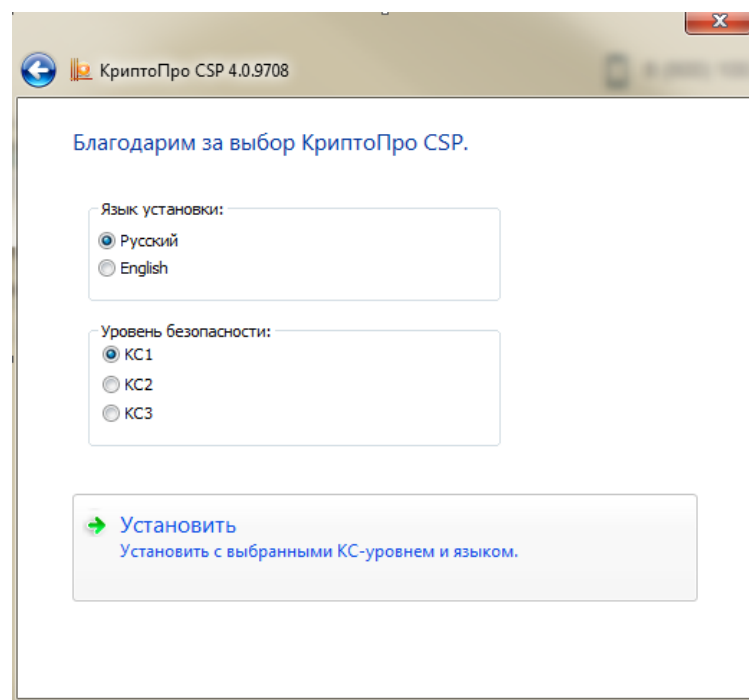
Примечание: По истечении срока действия временной лицензии (3 месяца) необходимо серийный номер, указанный в бланке лицензии на использование программного продукта КриптоПро CSP версии 4.0 в настройках продукта.

Для установки полной версии продукта с вводом серийного номера из лицензии выполните следующие шаги:

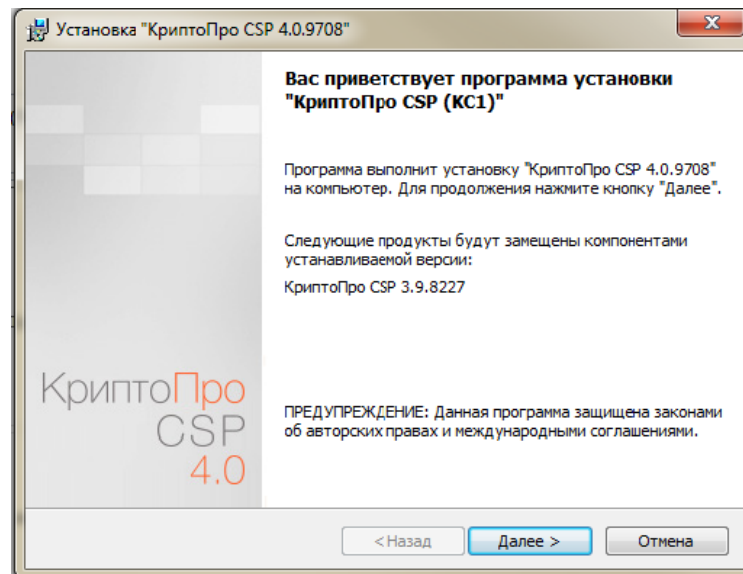
1. Нажмите кнопку **Дополнительные опции**.



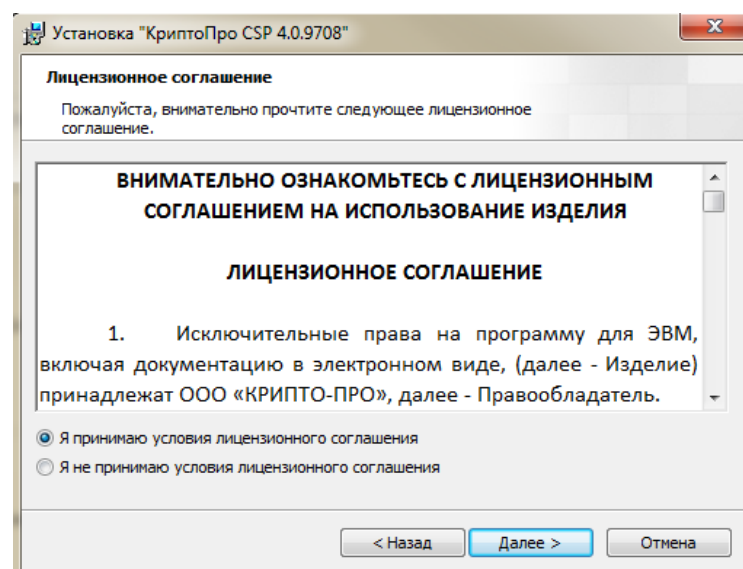
2. Выберите язык установки и уровень безопасности, и нажмите кнопку **Установить**.



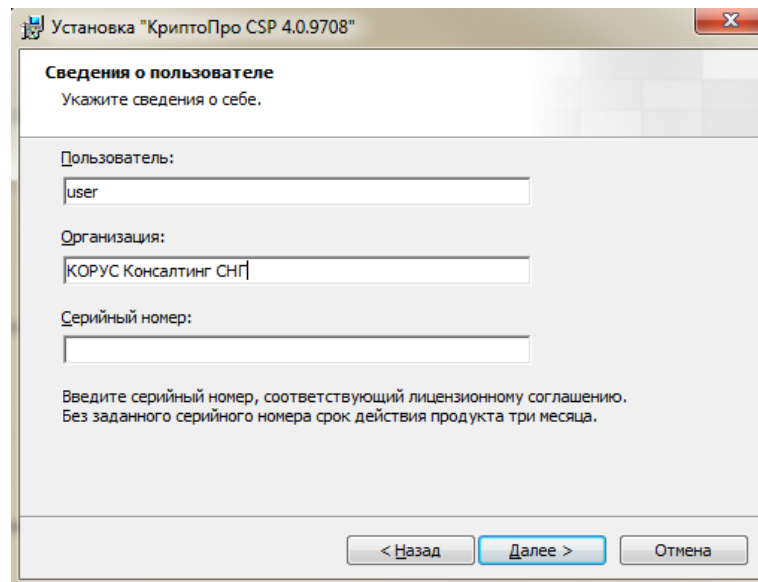
3. Нажмите кнопку **Далее** в окне программы установки.



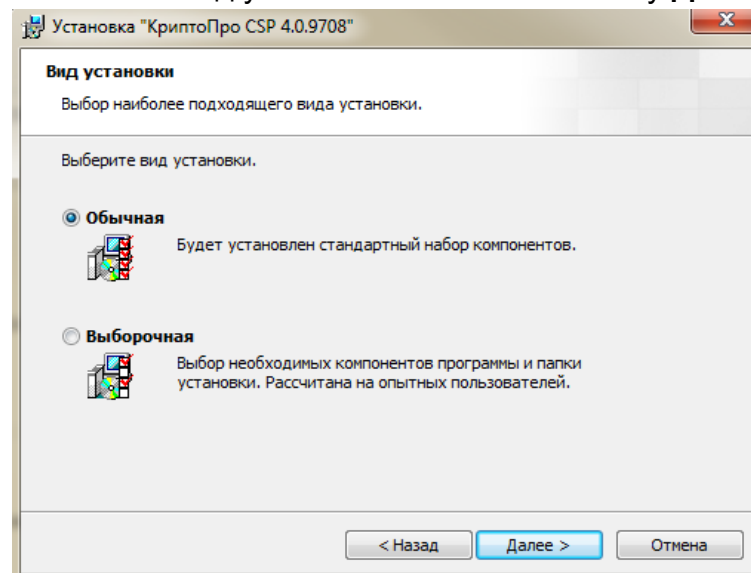
4. Ознакомьтесь с текстом лицензионного соглашения, установите отметку «Я принимаю условия лицензионного соглашения» и нажмите кнопку **Далее**.



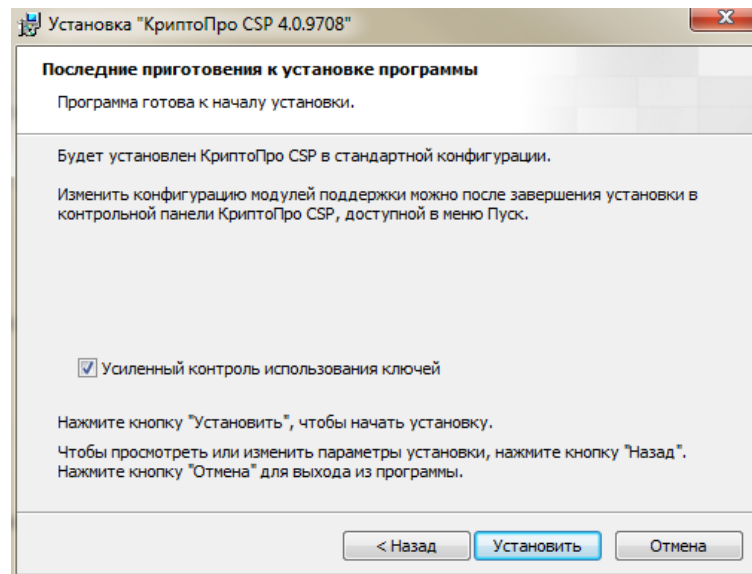
5. В окне «Сведения о пользователе» введите имя, название организации, а также серийный номер, указанный в документе «Лицензия на использование программного продукта КриптоПро CSP версии 4.0» и нажмите кнопку **Далее**.



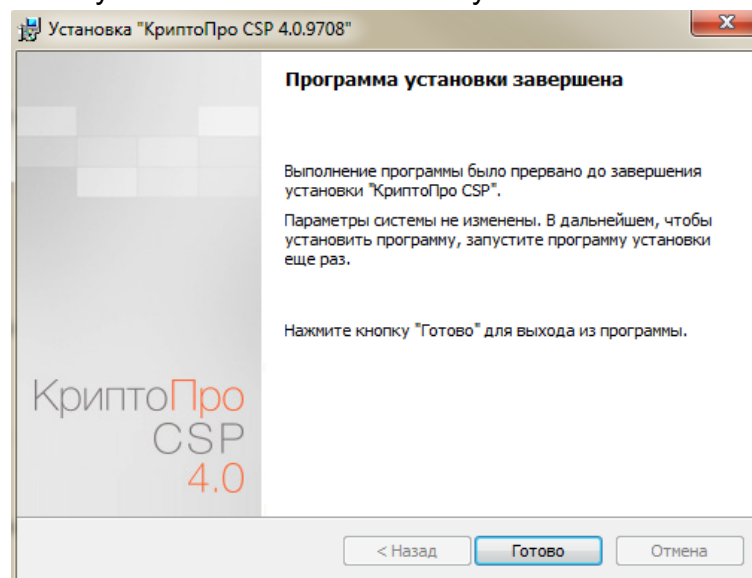
6. Выберите обычный вид установки и нажмите кнопку **Далее**.



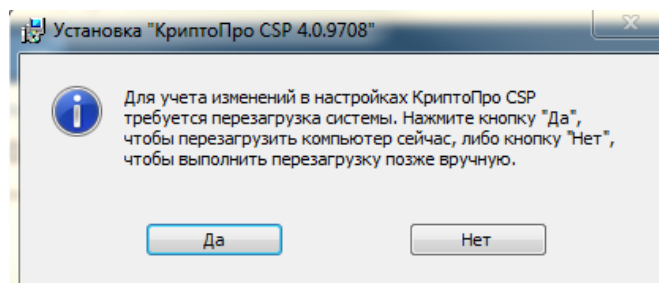
7. Установите отметку «Усиленный контроль использования ключей». Нажмите кнопку **Установить**.



8. По окончании установки нажмите кнопку **Готово**.



9. Нажмите кнопку **Да** для перезагрузки компьютера, чтобы завершить установку.



УСТАНОВКА КРИПТОПРО BROWSER PLUG-IN

КриптоПро ЭЦП Browser plug-in предназначен для создания и проверки электронной подписи на web-страницах. Процесс установки различается для браузеров IE и Chrome.

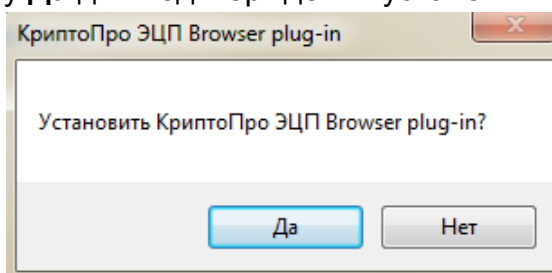
КриптоПро ЭЦП Browser plug-in можно скачать с сайта производителя, а также по следующим ссылкам в разделе «Дистрибутивы для КриптоПро ЭЦП Browser plug-in»:

[Версия 1.5 для пользователей \(автоматическая загрузка версии плагина, соответствующей Вашей ОС\)](#)

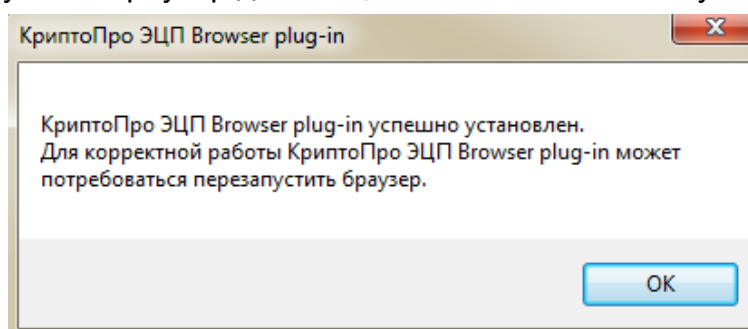
[Версия 2.0 для пользователей \(автоматическая загрузка версии плагина, соответствующей Вашей ОС\)](#)

Для установки КриптоПро ЭЦП Browser plug-in выполните следующие шаги:

1. Запустите исполняемый файл.
2. Подтвердите внесение изменений на компьютере.
3. Нажмите кнопку **Да** для подтверждения установки.



