

Инструкция по установке и настройке программного обеспечения

Сервис СФЕРА Отчетность

ОГЛАВЛЕНИЕ

НЕОБХОДИМЫЕ КОМПОНЕНТЫ	2
ПОРЯДОК УСТАНОВКИ И НАСТРОЙКИ	3
Установка СКЗИ КриптоПро CSP версии 3.9	3
Установка компонента СФЕРА.....	6
Установка драйвера ключевого носителя	8
Установка драйвера ключевого носителя Rutoken.....	8
Установка драйвера ключевого носителя ESMART Token	10
Установка драйвера ключевого носителя eToken	15
Установка сертификата ключа подписи	17
Установка корневого сертификата.....	23
Настройка браузера Internet Explorer.....	27

НЕОБХОДИМЫЕ КОМПОНЕНТЫ

Для корректной работы системы необходимо, чтобы на рабочей станции было установлено следующее программное обеспечение:

1. Лицензионная операционная система (с последними пакетами обновлений):
 - 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.
3. Интернет браузер Internet Explorer 9.0 и выше.
4. СКЗИ КриптоПро CSP версии 3.6 и выше.
5. Компонент СФЕРА.
6. Драйвер для защищенного носителя ЭП (если таковой используется).

Также необходимо наличие USB-порта и доступа в Интернет.

Компоненты 1-3 должны быть установлены на компьютер самостоятельно; в настоящем руководстве рассматривается только установка компонентов 4-6 и настройка компонента 3.

Все необходимые для установки дистрибутивы можно скачать по указанным в инструкции ссылкам либо с [сайта](#) в разделе «Установка программного обеспечения и настройка сервиса».

ПОРЯДОК УСТАНОВКИ И НАСТРОЙКИ

Установка и настройка компонентов осуществляется в следующем порядке:

1. Установка СКЗИ КриптоПро CSP версии 3.6 и выше.
2. Установка компонента СФЕРА.
3. Установка драйвера ключевого носителя.
4. Установка сертификата ключа подписи.
5. Установка корневого сертификата Удостоверяющего центра.
6. Настройка браузера.

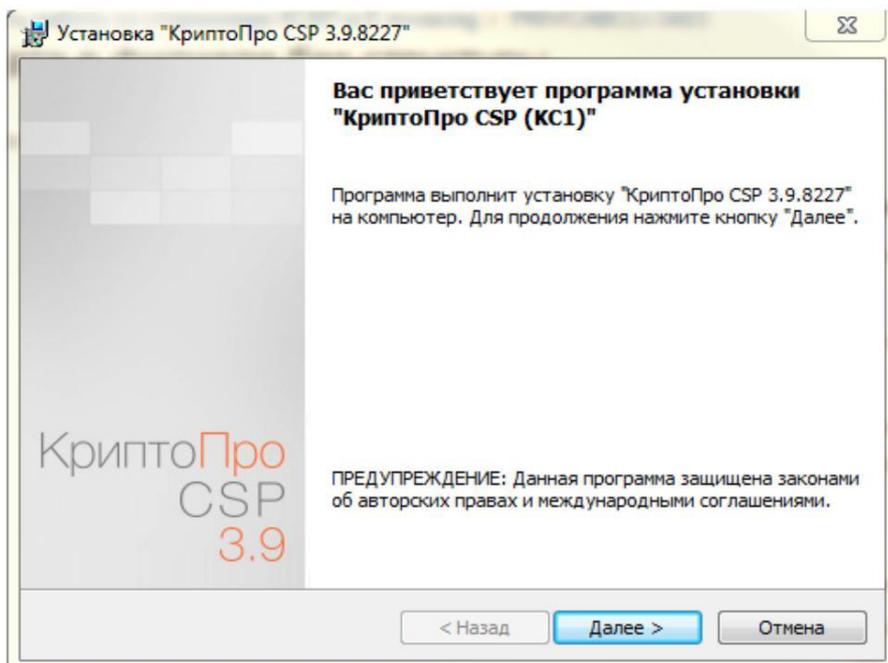
УСТАНОВКА СКЗИ КРИПТОПРО CSP ВЕРСИИ 3.9

Дистрибутив программы СКЗИ КриптоПро CSP можно скачать:

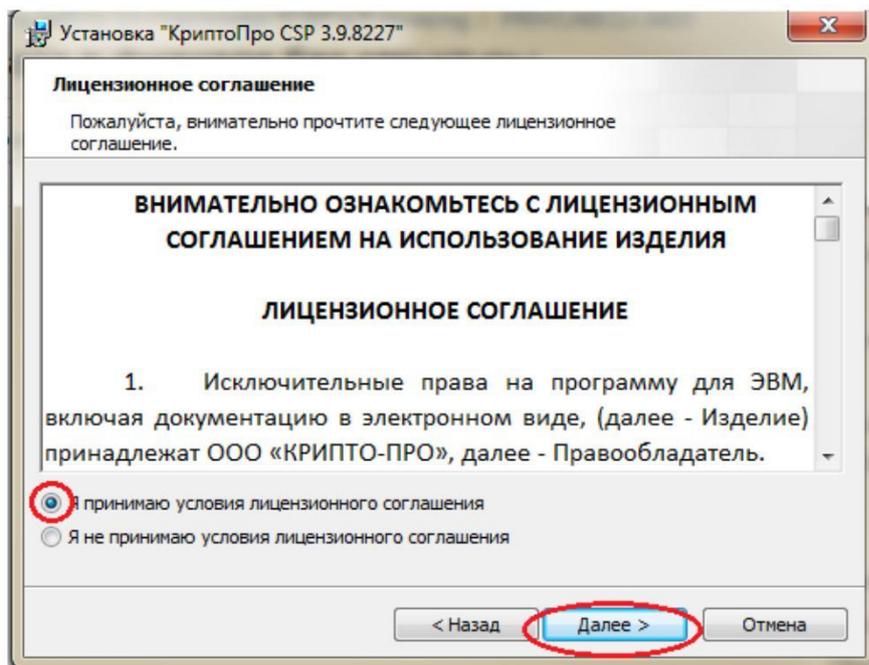
- С [сайта](#) производителя;
- Универсальный установщик:
http://www.esphere.ru/assets/download/uc/csp_3_9_win_universal.zip.

Для установки ПО на компьютер необходимо выполнить следующие действия:

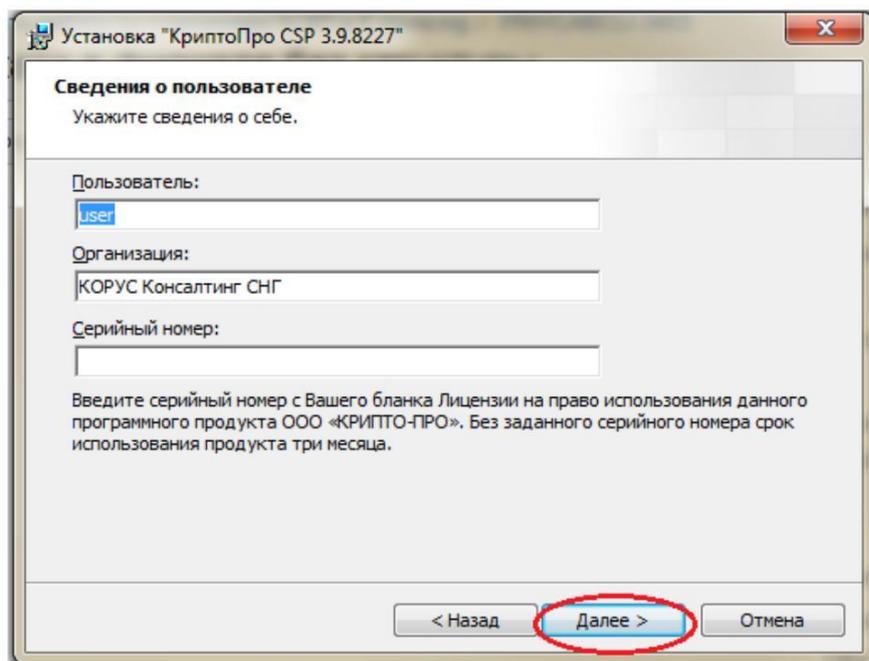
1. Скачайте, разархивируйте и запустите установочный файл программы.
2. В появившемся окне программы установки «КриптоПро CSP (КС1)» нажмите кнопку **Далее**.



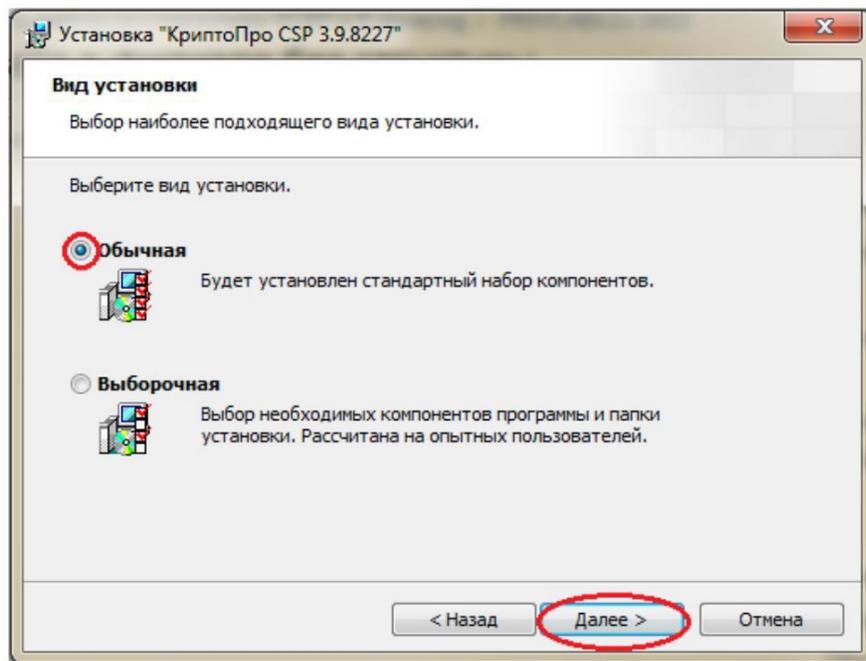
3. Ознакомьтесь с текстом лицензионного соглашения, поставьте отметку **«Я принимаю условия лицензионного соглашения»** и нажмите кнопку **Далее**.



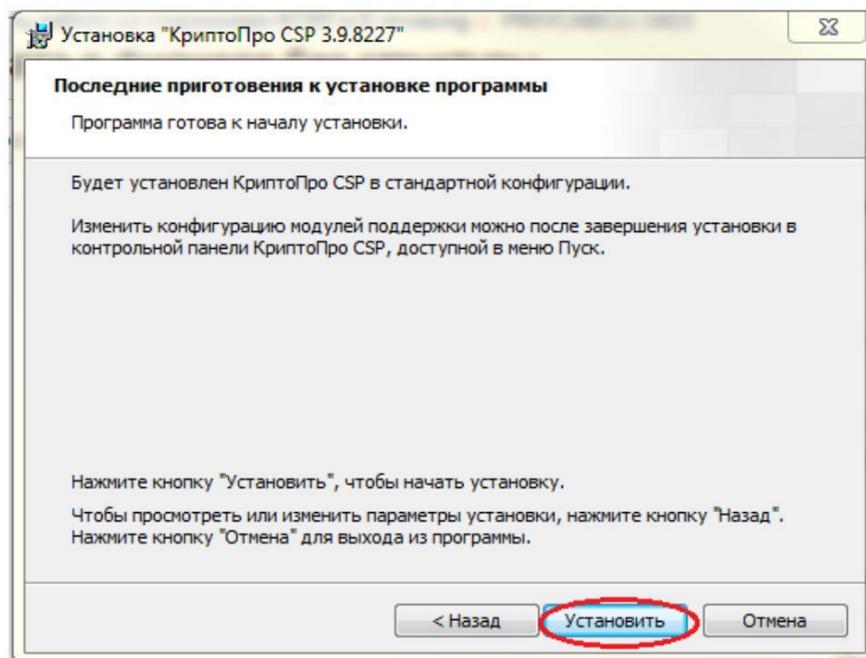
4. В окне «Сведения о пользователе» введите имя, название организации, а также серийный номер, указанный в документе **«Лицензия на использование программного продукта КриптоПро CSP версии 3.9»**, нажмите кнопку **Далее**.



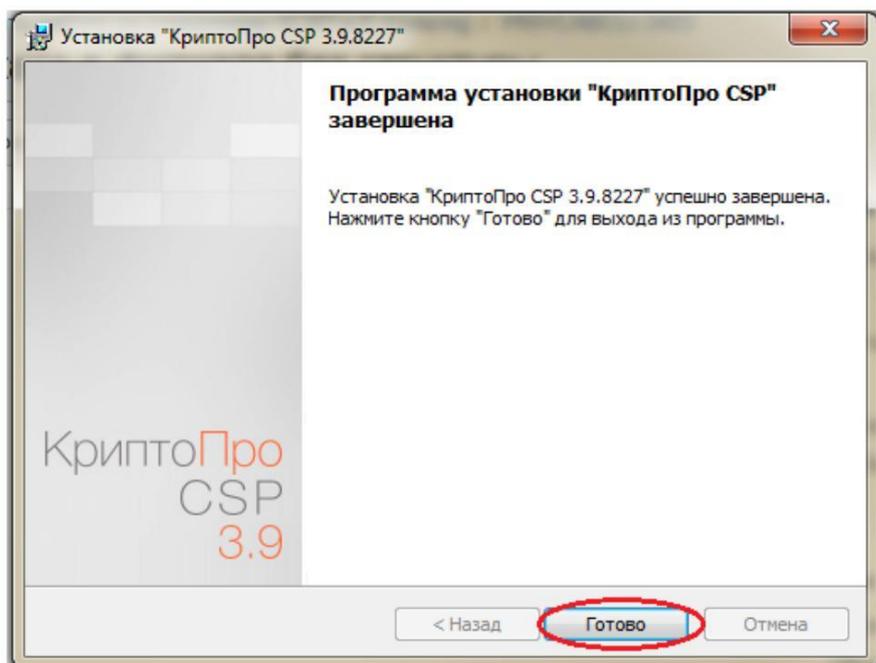
5. В следующем окне выберите вид установки «Обычная» и нажмите кнопку **Далее**.



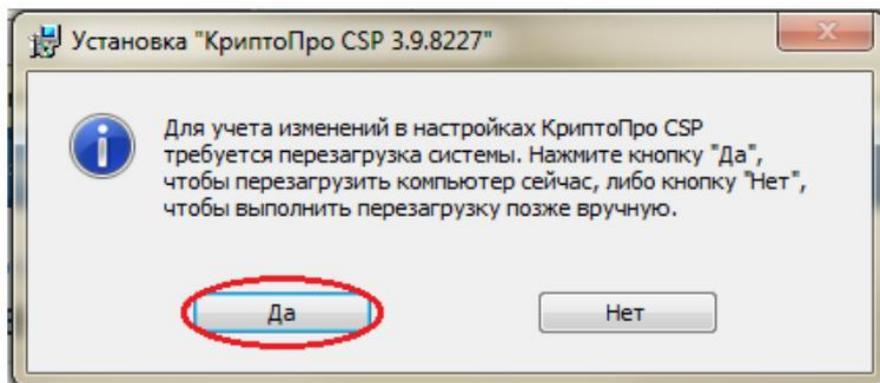
6. Нажмите кнопку **Установить**.



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



8. Для завершения процесса установки программы необходимо перезагрузить компьютер. При появлении окна «Сведения о программе установки КриптоПро CSP» с предложением перезагрузки, нажмите кнопку **Да**.

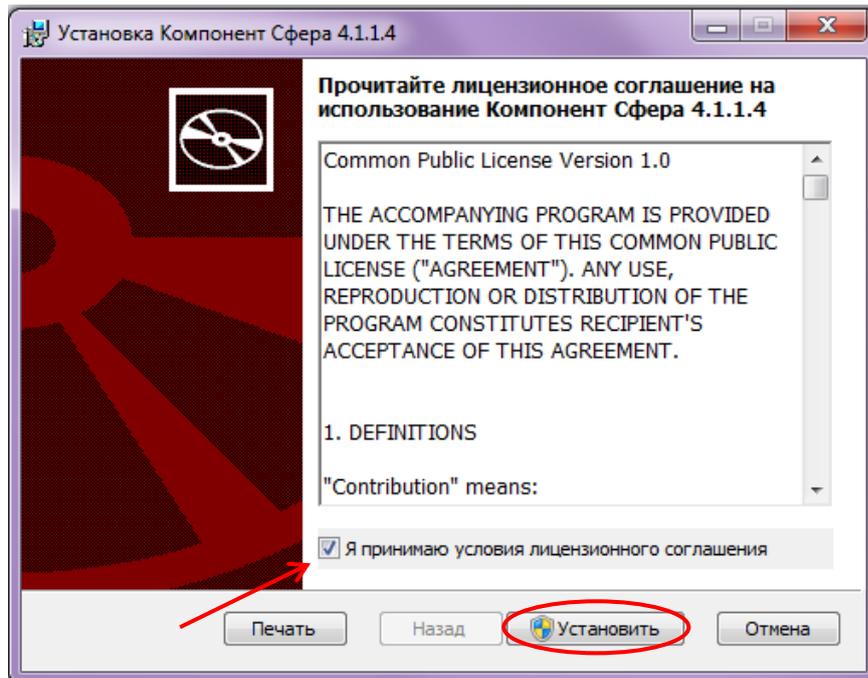


УСТАНОВКА КОМПОНЕНТА СФЕРА

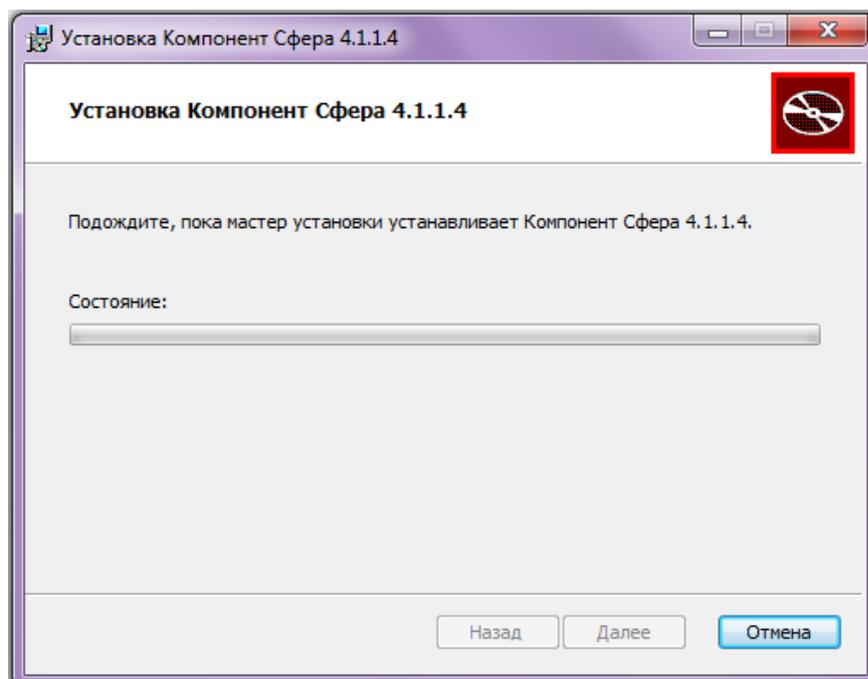
Компонент СФЕРА можно скачать по ссылке:

<http://www.esphere.ru/assets/download/nalogov/SphereClientSetup.zip>.