4. Нажмите кнопку **ОК** в сообщении об успешной установке.
5. Перезапустите браузер для того, чтобы изменения вступили в силу.

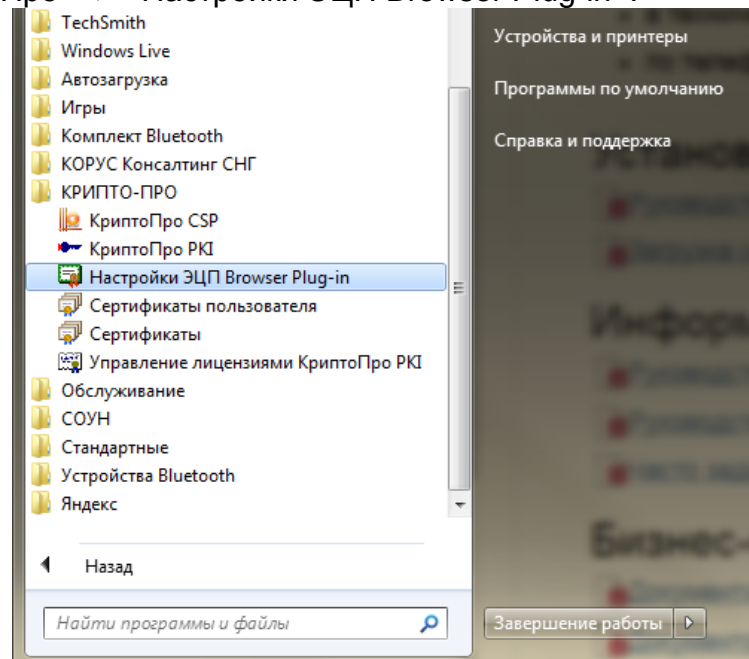


Примечание: В случае некорректной установки, которая проявляется в виде зависания выполнения процесса подписания ЭЦП, удалите скачанный файл плагина и повторите действия по установке.

Настройка КриптоПро ЭЦП Browser plug-in при использовании браузера IE

Для настройки браузера Internet Explorer выполните следующие шаги:

1. Перейдите в меню кнопки **Пуск** и выберите пункты «Все программы» -> «КриптоПро» -> «Настройки ЭЦП Browser Plug-in».



2. В окне браузера откроется страница «Настройки КриптоПро ЭЦП Browser Plug-in».

***Примечание:** Если при открытии страницы браузер заблокировал ее содержимое, необходимо разрешить заблокированное содержимое и обновить страницу.*

3. В графе «Добавить новый» укажите адрес <https://courier.esphere.ru/> и нажмите кнопку **+ Добавить**.

Настройки КриптоПро ЭЦП Browser Plug-in

Список надежных узлов, которые не причинят вред вашему компьютеру и данным. Для заданных веб-узлов КриптоПро ЭЦП Browser Plug-in не будет требовать подтверждения пользователя при открытии хранилища сертификатов, создании подписи или расшифровании сообщения.

Важно! При добавлении веб-узла в список надежных, вы должны быть уверены, что веб-скрипты, загруженные или запущенные с данного веб-узла, не могут нанести вред компьютеру или данным.

Список доверенных узлов

https://courier.esphe +

Сохранить

4. Нажмите кнопку **Сохранить**.

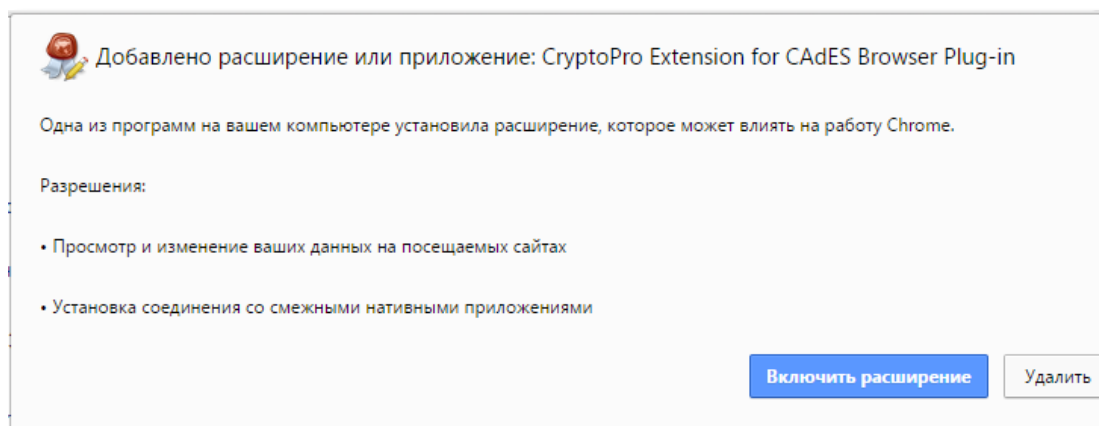
5. Перезапустите браузер.

Для заданного веб-узла КриптоПро ЭЦП Browser Plug-in не будет требовать подтверждения пользователя при открытии хранилища сертификатов и создании подписи.

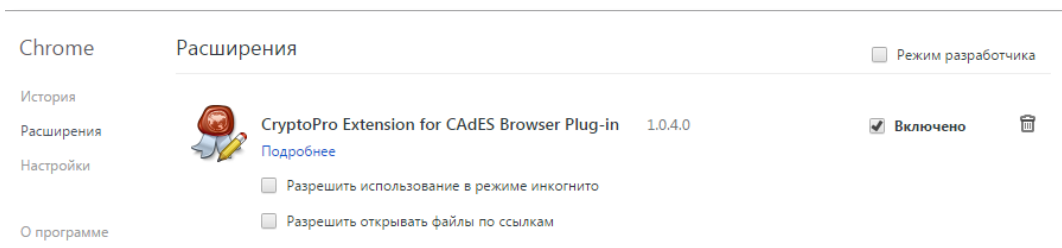
Настройка КриптоПро ЭЦП Browser plug-in при использовании браузера Chrome версии 45 и выше

Для настройки КриптоПро ЭЦП Browser plug-in выполните следующие шаги:

1. Откройте интернет браузер Chrome.
2. Нажмите кнопку **Включить расширение** в открывшемся окне.

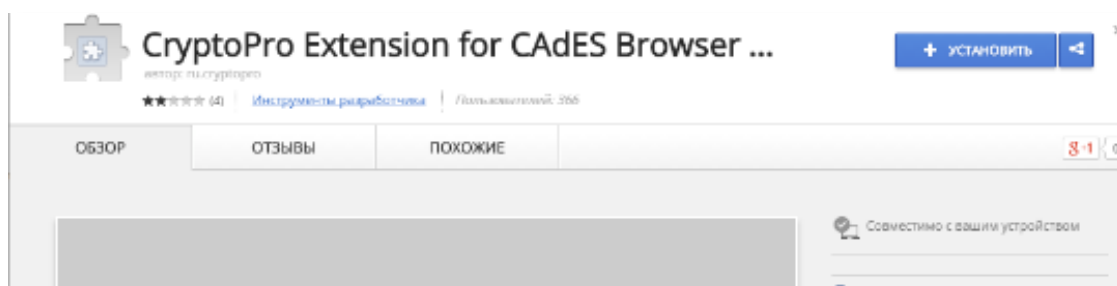


3. Проверьте включение расширения, выбрав в меню браузера пункты: «Дополнительные настройки» -> «Расширения».

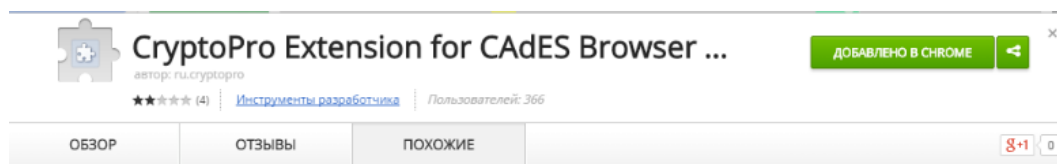


Если сообщение о добавлении расширения не появилось, то для включения расширения перейдите по ссылке:

https://chrome.google.com/webstore/detail/cryptopro-extension-for-c/iifchhfnmpdbibifmljnfjhpififfog?utm_source=chrome-app-launcher-info-dialog



4. Нажмите кнопку **Установить**.



УСТАНОВКА ДРАЙВЕРА КЛЮЧЕВОГО НОСИТЕЛЯ

Для работы с ЭП на любом физическом носителе необходимо установить драйвер ключевого носителя ЭП (Rutoken, ESMART Token, eToken и т. д.). В данном руководстве представлено описание установки драйвера ключевого носителя Rutoken, ESMART Token, eToken.

Установка драйвера ключевого носителя Rutoken

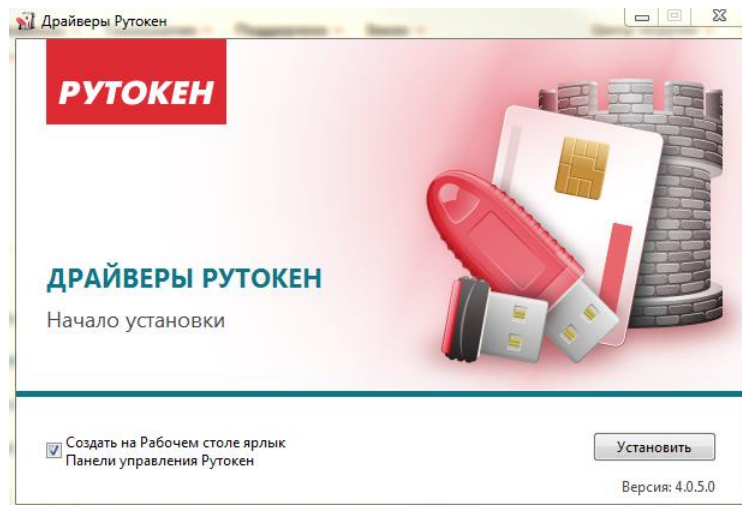
Драйвер ключевого носителя Rutoken можно скачать с сайта производителя, а также по ссылке в разделе «Дистрибутивы для РУТОКЕН»:

Драйверы Рутокен для Windows (x86 и x64) универсальный установщик

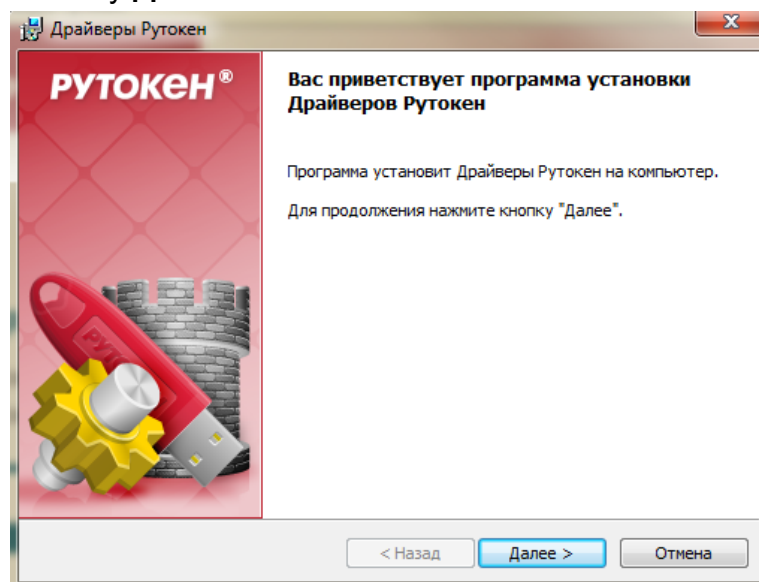
Примечание: При установке драйвера ключевой носитель Rutoken **не должен** быть вставлен в USB-порт компьютера.

Для установки драйвера ключевого носителя Rutoken выполните следующие шаги:

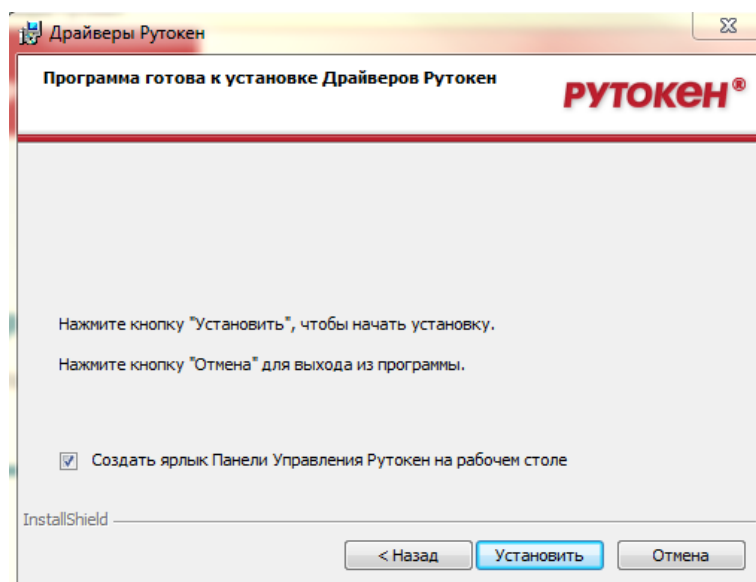
1. Нажмите кнопку «Установить» для запуска установки.