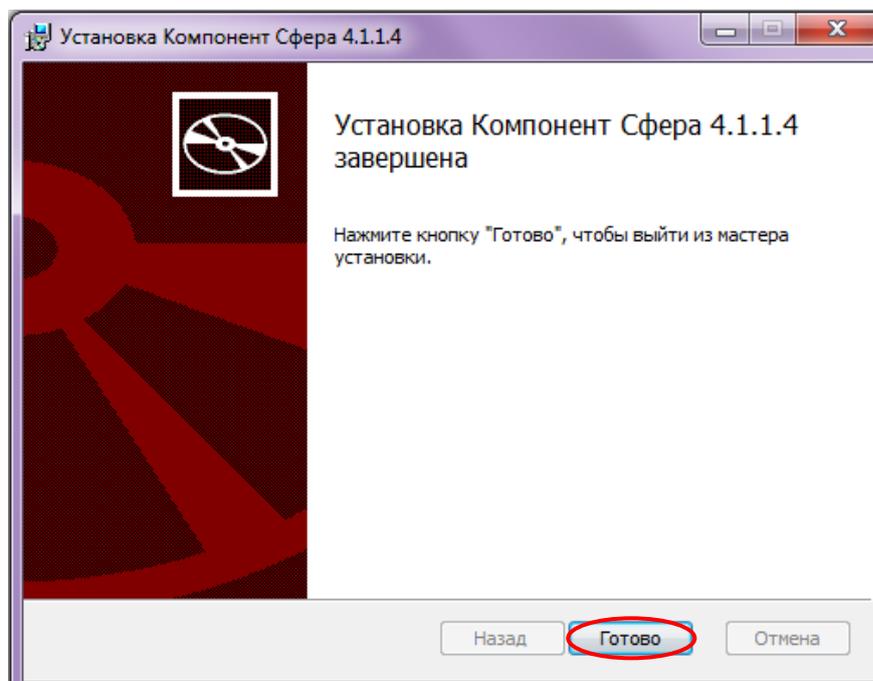
1. Скачайте, разархивируйте и запустите установочный файл.
2. В окне мастера установки ознакомьтесь с текстом лицензионного соглашения, поставьте отметку «**Я принимаю условия лицензионного соглашения**» и нажмите кнопку **Установить**.



3. Дождитесь окончания установки компонента СФЕРА.



4. Нажмите кнопку **Готово**.



УСТАНОВКА ДРАЙВЕРА КЛЮЧЕВОГО НОСИТЕЛЯ

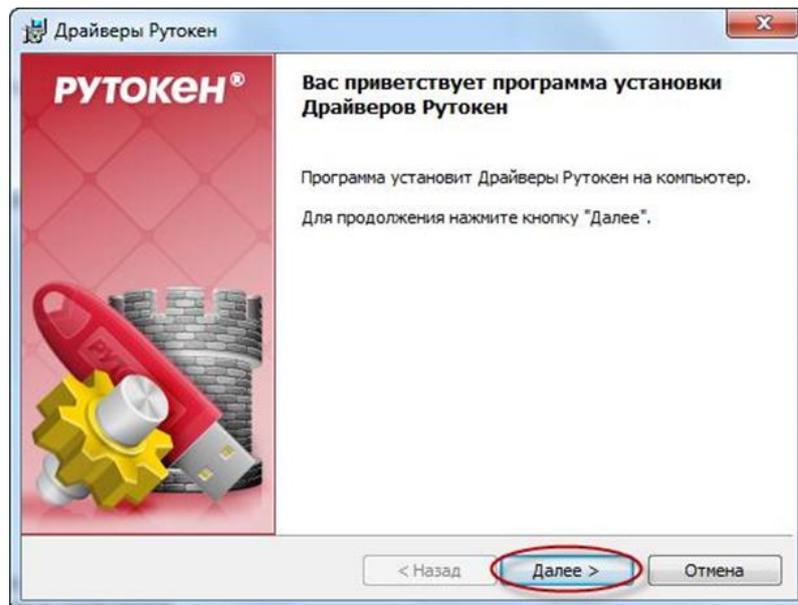
Для работы с ЭП на любом физическом носителе необходима установка драйвера ключевого носителя ЭП (Rutoken, ESMART Token, eToken и т. д.). В данном руководстве представлено описание установки драйвера ключевого носителя [Rutoken](#), [ESMART Token](#), [eToken](#).

Установка драйвера ключевого носителя Rutoken

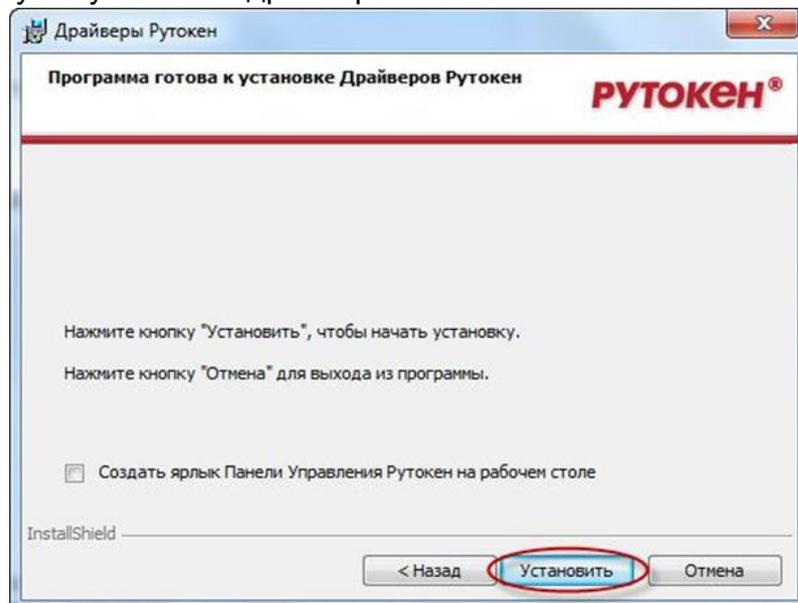
Универсальный установщик драйвера ключевого носителя Rutoken можно скачать с [сайта](#):

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

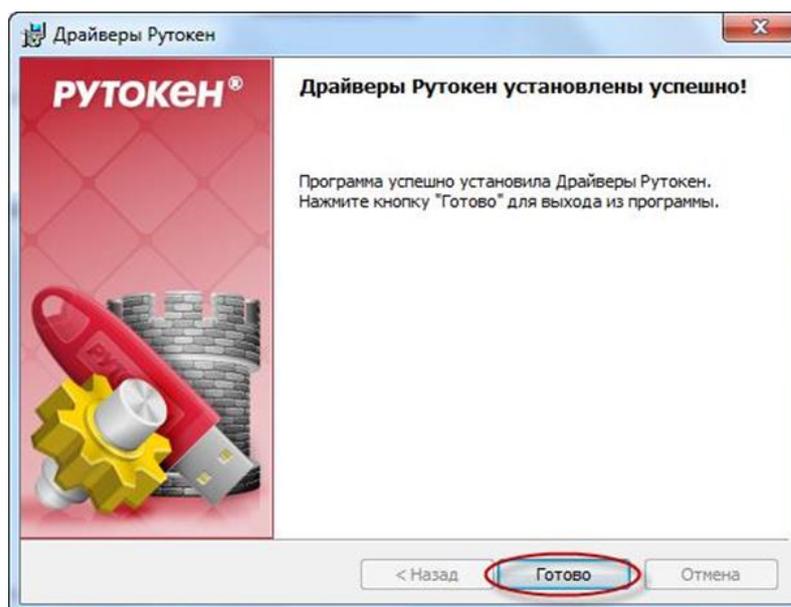
1. Запустите установочный файл драйвера.
2. В открывшемся окне установки нажмите кнопку **Далее**.



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



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

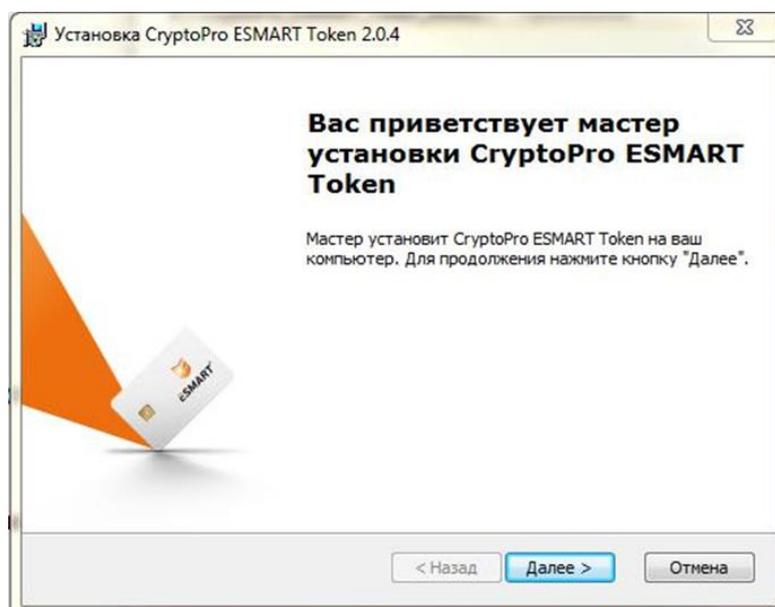


Установка драйвера ключевого носителя ESMART Token

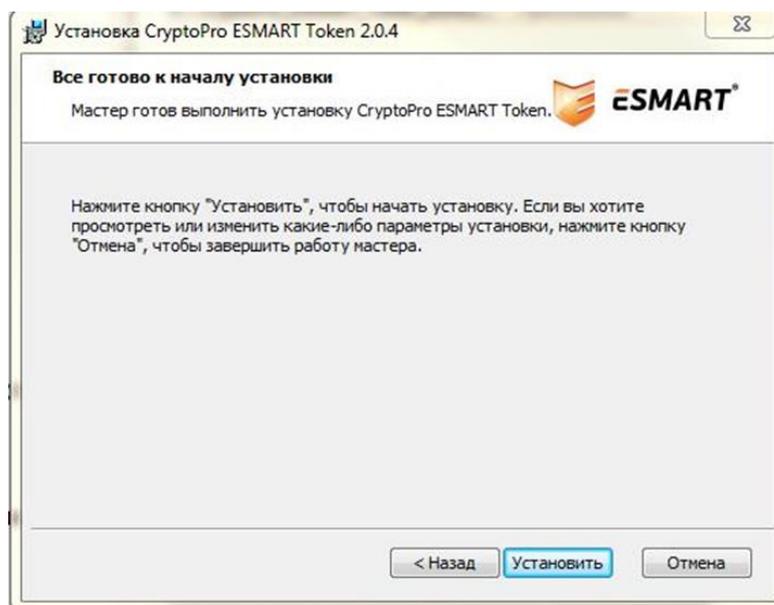
ESMART Token поддерживается в СКЗИ "КриптоПро CSP", начиная с версии 3.6 R3. Для более ранних версий необходимо установить модуль поддержки, который можно скачать по ссылке:

[Модуль поддержки ESMART Token КриптоПро CSP для Windows](#) .

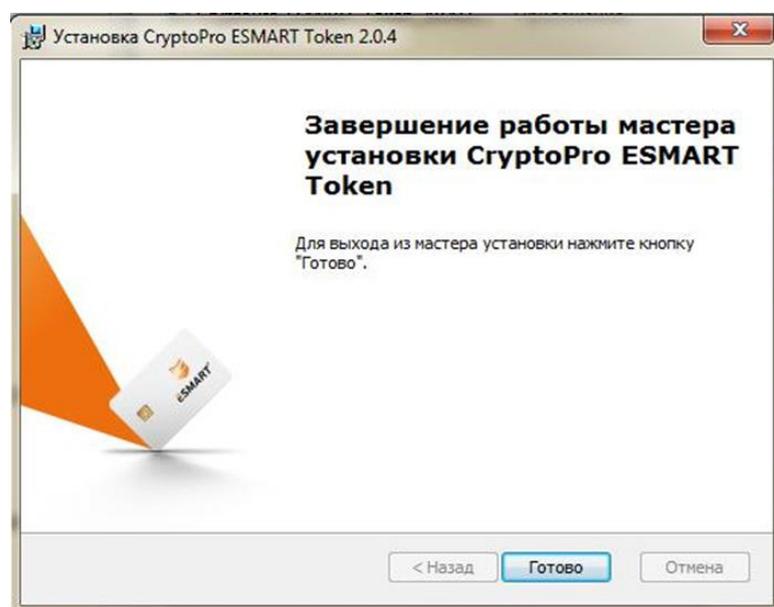
1. Запустите установочный файл.
2. Выберите язык установки.
3. В открывшемся окне установки нажмите кнопку **Далее**.



4. Для запуска установки CryptoPro ESMART Token нажмите кнопку **Установить**.



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



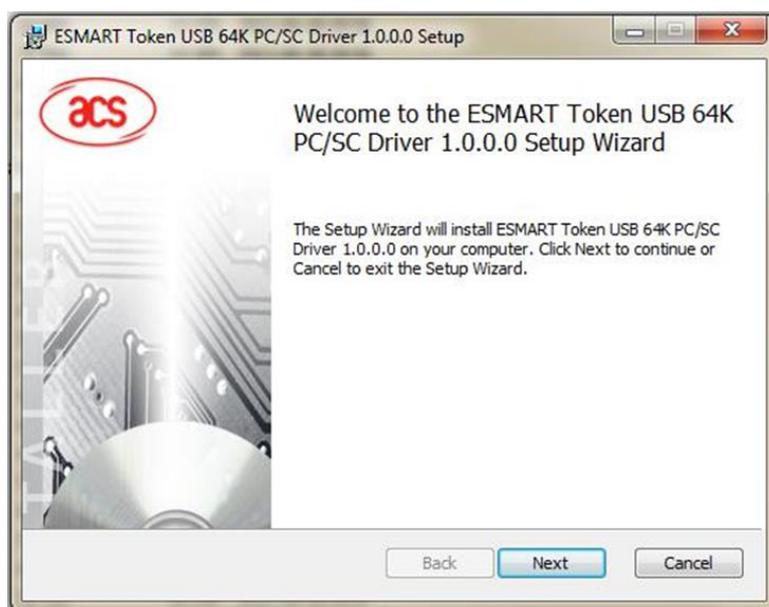
В случае, когда обновление Windows производится регулярно, установка драйвера ключевого носителя не требует дополнительных операций – при первом использовании драйвер автоматически скачивается из центра обновлений.

Иначе драйверы для USB-ключа ESMART Token 64K можно скачать по следующей ссылке:

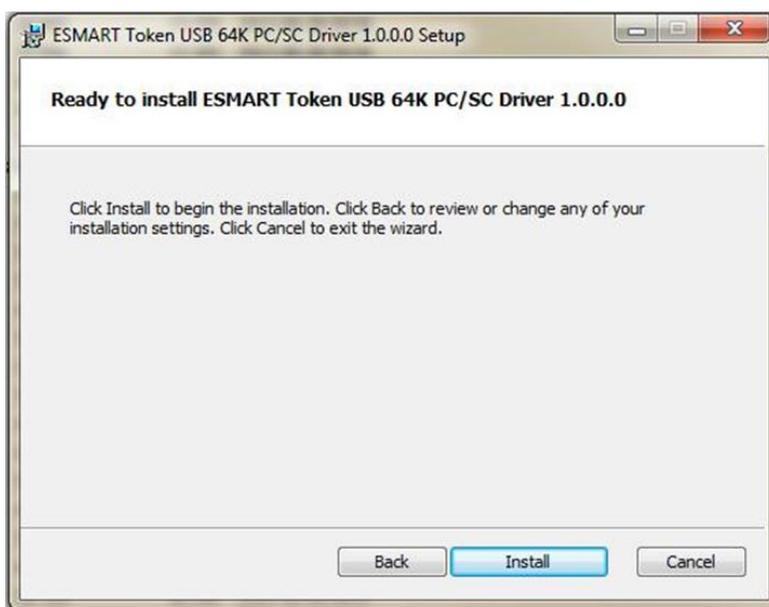
[Драйвер ESMART Token USB 64K для Windows.](#)

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

6. Запустите установочный файл драйвера.
7. В открывшемся окне установки нажмите кнопку **Next**.



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



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

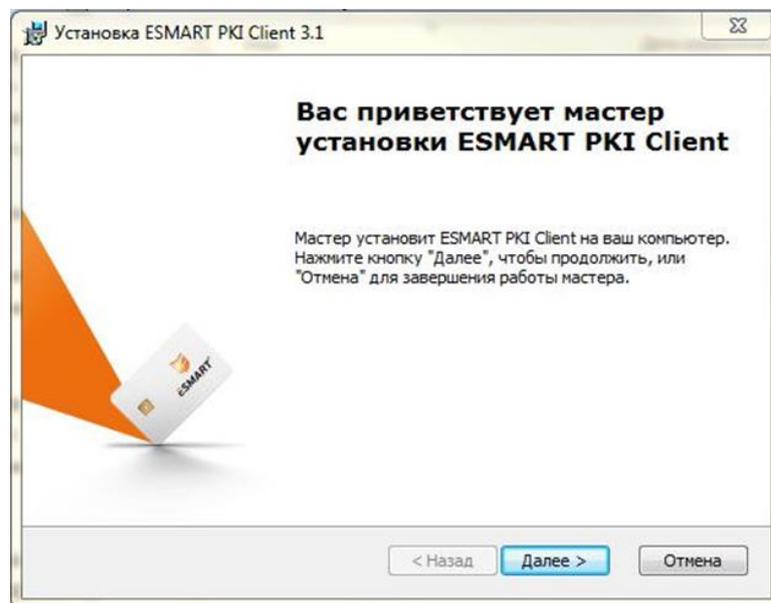


Для операции с ключами ESMART Token без использования командной строки: например, для изменения пин-кодов, необходима установка ПО ESMART PKI Client.