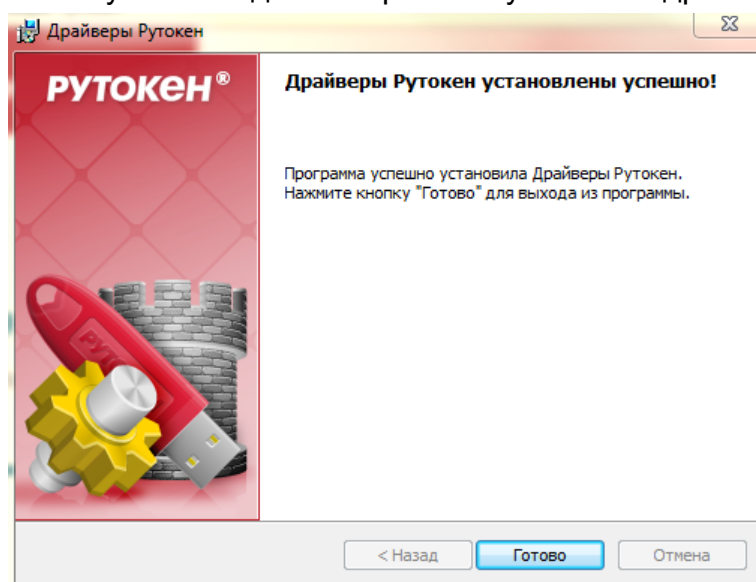
2. Нажмите кнопку **Далее**.



3. Для запуска установки драйвера Rutoken нажмите **Установить**.



4. Нажмите кнопку **Готово** для завершения установки драйвера.



Установка драйвера ключевого носителя ESMART Token

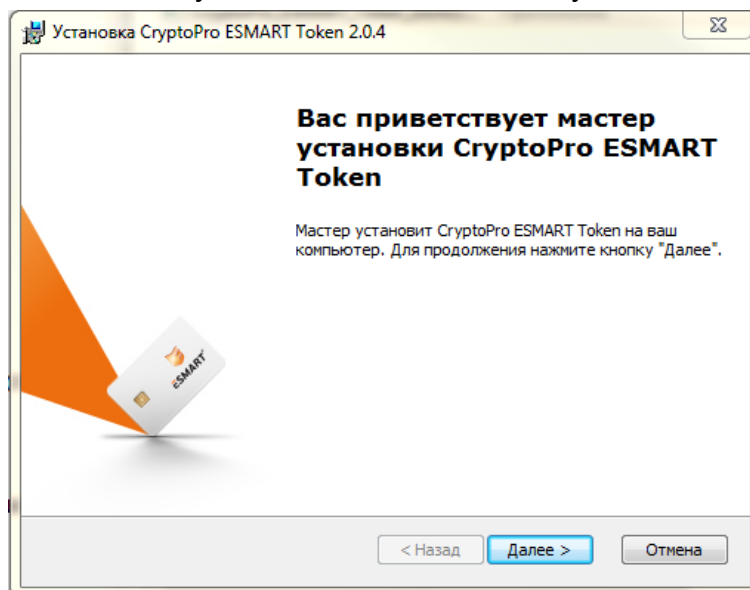
ESMART Token поддерживается в СКЗИ "КриптоПро CSP", начиная с версии 3.6 R3. Для более ранних версий необходимо установить модуль поддержки, который можно скачать по ссылке в разделе «Дистрибутивы для ESMART Token»:

Модуль поддержки ESMART Token КриптоПро CSP для Windows

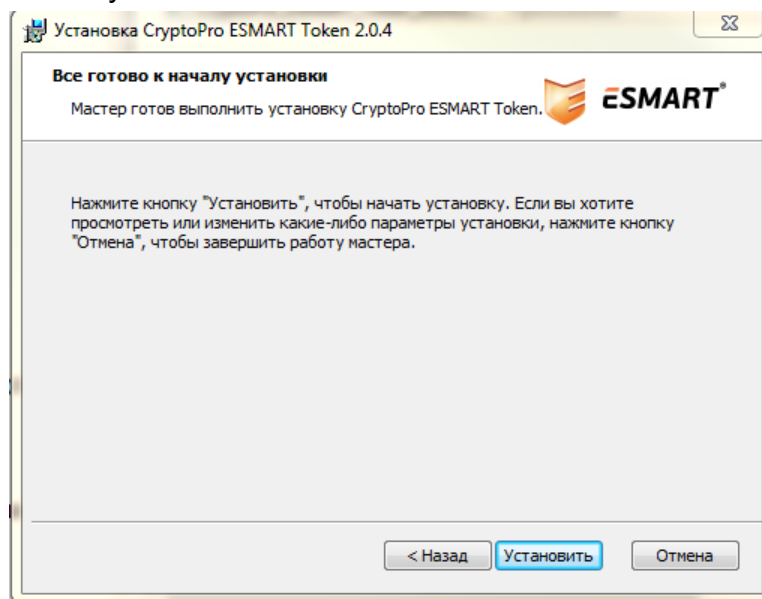
Для установки выполните следующие шаги:

1. Запустите установочный файл.

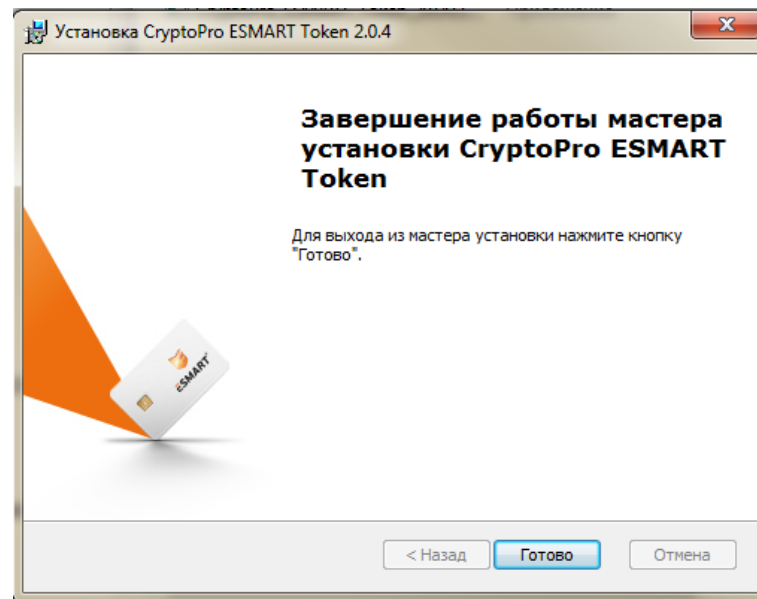
2. Выберите язык установки.
3. В открывшемся окне установки нажмите кнопку **Далее**.



4. Нажмите кнопку **Установить**.



5. Для завершения установки нажмите кнопку **Готово**.



В случае, когда обновление Windows производится регулярно, установка драйвера ключевого носителя не требует дополнительных операций – при первом использовании драйвер автоматически скачивается из центра обновлений.

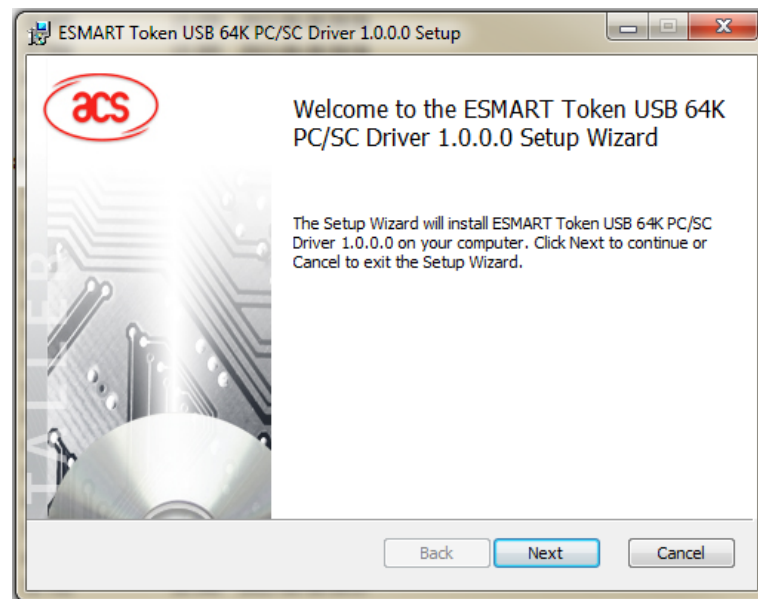
Иначе драйверы для USB-ключа ESMART Token 64K можно скачать по следующей ссылке в разделе «Дистрибутивы для ESMART Token»:

[Драйвер ESMART Token USB 64K для Windows](#)

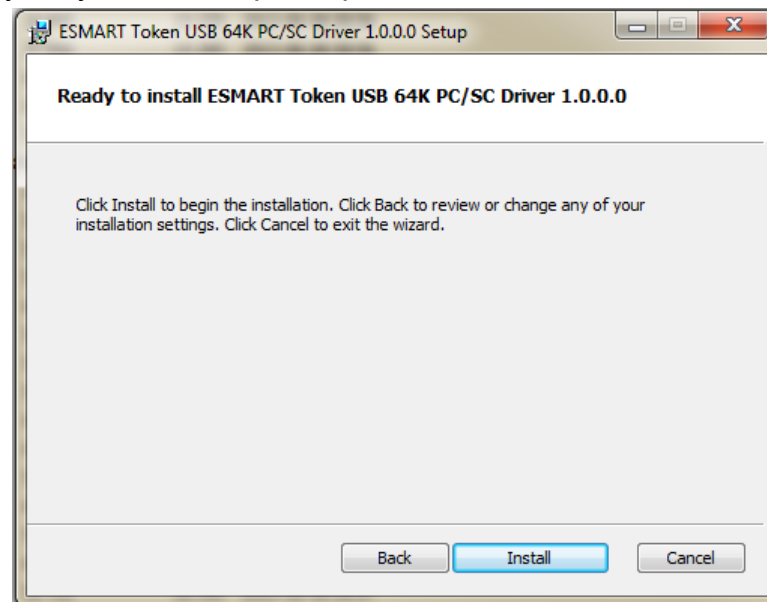
***Примечание:** Обратите внимание, что при установке драйвера ключевой носитель ESMART Token не должен быть вставлен в USB-порт компьютера.*

Для установки выполните следующие шаги:

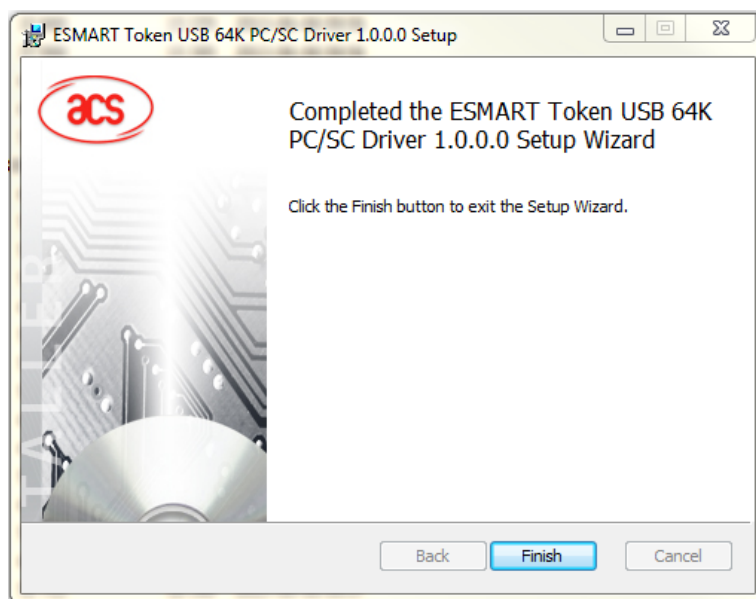
1. Запустите установочный файл драйвера ESMART Token USB 64K PCSC Driver-1.0.0.0.msi
2. В открывшемся окне установки нажмите кнопку **NEXT**.



3. Для запуска установки драйвера ESMART Token нажмите кнопку **Install**.



4. Для завершения установки драйвера нажмите кнопку **Finish**.



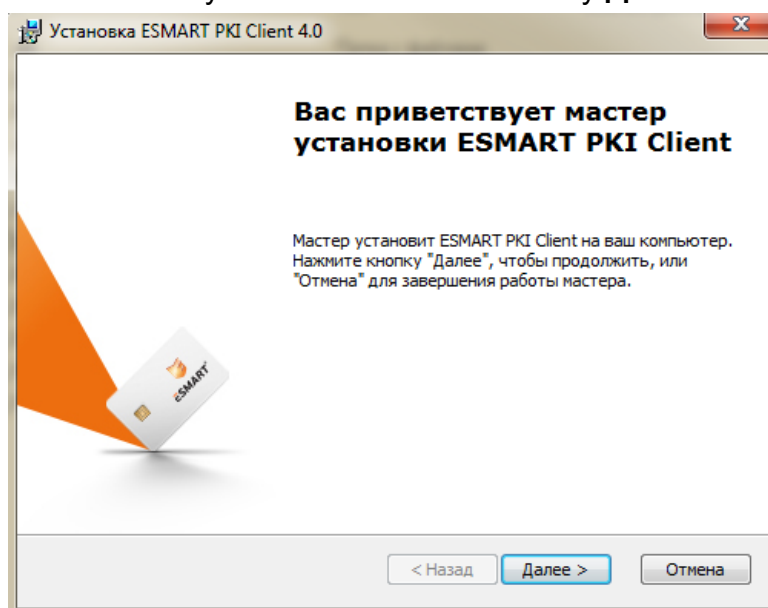
Для операции с ключами ESMART Token без использования командной строки: например, для изменения пин-кодов, необходима установка ПО ESMART PKI Client.