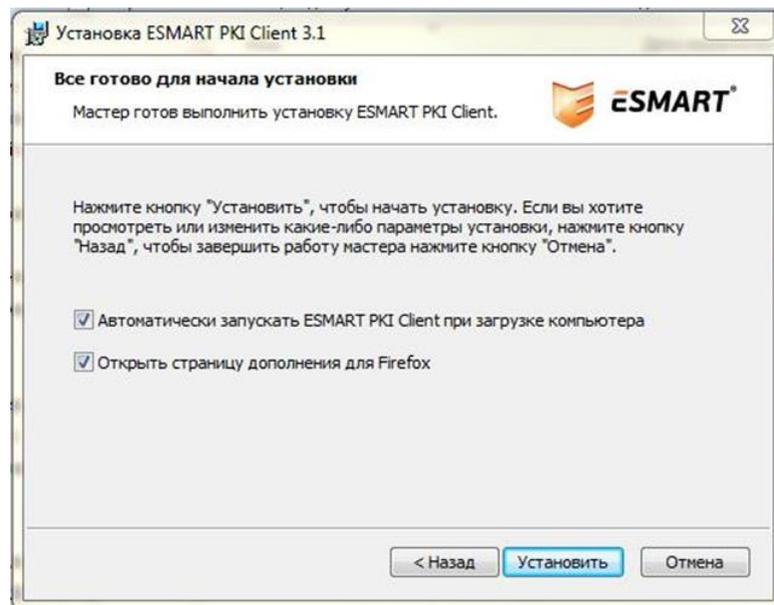
Установочный файл ESMART PKI Client для Windows можно скачать по следующей ссылке:

[ESMART PKI Client для Windows.](#)

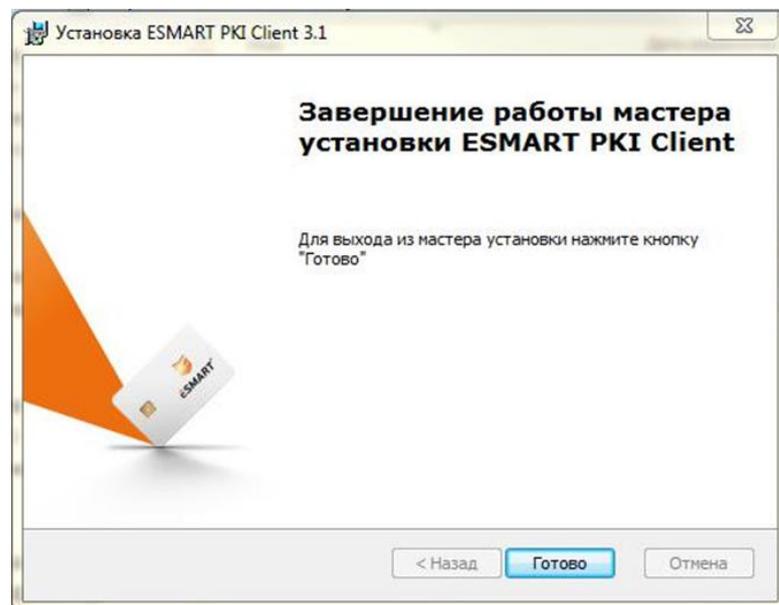
1. Запустите установку **setup**.
2. В открывшемся окне установки нажмите кнопку **Далее**.



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



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



Рекомендуется провести замену пин-кода для обеспечения безопасного хранения ключевой информации. Для этого:

1. Зайдите в меню «Пуск» – «ESMART» – «ESMART PKI Client».
2. Нажмите кнопку **Авторизоваться**, введите Ваш текущий пин-код, нажмите ОК.
3. Нажмите кнопку **Сменить PIN-код**, введите новый пин-код.

Внимание! В случае утраты нового пин-кода, восстановить его будет **невозможно!**

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.

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

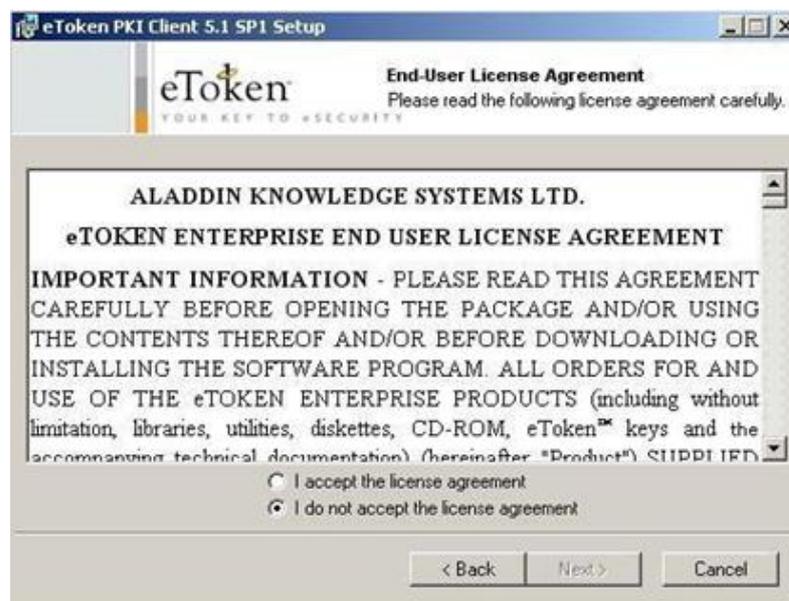


3. В списке доступных языков интерфейса выберите Russian (Русский) и нажмите кнопку **Next**.

Если в этом окне вам будет предложено сохранить настройки, оставшиеся от предыдущей версии, вы можете оставить отметку (сохранить настройки) или снять отметку (удалить настройки).



4. В окне с текстом лицензионного соглашения (на английском языке) внимательно прочитайте лицензионное соглашение, и, если вы согласны со всеми условиями, отметьте пункт **I accept the license agreement** и нажмите кнопку **Next**. Если вы не понимаете или не согласны с каким-либо пунктом, откажитесь от установки, нажмите кнопку **Cancel**.



5. После принятия соглашения в открывшемся окне укажите путь для установки (нажмите кнопку **Browse**), или оставьте по умолчанию. Для запуска установки нажмите кнопку **Next**.



6. После установки программы в окне с соответствующим подтверждающим сообщением нажмите кнопку **Finish**.

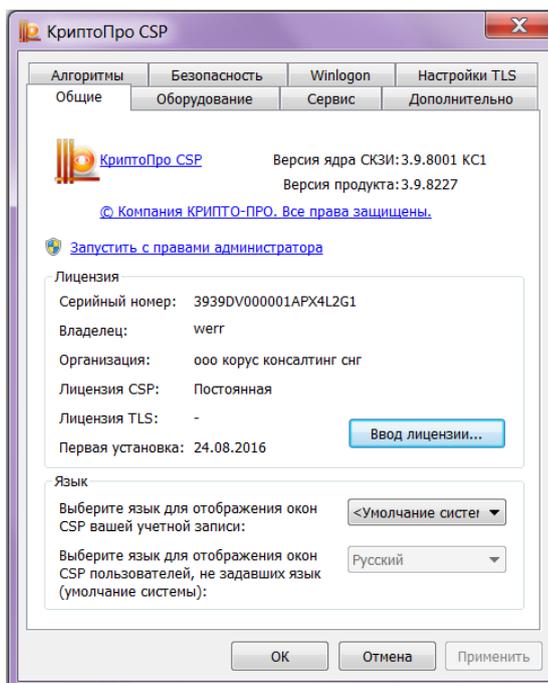


УСТАНОВКА СЕРТИФИКАТА КЛЮЧА ПОДПИСИ

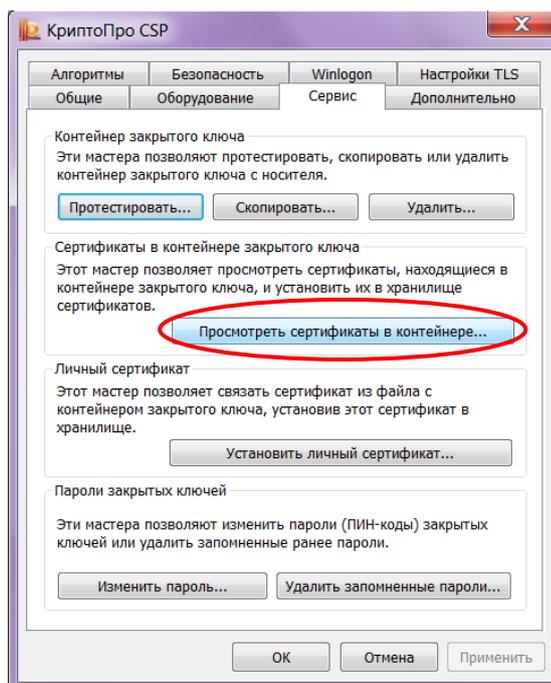
Внимание! Перед установкой сертификата ключа подписи необходимо вставить ключевой носитель в USB-порт компьютера.

Если у вас имеется несколько сертификатов ключей подписи, указанные действия необходимо произвести для каждого сертификата.

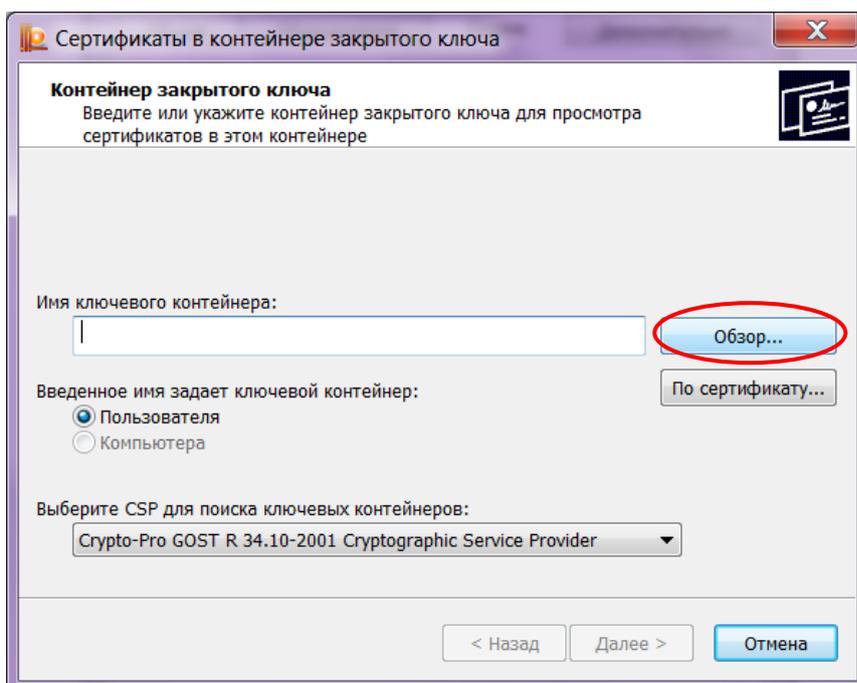
1. Запустите **КриптоПро CSP** (Пуск -> Панель Управления -> КриптоПро CSP).



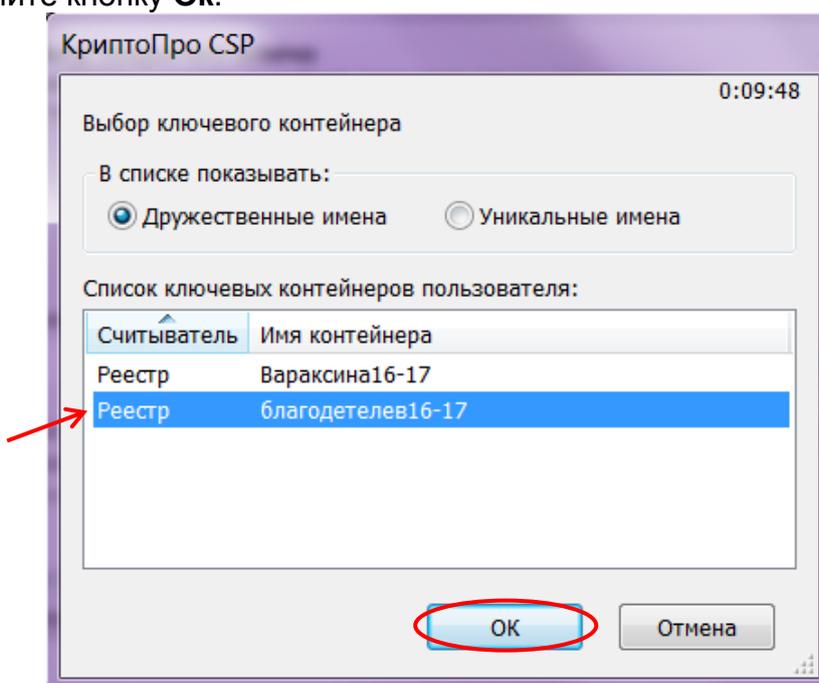
2. Выберите вкладку «Сервис» и нажмите кнопку **Просмотреть файлы в контейнере**.



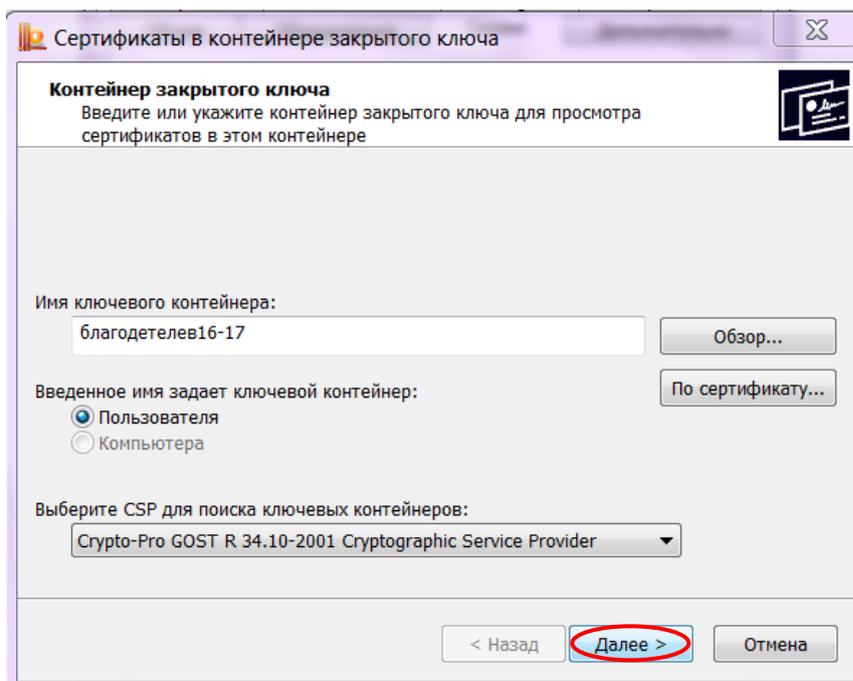
3. В окне «Сертификаты в контейнере закрытого ключа» нажмите кнопку **Обзор**.



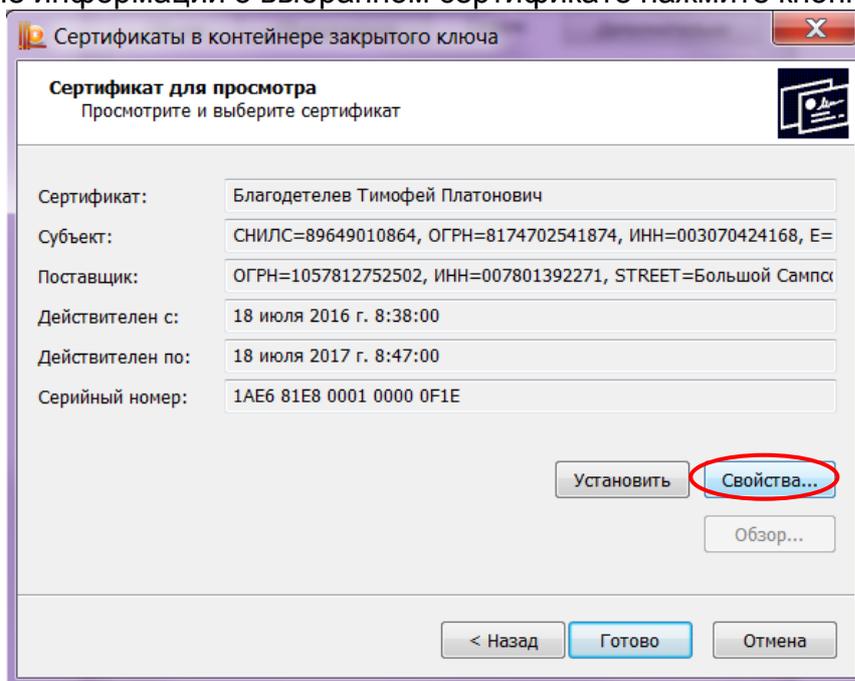
4. В списке ключевых носителей выберите нужный личный сертификат и нажмите кнопку **Ок**.



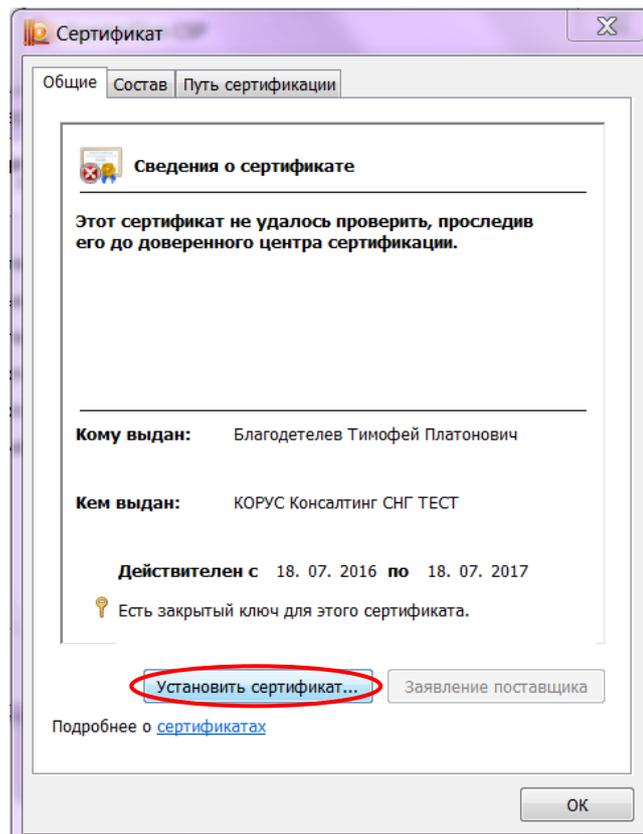
5. Нажмите кнопку **Далее** для продолжения установки.