Установочный файл ESMART PKI Client для Windows можно скачать по следующей ссылке в разделе «Дистрибутивы для ESMART Token»:

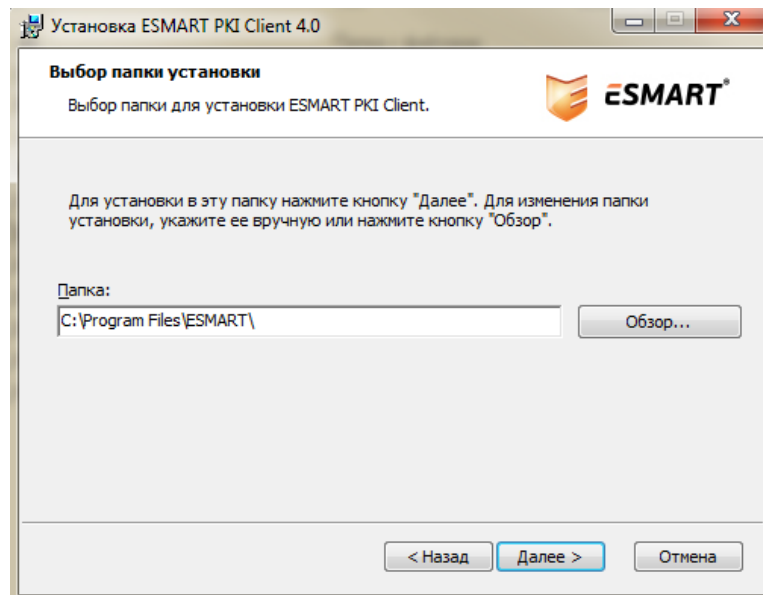
[ESMART PKI Client для Windows](#)

Для установки выполните следующие шаги:

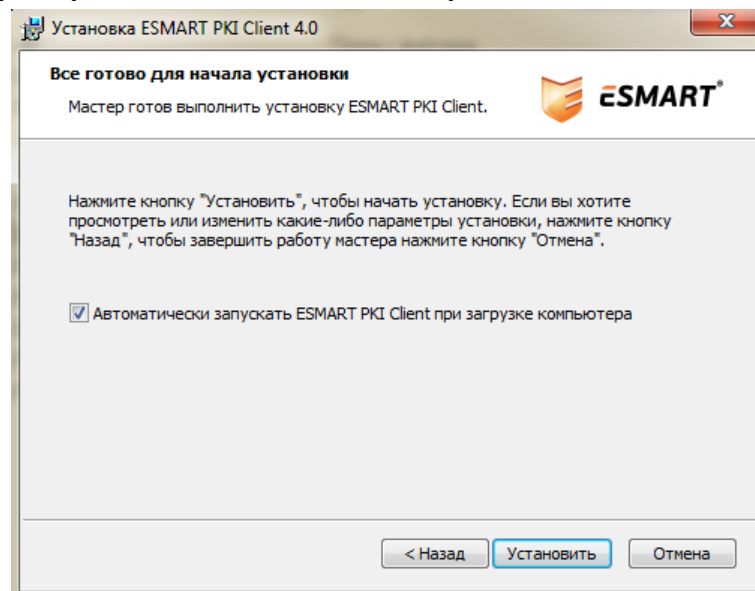
1. Запустите установку **setup**.
2. В открывшемся окне установки нажмите кнопку **Далее**.



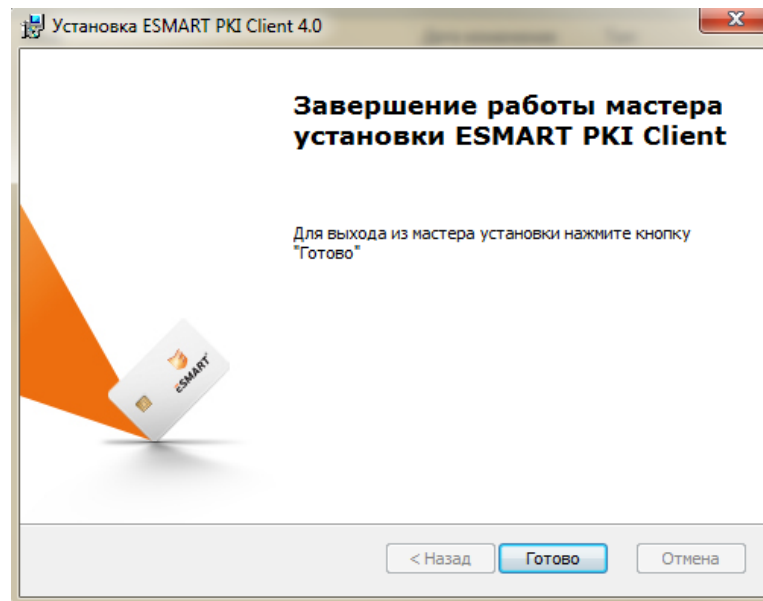
3. Выберите папку установки и нажмите кнопку **Далее**.



4. Для запуска установки нажмите кнопку **Установить**.



5. Для завершения установки нажмите кнопку **Готово**.



Установка драйвера ключевого носителя eToken

Драйвер ключевого носителя eToken можно скачать по следующей ссылке:

Драйверы eToken

***Примечание:** Обратите внимание, что при установке драйвера ключевой носитель eToken не должен быть вставлен в USB-порт компьютера.*

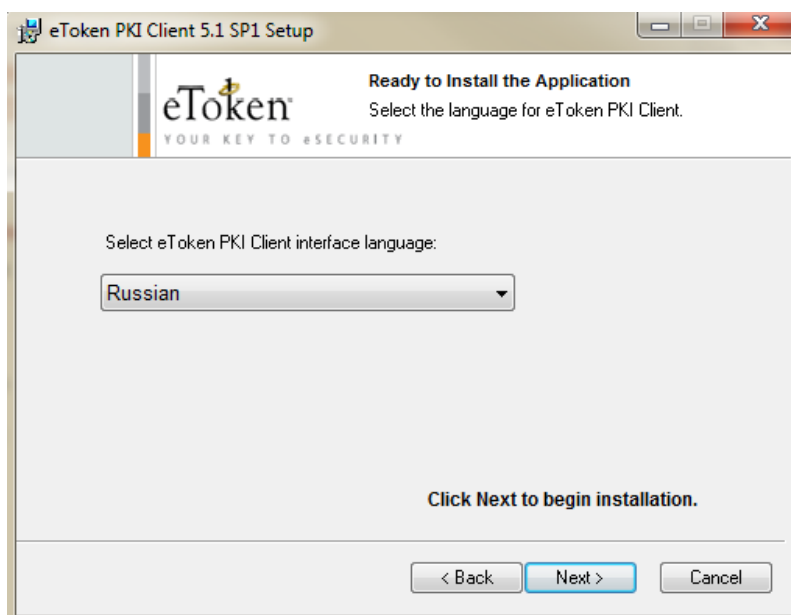
Для установки выполните следующие шаги:

1. Запустите установочный файл из файла **.msi** (выберите 32- или 64-битную версию в зависимости от вашей операционной системы).
2. В открывшемся окне установки нажмите кнопку **Next**.

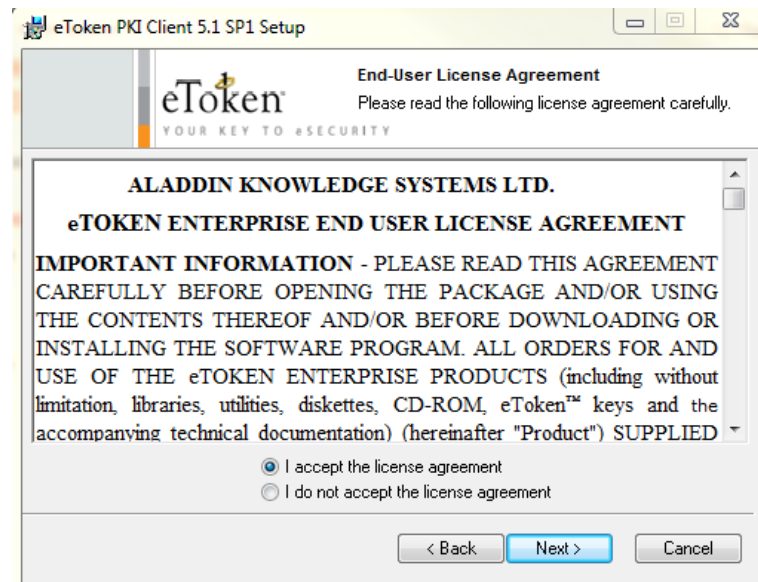


3. В списке доступных языков интерфейса выберите «Russian» (Русский) и нажмите кнопку **Next**.

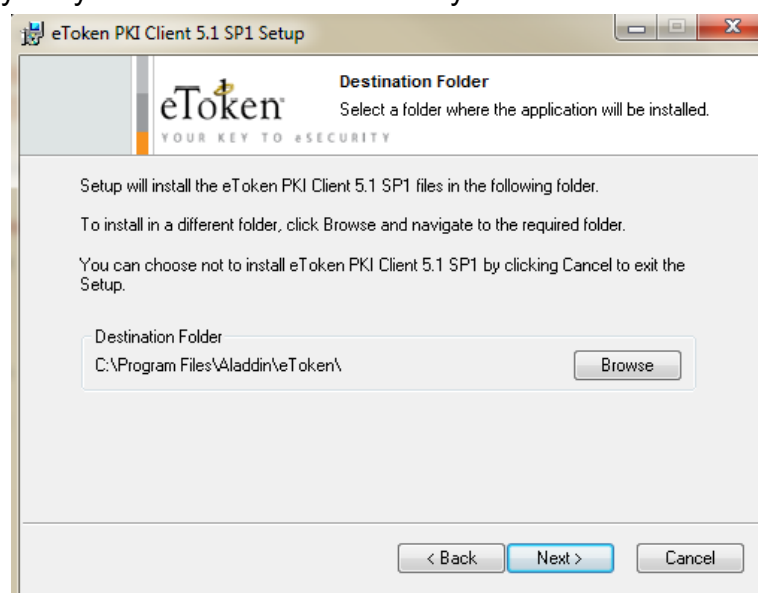
Примечание: Для сохранения настроек, оставшихся от предыдущей версии, поставьте отметку.



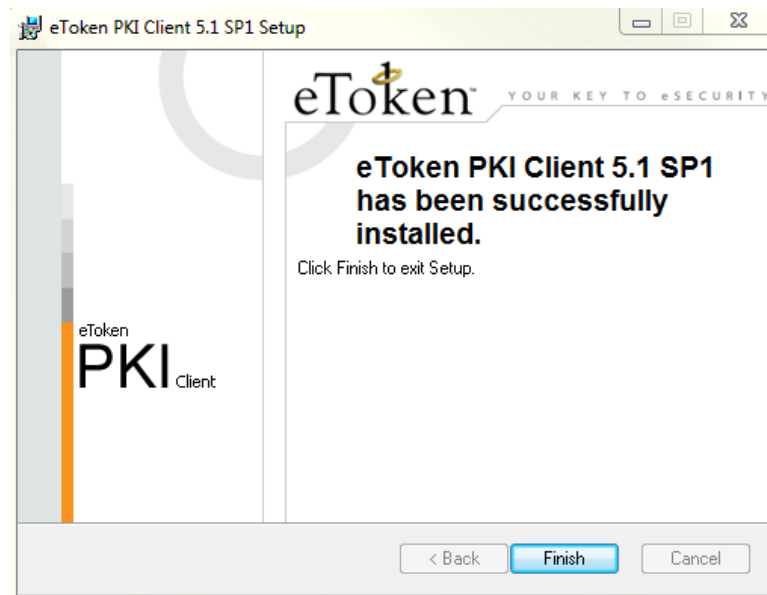
4. Прочтите внимательно лицензионное соглашение и, если вы согласны со всеми его условиями, отметьте пункт «I accept the license agreement» и нажмите кнопку **Next**.



5. После принятия соглашения в открывшемся окне укажите путь для установки, нажав кнопку **Browse**, или оставьте его таким, как он указан по умолчанию.
6. Для запуска установки нажмите кнопку **Next**.



7. После установки нажмите кнопку **Finish**.



УСТАНОВКА СЕРТИФИКАТА КЛЮЧА ПОДПИСИ

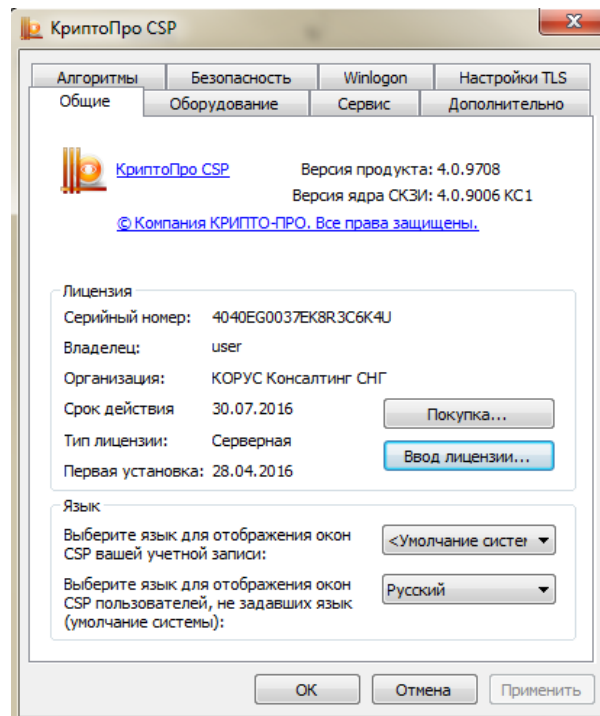
Ниже приведено описание установки сертификата ключа подписи с ключевого носителя.