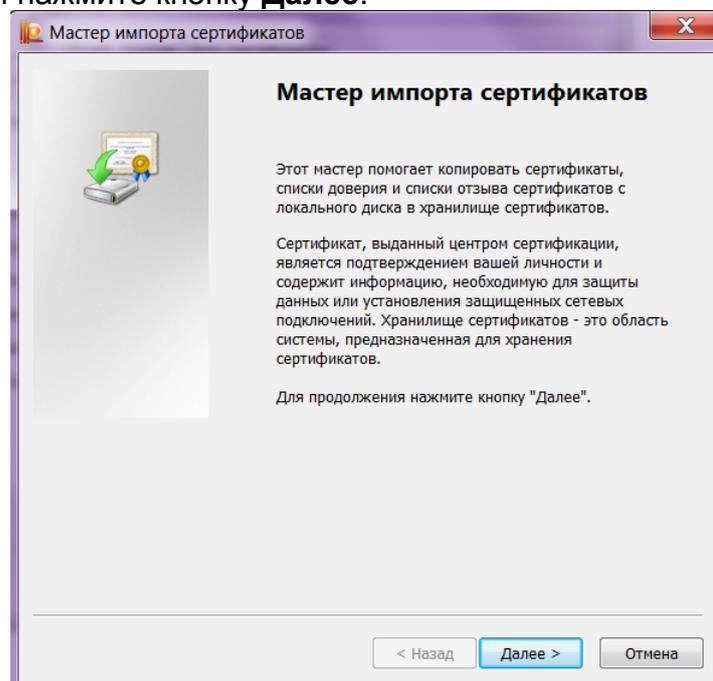
6. В окне информации о выбранном сертификате нажмите кнопку **Свойства**.



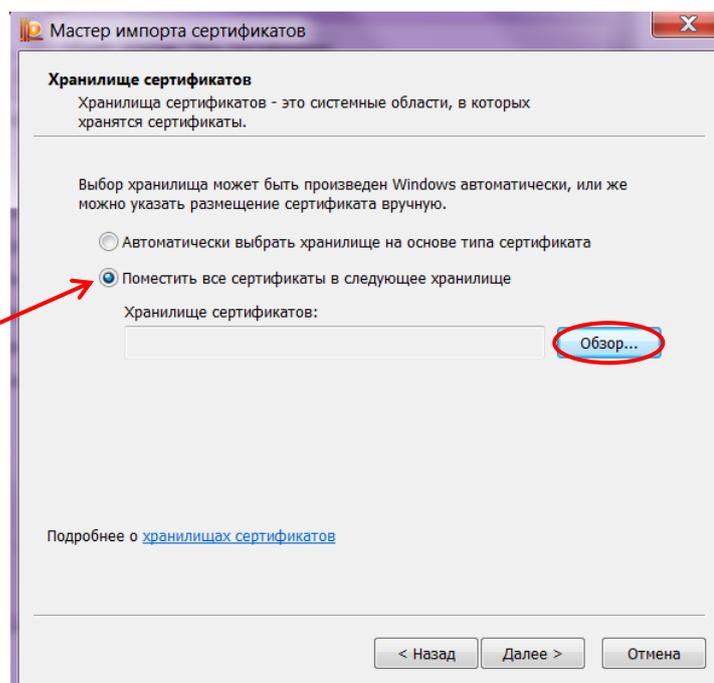
7. В открывшемся окне сертификата нажмите кнопку **Установить сертификат**.



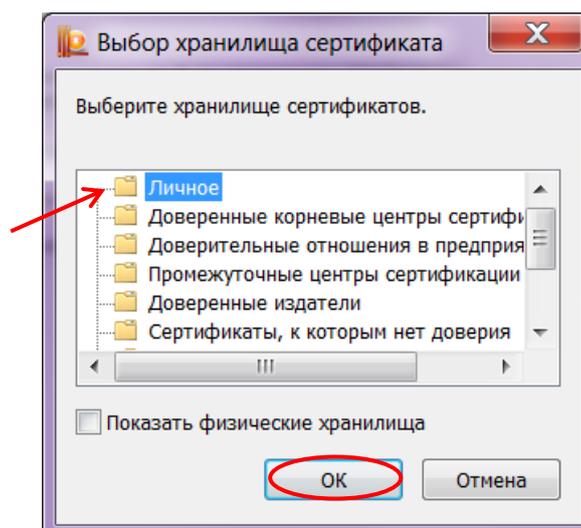
8. Далее будет запущен **Мастер импорта сертификатов**. Для продолжения установки нажмите кнопку **Далее**.



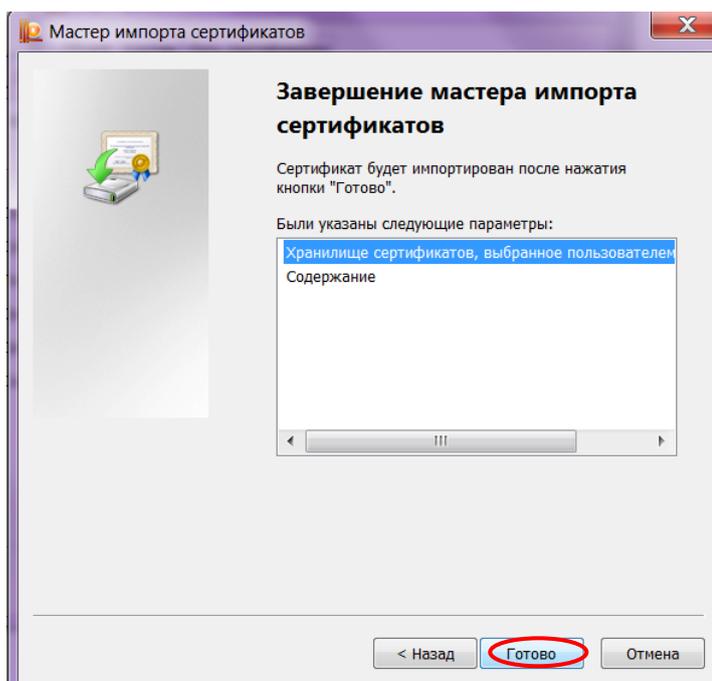
9. В появившемся окне поставьте отметку **Поместить все сертификаты в следующее хранилище** и нажмите кнопку **Обзор**.



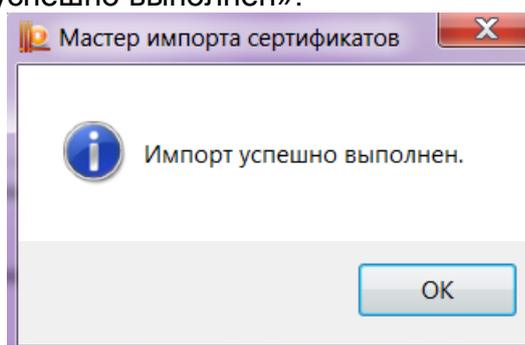
10. В списке хранилищ выберите хранилище «Личное», нажмите кнопку **Ок** и **Далее**.



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



В случае успешного импорта сертификата в хранилище будет выведено сообщение: «Импорт успешно выполнен».



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:

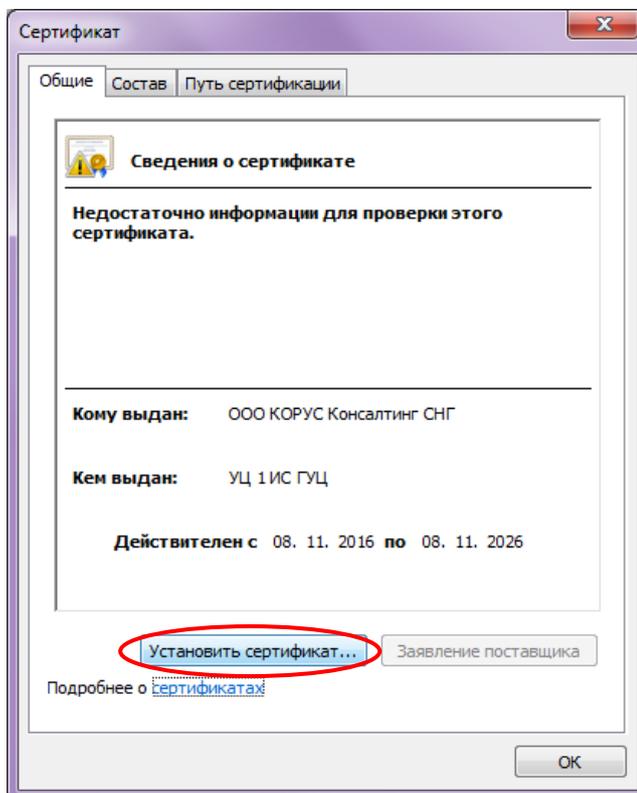
[Доверенный корневой сертификат Удостоверяющего центра ООО "КОРУС Консалтинг СНГ";](#)

- 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:

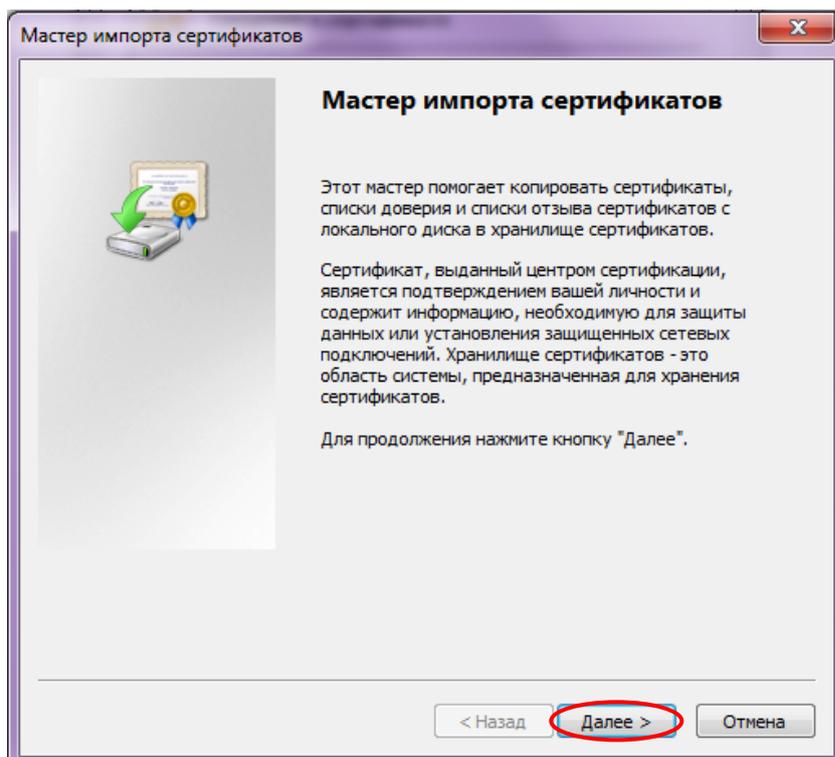
Доверенный корневой сертификат Головного удостоверяющего центра Минкомсвязи.