Перед установкой сертификата ключа подписи необходимо вставить ключевой носитель в USB-порт компьютера.

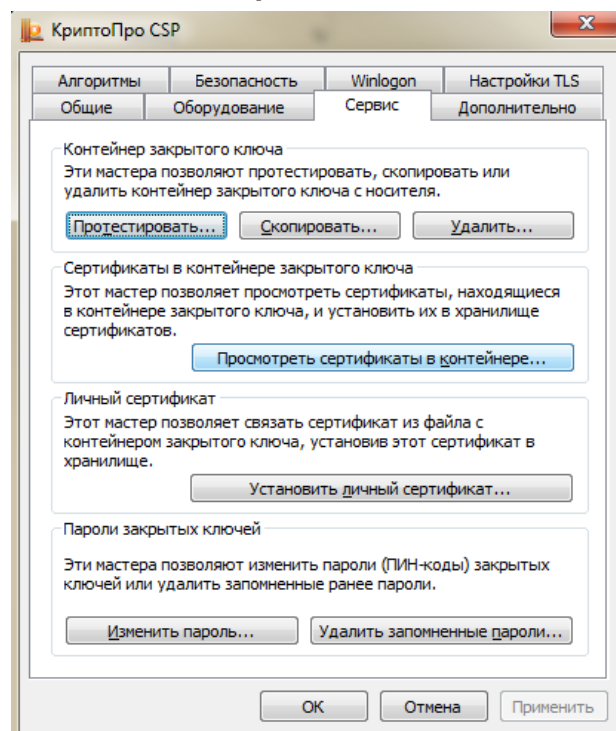
***Примечание:** Если планируется использовать несколько сертификатов ключей подписи, данные действия необходимо произвести для каждого сертификата.*

Для установки сертификата ключа подписи выполните следующие шаги:

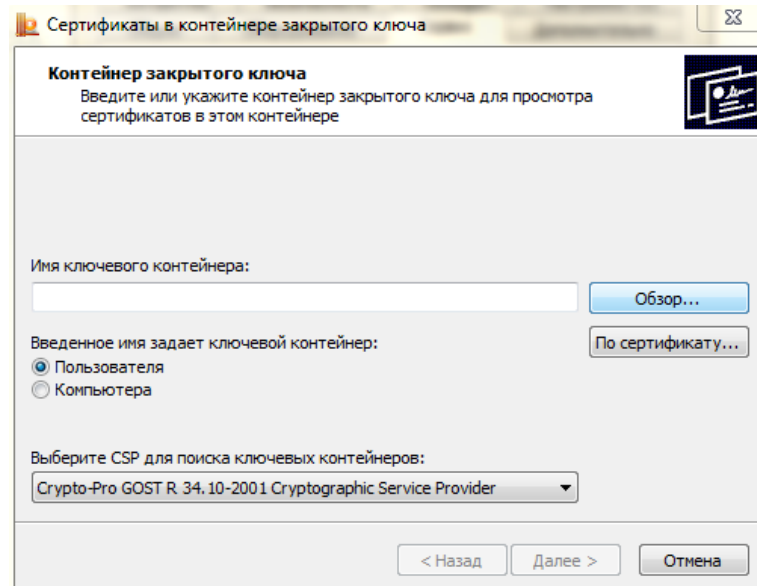
1. Для запуска КриптоПро CSP нажмите кнопку **Пуск** и выберите в меню пункт «КриптоПро CSP».



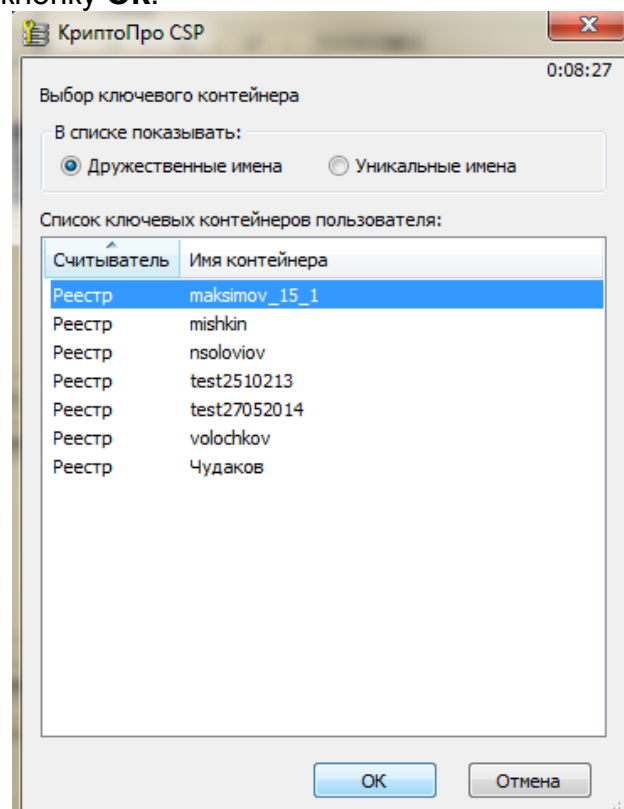
2. Выберите вкладку «Сервис» и нажмите кнопку **Просмотреть сертификаты в контейнере**.



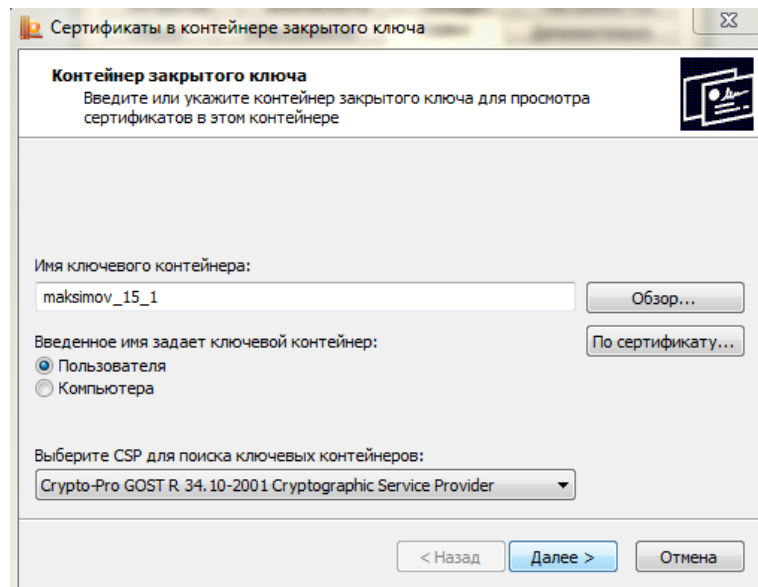
3. Нажмите кнопку **Обзор**.



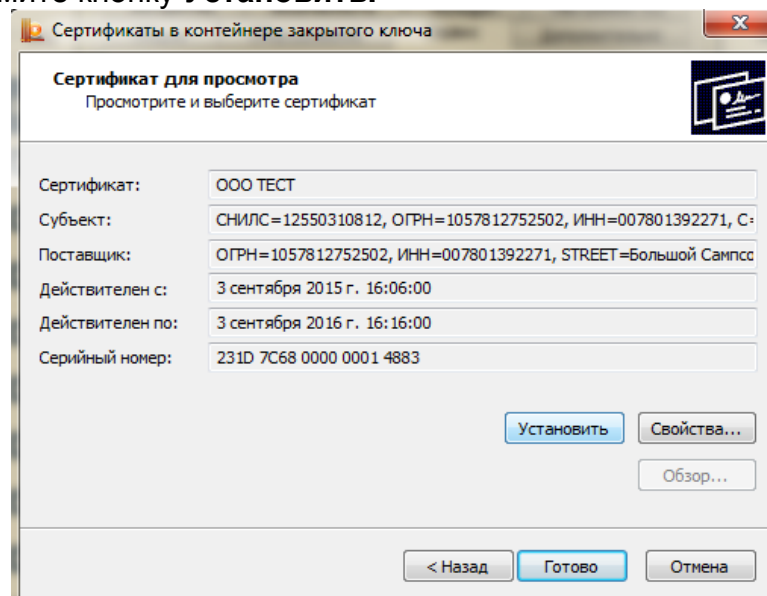
4. В списке ключевых носителей выберите нужный личный сертификат и нажмите кнопку **ОК**.



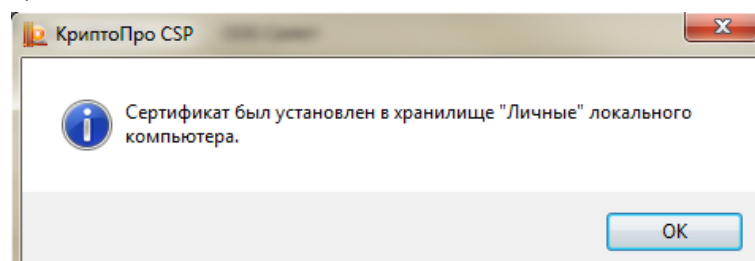
5. Нажмите кнопку «**Далее**» для продолжения установки.



6. Нажмите кнопку **Установить**.



7. Нажмите кнопку **ОК** в сообщении об успешном импорте сертификата в хранилище.



УСТАНОВКА КОРНЕВОГО СЕРТИФИКАТА

Для работы с электронной подписью необходимо установить корневой сертификат.

Для работы с электронной подписью, выданной Удостоверяющим центром ООО «КОРУС Консалтинг СНГ»:

- до 16.11.2016 - необходимо установить корневой сертификат Удостоверяющего центра ООО «КОРУС Консалтинг СНГ», который можно скачать в разделе «Корневой сертификат и реестр аннулированных сертификатов» на сайте или по ссылке:

Доверенный корневой сертификат Удостоверяющего центра ООО "КОРУС Консалтинг СНГ";

- после 16.11.2016 - необходимо установить корневой сертификат Головного удостоверяющего центра Минкомсвязи, который можно скачать в разделе «Корневой сертификат и реестр аннулированных сертификатов» на сайте или по ссылке:

Доверенный корневой сертификат Головного удостоверяющего центра Минкомсвязи.

Для работы с электронной подписью, выданной сторонним Удостоверяющим центром:

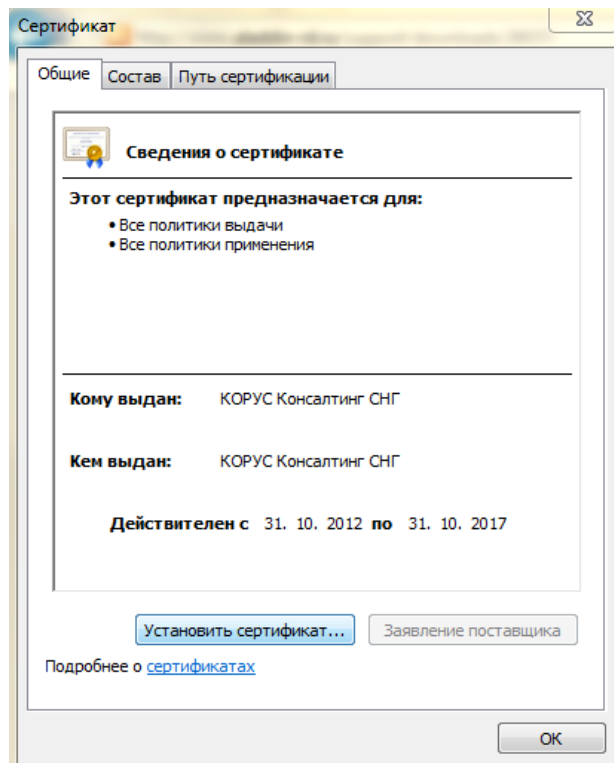
- *до перехода на подчиненный режим работы УЦ* - необходимо установить корневой сертификат данного Удостоверяющего центра;
- *после перехода на подчиненный режим работы УЦ* - необходимо установить корневой сертификат Головного удостоверяющего центра Минкомсвязи.

Для работы с электронной подписью усовершенствованного формата, выданной сторонним Удостоверяющим центром:

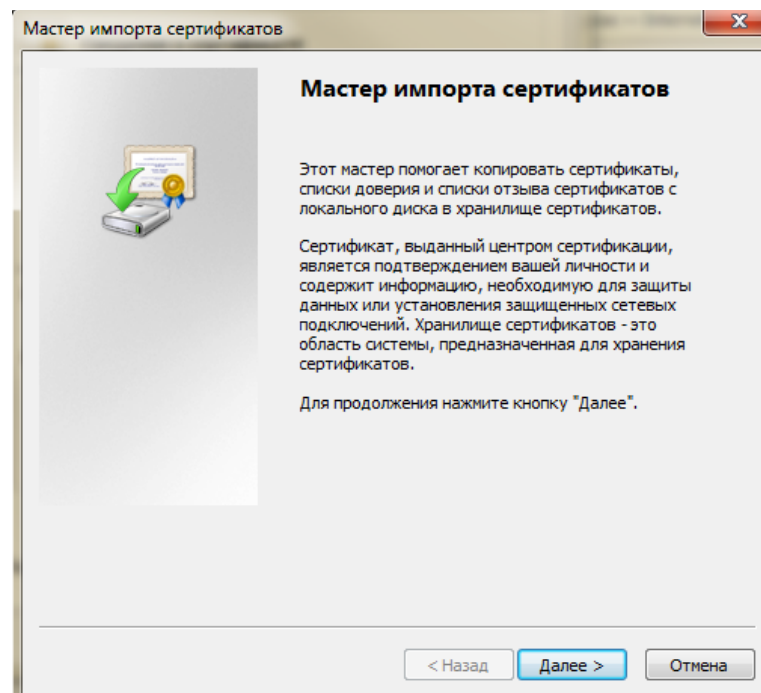
- *до перехода на подчиненный режим работы УЦ* - необходимо установить корневой сертификат данного Удостоверяющего центра и корневой сертификат Удостоверяющего центра ООО «КОРУС Консалтинг СНГ»;
- *после перехода на подчиненный режим работы УЦ* - необходимо установить корневой сертификат Головного удостоверяющего центра Минкомсвязи и корневой сертификат Удостоверяющего центра ООО «КОРУС Консалтинг СНГ».

Для установки корневого сертификата выполните следующие шаги:

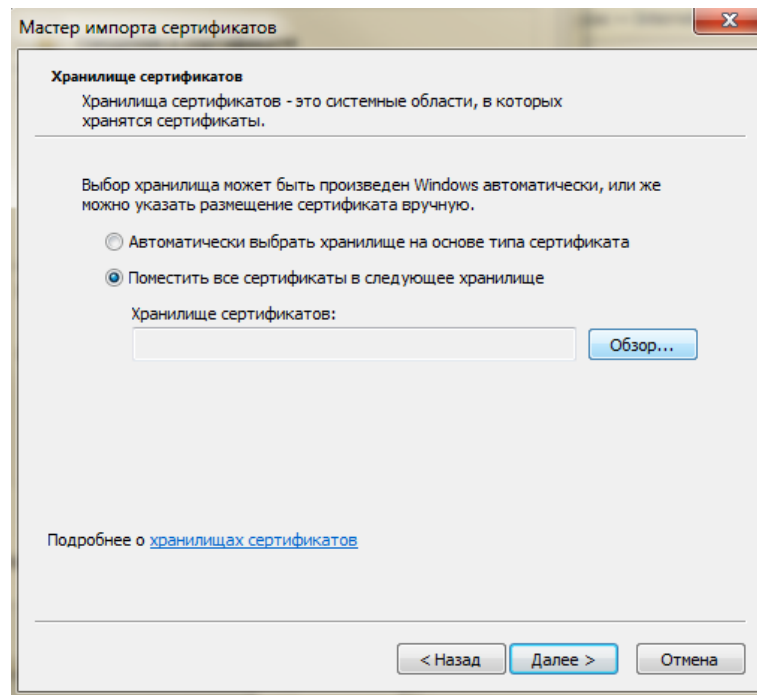
1. Откройте файл корневого сертификата.
2. Нажмите кнопку **Установить сертификат**.



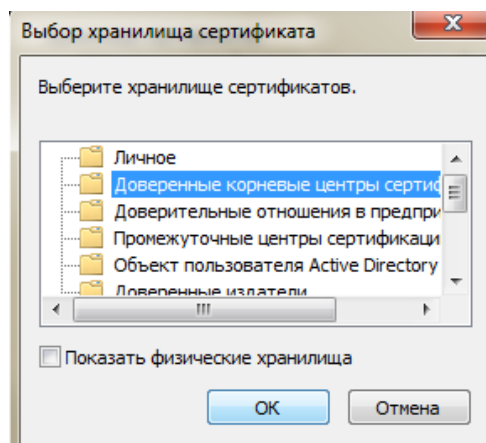
3. После этого запустится «Мастер импорта сертификатов». Для продолжения установки нажмите кнопку **Далее**.



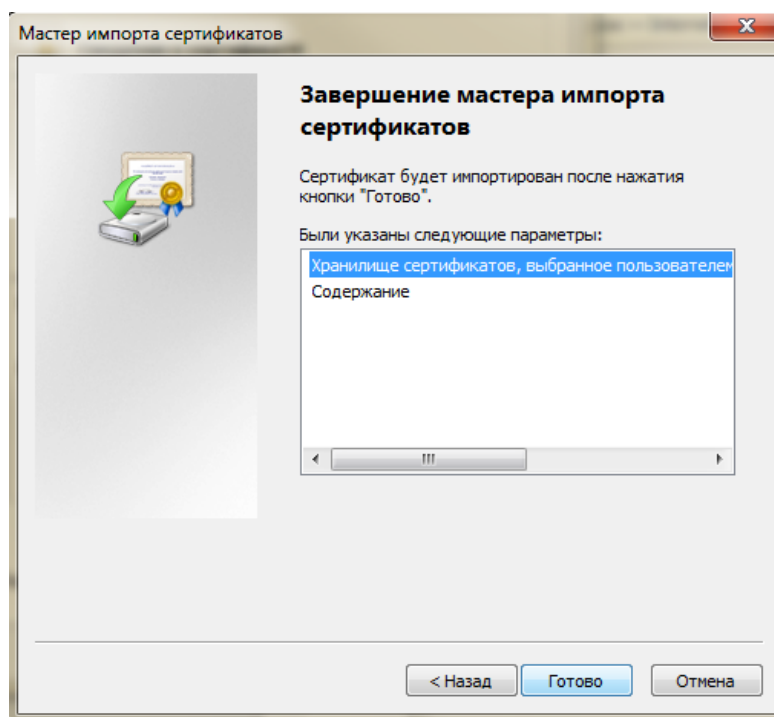
4. Установите отметку «Поместить все сертификаты в следующее хранилище» и нажмите кнопку **Обзор**.



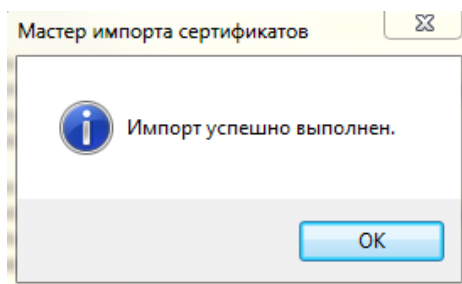
5. Выберите хранилище «Доверенные корневые центры сертификации», нажмите **ОК** и **Далее**.



6. Нажмите кнопку **Готово** для завершения установки сертификата.



7. Нажмите кнопку **OK** в сообщении об успешном импорте сертификата в хранилище.



НАСТРОЙКА БРАУЗЕРА INTERNET EXPLORER

При использовании браузера Internet Explorer, для корректной работы в сервисе требуется произвести дополнительные настройки браузера.

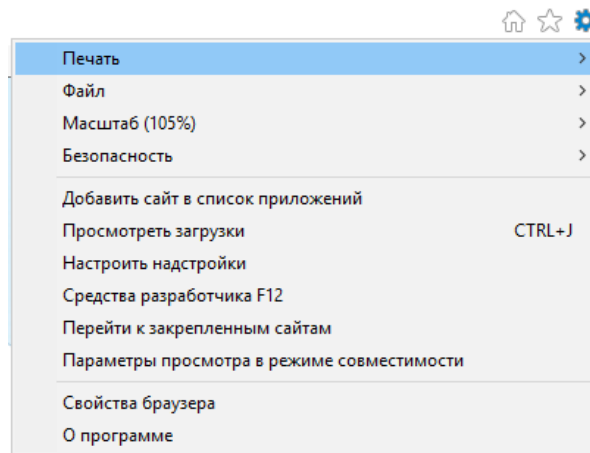
Для настройки браузера Internet Explorer выполните следующие шаги:

1. Откройте браузер Internet Explorer.

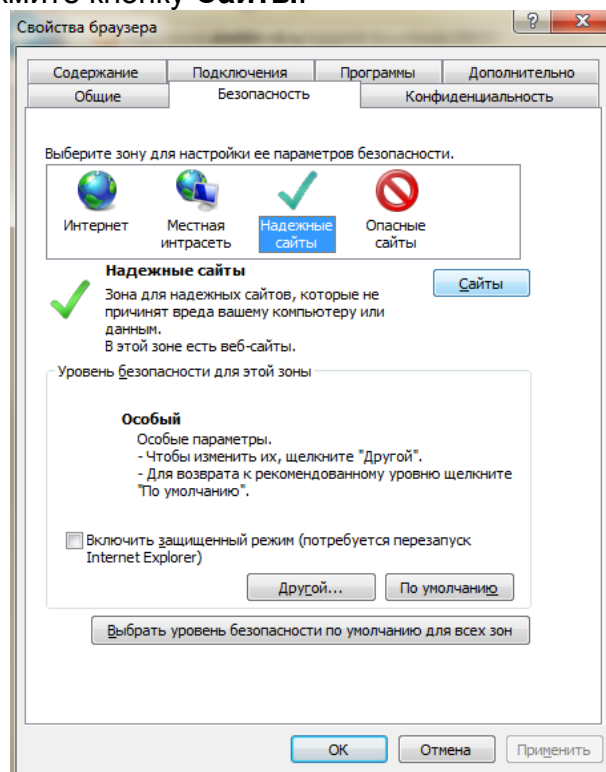
Примечание: Для поиска и запуска браузера Internet Explorer в ОС Windows 10 выполните следующие шаги:

1. Перейдите в меню «Пуск» и выберите «Поиск в Windows».
 2. Введите в поисковой строке «internet» и нажмите на приложение для открытия.
 3. Закрепите ярлык на Рабочем столе или в Панели задач для удобства дальнейшего использования.
-

2. Нажмите кнопку **Сервис** и выберите в меню пункт «Свойства браузера».

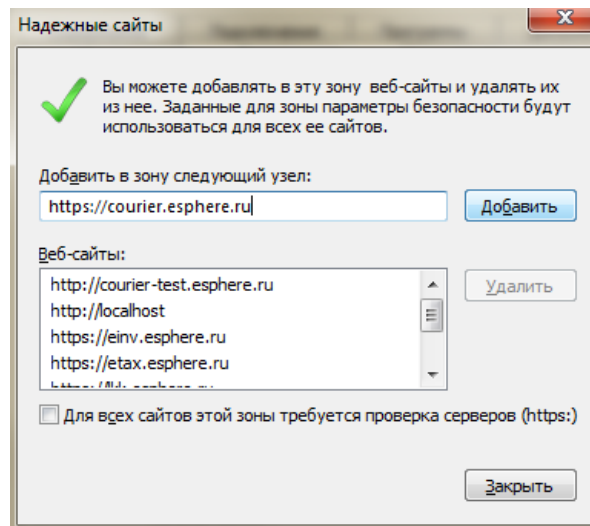


3. Откройте вкладку «Безопасность».
4. Во вкладке «Безопасность» отметьте зеленую пиктограмму «Надежные сайты» и нажмите кнопку **Сайты**.

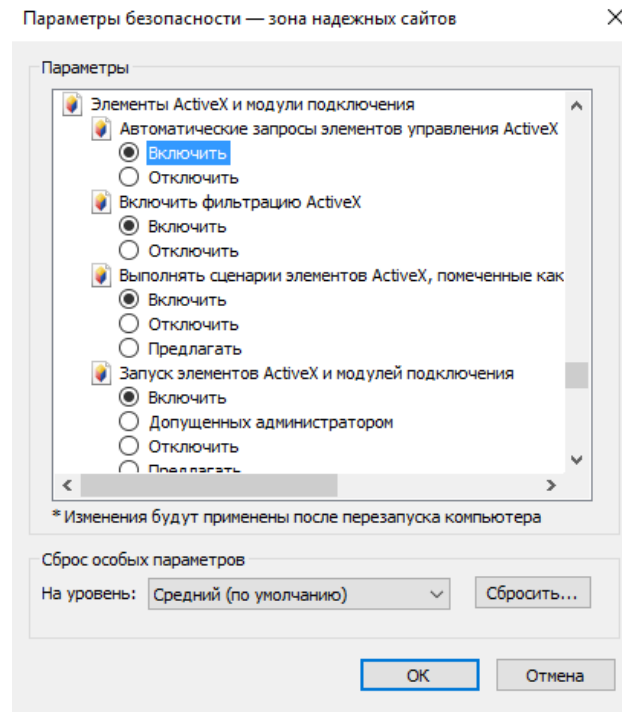


5. В окне «Надежные сайты» в поле «Добавить в зону следующий узел» введите адрес <https://courier.esphere.ru> и нажмите кнопку **Добавить**.

Примечание: Флаг «Для всех узлов этой зоны требуется проверка серверов (https:)» не должен быть установлен.



6. Адрес сервиса «СФЕРА Курьер» будет добавлен в список надежных узлов. Чтобы закрыть окно, нажмите кнопку **Заккрыть**.
7. После добавления адреса сервиса «СФЕРА Курьер» в надежные узлы во вкладке «Безопасность», нажмите кнопку **Другой**.
8. В настройках параметров безопасности в разделе «Элементы ActiveX и модули подключения» включите следующие настройки:
 - Автоматические запросы элементов управления ActiveX;
 - Выполнять сценарии элементов ActiveX, помеченные как безопасные;
 - Запуск элементов ActiveX и модулей подключения;



- Использование элементов управления ActiveX, не помеченные как безопасные для использования;
- Разрешать использовать ActiveX без запроса только утвержденным доменам;

- Разрешать запуск элементов управления ActiveX, которые не использовались ранее, без предупреждения;
- Скачивание неподписанных элементов ActiveX;
- Скачивание подписанных элементов ActiveX.

9. После включения опций нажмите кнопку **ОК**.

10. Для корректной работы рекомендуется перезапустить браузер.

Ваше программное обеспечение готово к работе с сервисом «СФЕРА Курьер».

ДОБАВЛЕНИЕ СЕРТИФИКАТА В КАРТОЧКУ ПОЛЬЗОВАТЕЛЯ СЕРВИСА

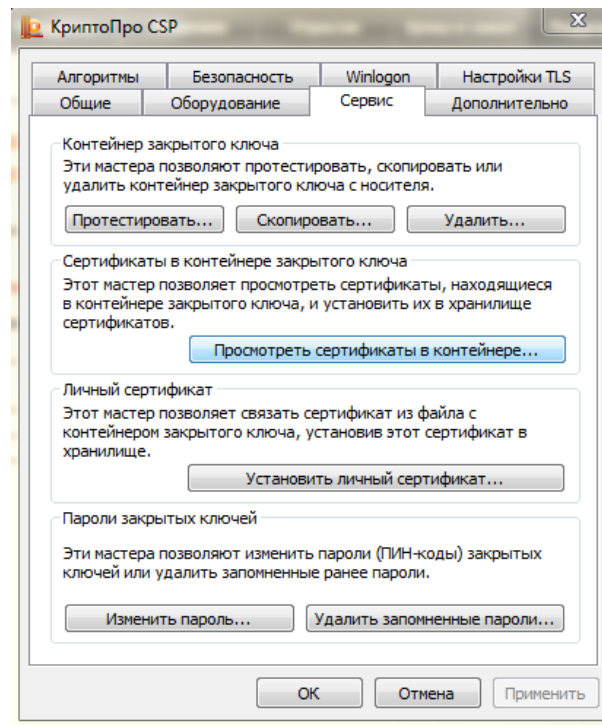
Для загрузки сертификата в карточку пользователя необходимо сделать следующее:

1. Экспортировать сертификат с ключевого носителя.
2. Загрузить сертификат в карточку пользователя сервиса.

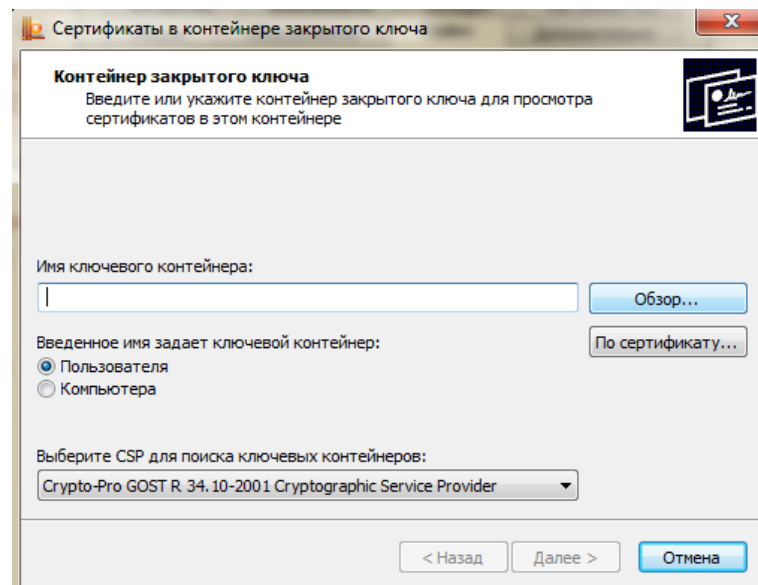
Экспорт сертификата с ключевого носителя

Для экспорта сертификата с ключевого носителя выполните следующие шаги:

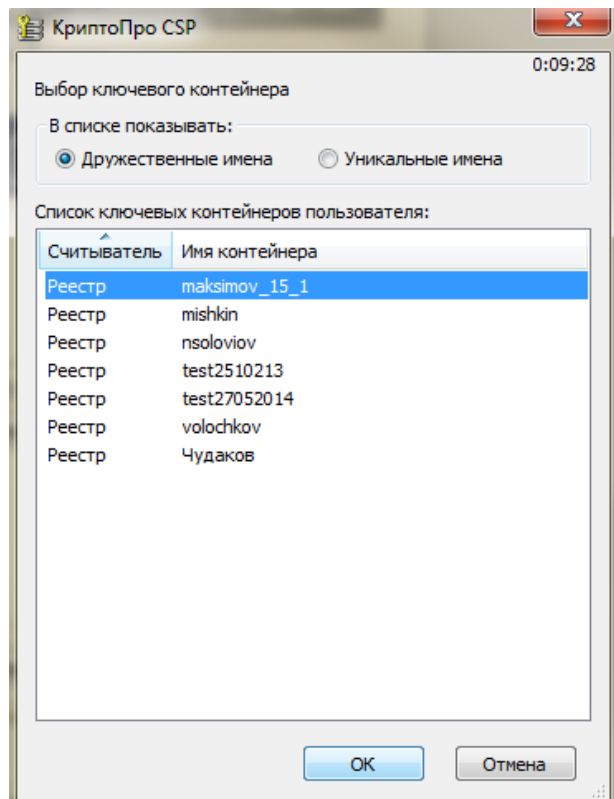
1. Для запуска КриптоПро CSP нажмите кнопку **Пуск** и выберите в меню пункт «КриптоПро CSP».
2. Выберите вкладку «Сервис» и нажмите кнопку **Просмотреть сертификаты в контейнере**.



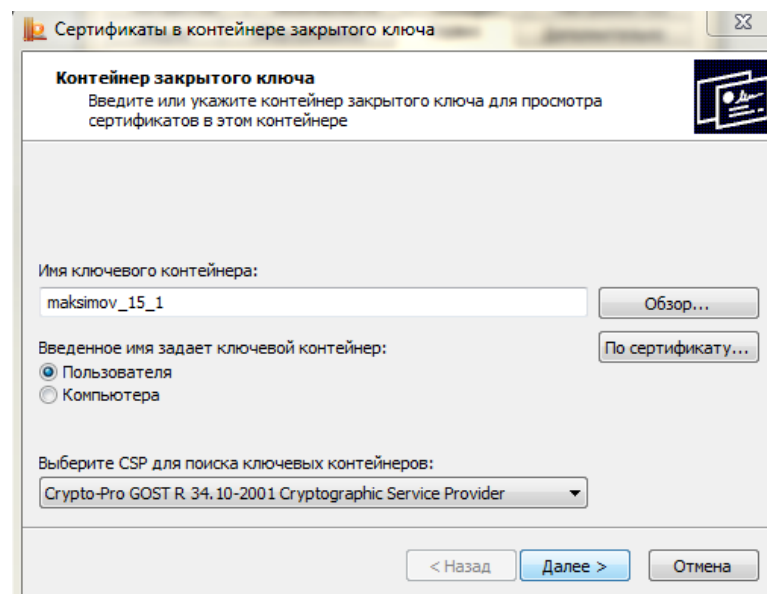
3. В окне «Сертификаты в контейнере закрытого ключа» нажмите кнопку **Обзор**.



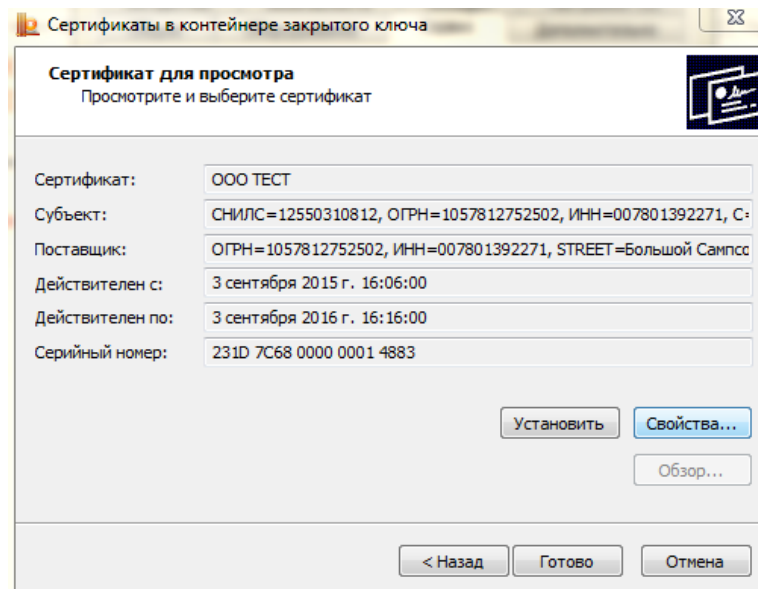
4. В списке ключевых носителей выберите используемый ключевой контейнер и нажмите кнопку **ОК**.



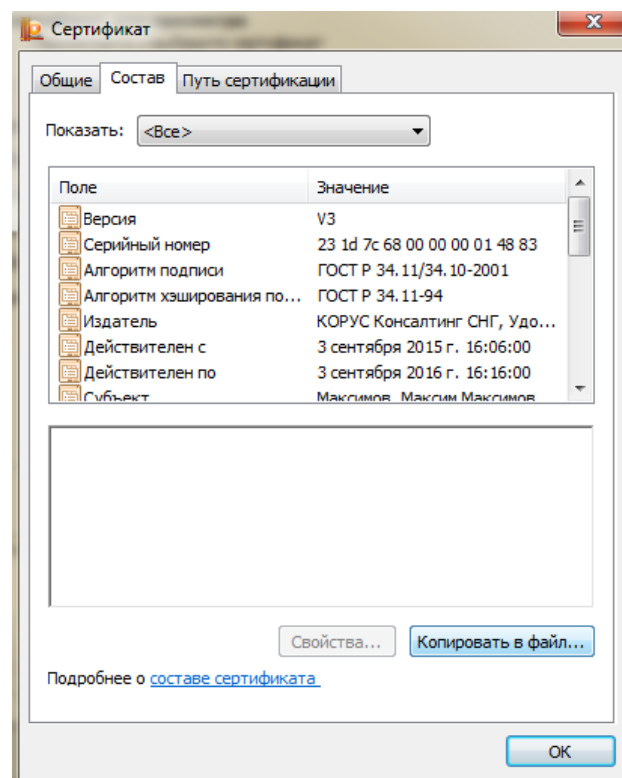
5. Нажмите кнопку **Далее** для продолжения.



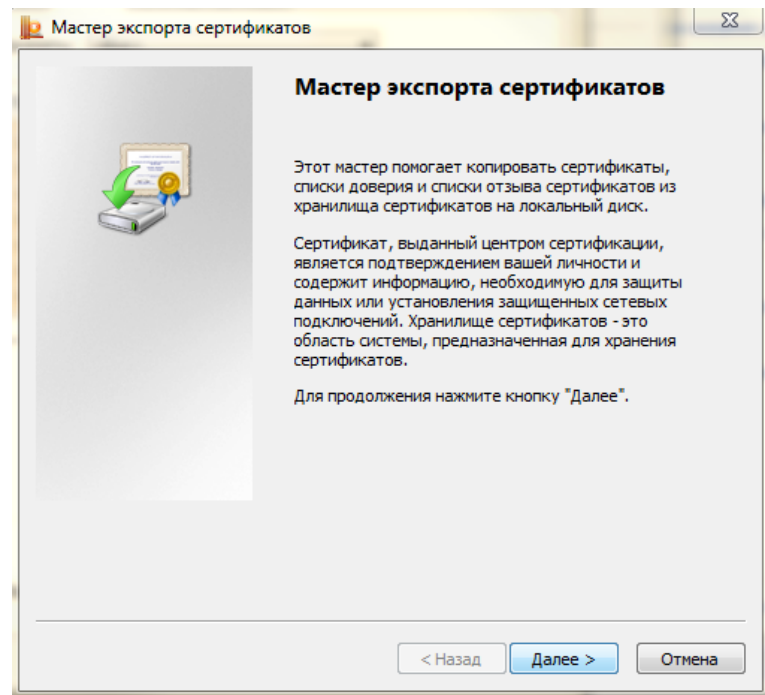
6. В окне с информацией о выбранном сертификате нажмите кнопку **Свойства**.



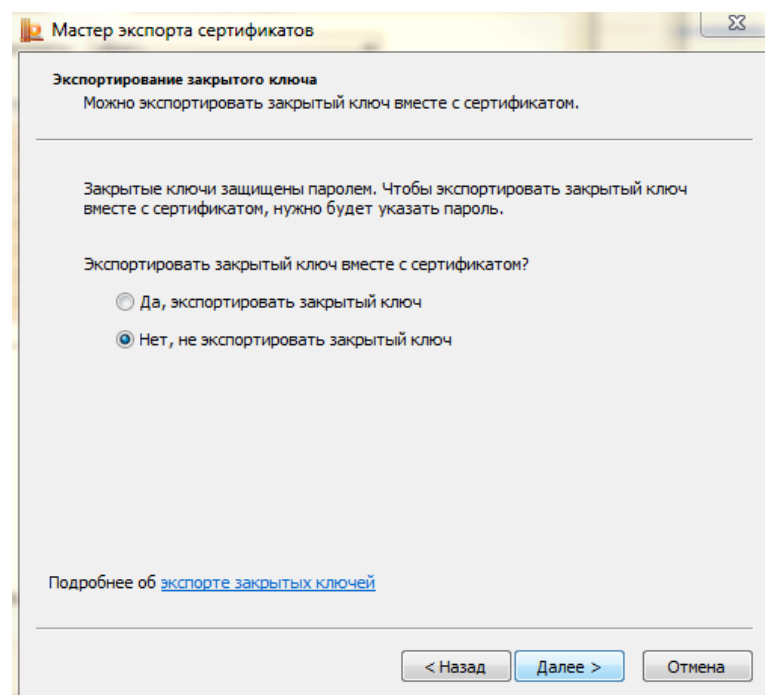
7. Выберите вкладку «Состав» и нажмите кнопку **Копировать в файл**.



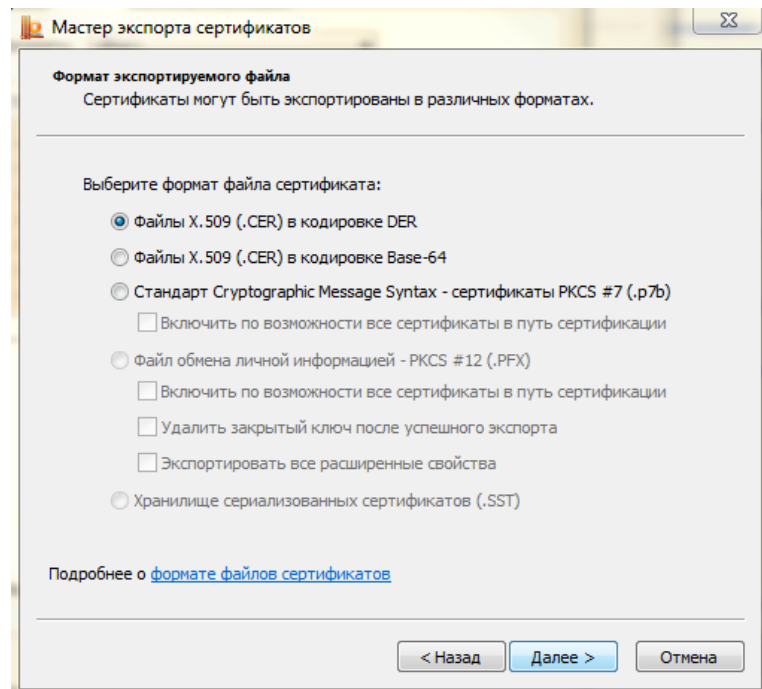
8. После этого запустится «Мастер экспорта сертификатов». Для продолжения установки нажмите **Далее**.



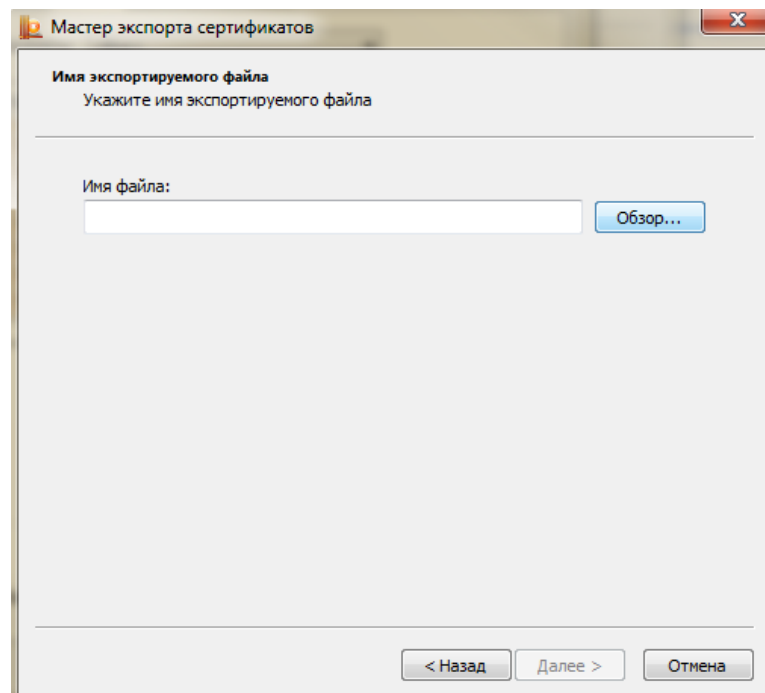
9. Отметьте вариант «Нет, не экспортировать закрытый ключ» и нажмите кнопку **Далее**.



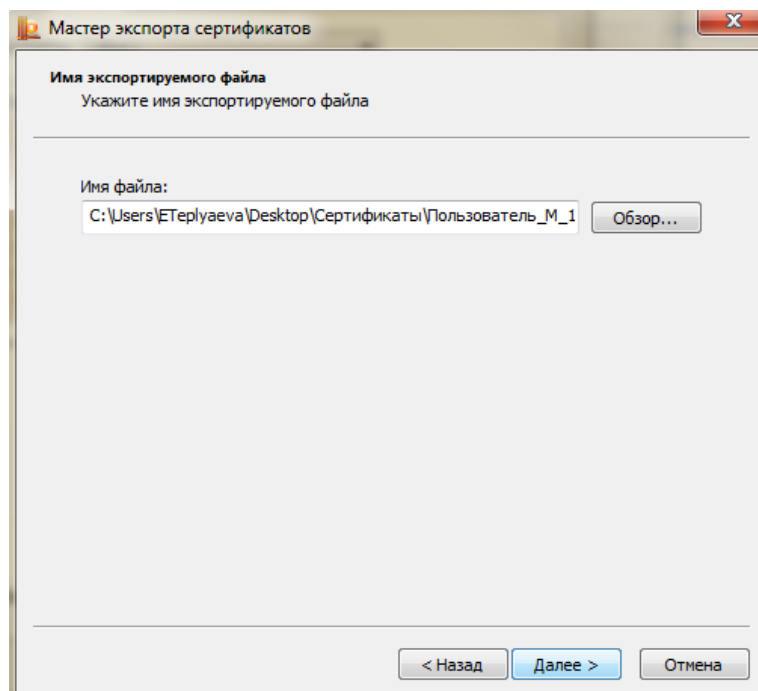
10. Выберите формат файла сертификата: «Файлы X.509 (.CER) в кодировке DER» и нажмите кнопку **Далее**.



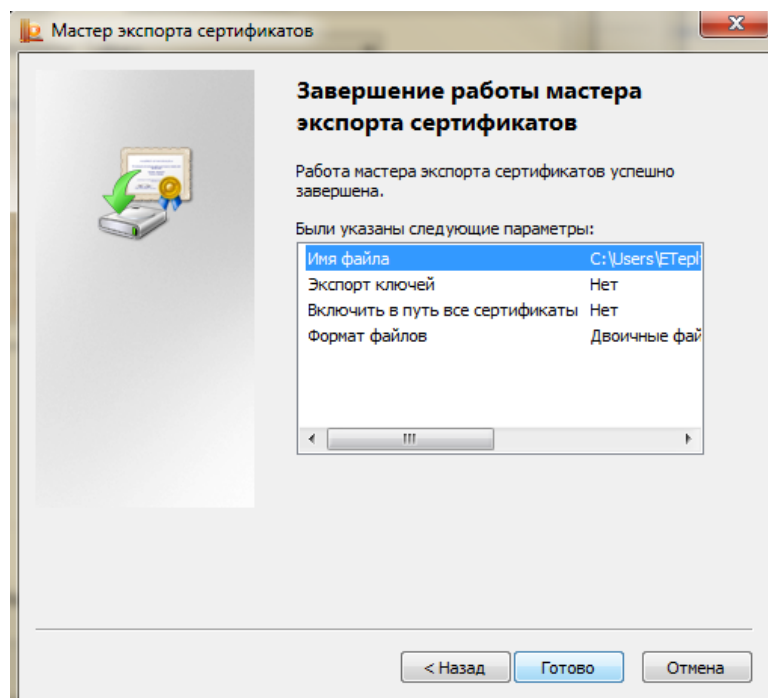
11. Нажмите кнопку **Обзор** и выберите место для сохранения экспортируемого файла. Задайте имя произвольно и нажмите кнопку **Сохранить**.



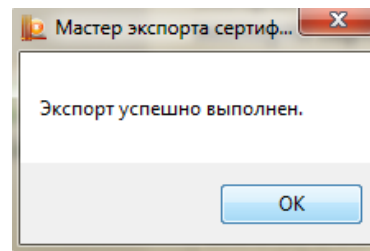
12. Нажмите кнопку **Далее** для продолжения работы мастера.



13. Нажмите кнопку **Готово** для завершения работы мастера экспорта сертификатов.




14. Нажмите кнопку **ОК**.



Загрузка сертификата пользователю системы

Для загрузки внешнего сертификата ЭП выполните следующие шаги:

1. Откройте страницу «Пользователи».
2. Нажмите кнопку  **Загрузить электронную подпись** в строке пользователя.

ПОЛЬЗОВАТЕЛИ Добавить

Введите фамилию, имя или отчество Расширенный поиск


Админ.	Пользователь	Документооборот
<input checked="" type="checkbox"/>	Васильева Виктория Перевыпускная sergip, [redacted]@esphere.ru	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Иванов Иван Иванович zahar, [redacted]@esphere.ru	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Лапотентова Надежда Дмитриевна nadezhda, [redacted]@esphere.ru	<input checked="" type="checkbox"/>


Кнопка Загрузить электронную подпись


3. Проверьте данные организации и владельца электронной подписи, при необходимости заполните недостающие данные, после чего нажмите кнопку **Подтвердить и продолжить**.


ЗАГРУЗКА ЭЛЕКТРОННОЙ ПОДПИСИ

Юридический адрес: 191020, ГО. САНКТ-ПЕТЕРБУРГ, пер. Мухомов, 7, лит.А, пом. 10-11

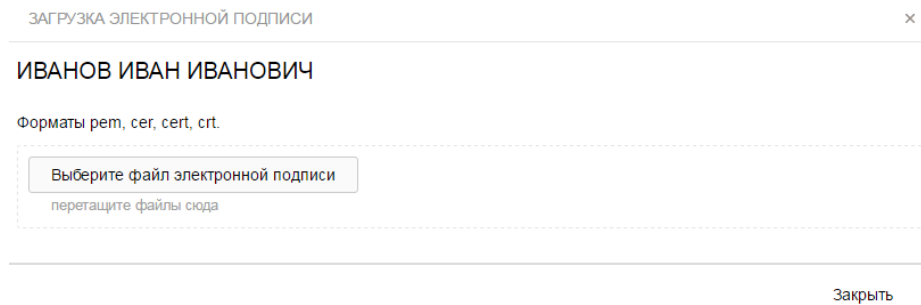
 [Иванов Иван Иванович](#)
+7 [redacted], [redacted]@esphere.ru
Регистрация 10.02.2017
zahar

 [Бухгалтер](#)
СНИЛС: 123-456-789 64

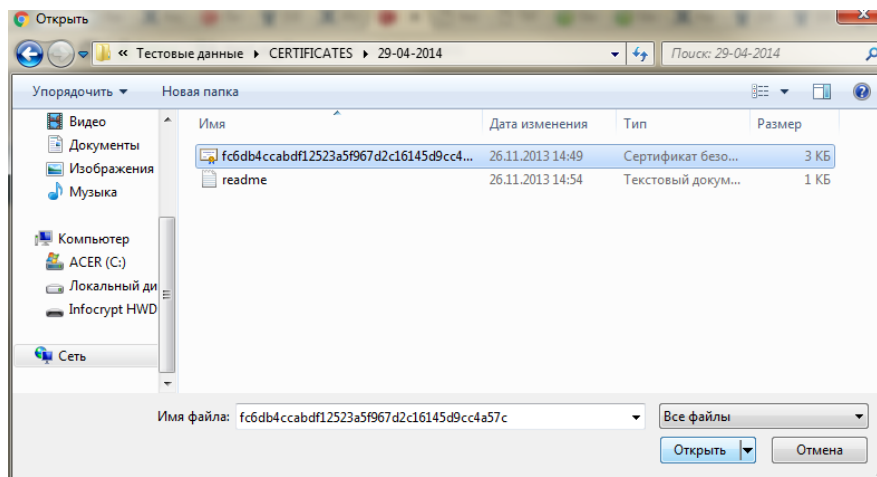
 [Паспорт гражданина РФ](#)
серия 2222 № 232323, выдан Отделом, 14.07.2000, код подразделения 151-542
пол Мужской, гражданство РОССИЯ
Место и дата рождения: Москва, 10.01.1979.

 [Адреса регистрации и проживания](#)
По документу, удостоверяющему личность: 109012, г Москва, проезд Третьяковский, 1
Фактический: совпадает с адресом по месту регистрации

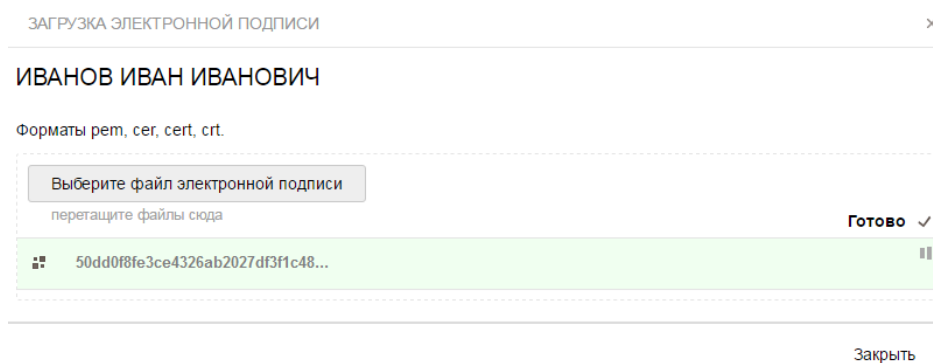
4. Нажмите кнопку **Выберите файл электронной подписи** или переместите файл в указанную область.



5. Выберите файл для загрузки и нажмите кнопку **Открыть**.



6. После успешной загрузки файл сертификата отображается в окне загрузки электронной подписи.



При загрузке файла сертификата осуществляются проверки. В случае ошибочной загрузки пользователь информируется сообщениями на форме.

ЗАГРУЗКА ЭЛЕКТРОННОЙ ПОДПИСИ

×

ИВАНОВ ИВАН ИВАНОВИЧ

Форматы pem, cer, cert, crt.

Выберите файл электронной подписи

перетащите файлы сюда

Загрузка невозможна.

Сертификат просрочен (с 20.05.2015 до 20.05.2016)
Сертификат не является квалифицированным
ФИО Кропикович Петр Петрович, указанные в сертификате, не совпадают с ФИО Иванов Иван Иванович при регистрации

Закреть

Для последнего загруженного сертификата автоматически устанавливается признак «Активный».