Для установки корневого сертификата выполните следующие шаги:

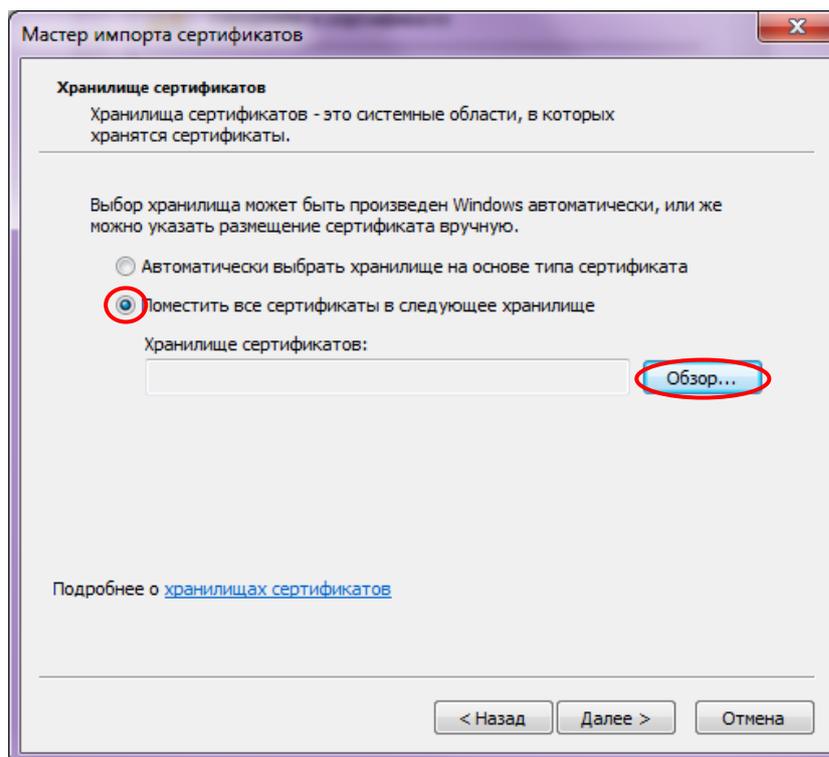
1. Откройте файл корневого сертификата.
2. Нажмите кнопку **Установить сертификат**.



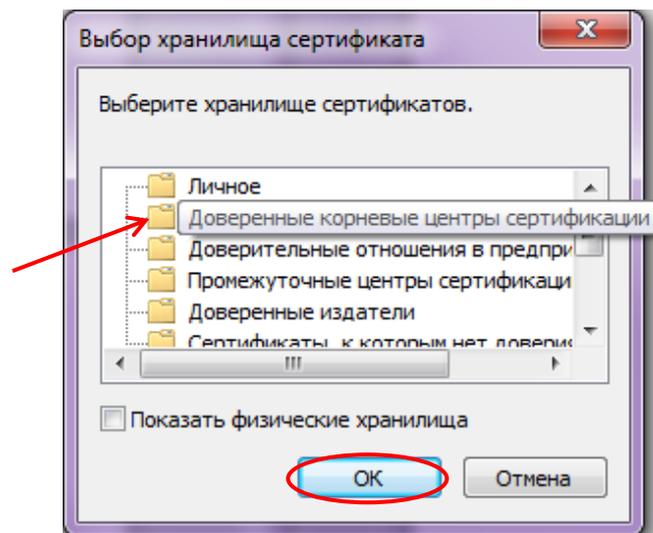
3. После этого запустится «Мастер импорта сертификатов». Для продолжения установки нажмите кнопку **Далее**.



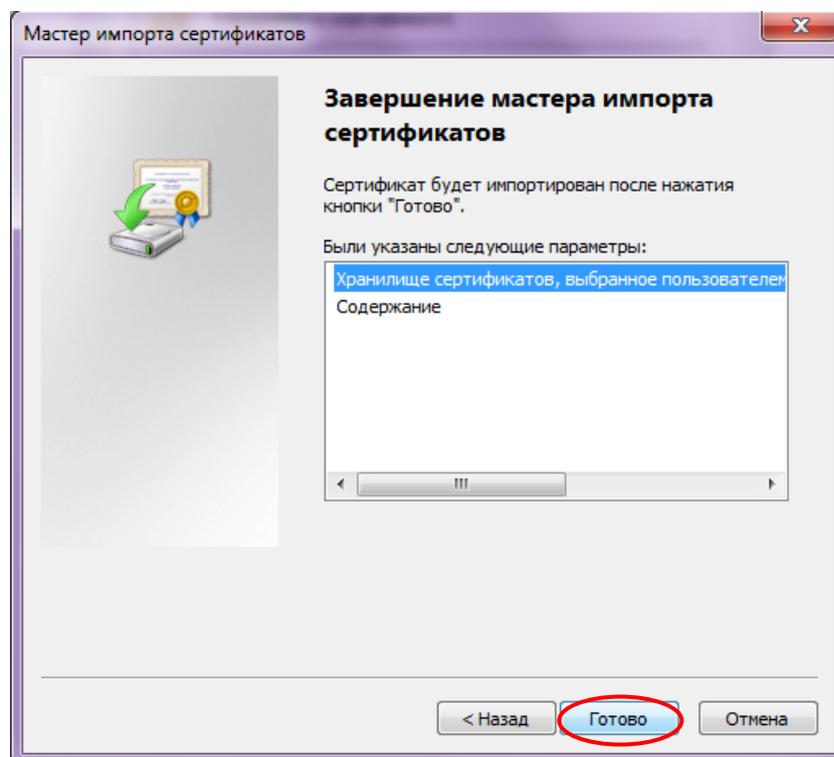
4. Установите отметку «Поместить все сертификаты в следующее хранилище» и нажмите кнопку **Обзор**.



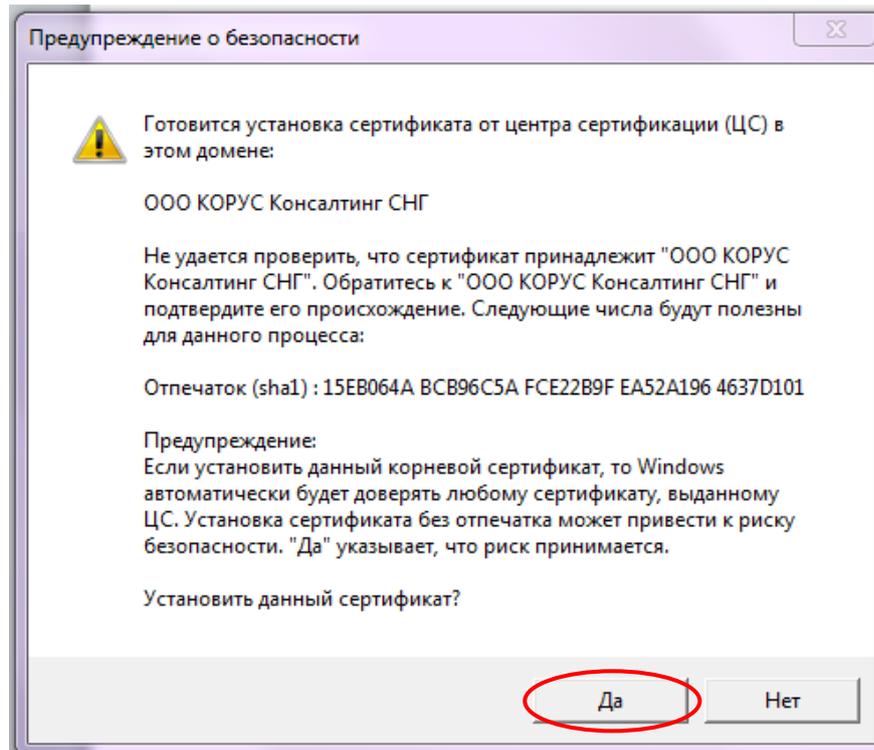
5. Выберите хранилище «Доверенные корневые центры сертификации», нажмите **ОК** и **Далее**.



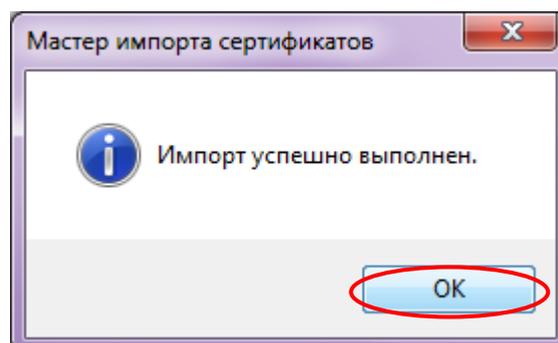
6. Нажмите кнопку **Готово** для завершения установки сертификата.



7. Нажмите кнопку **Да** для подтверждения доверия к данному издателю сертификата.



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

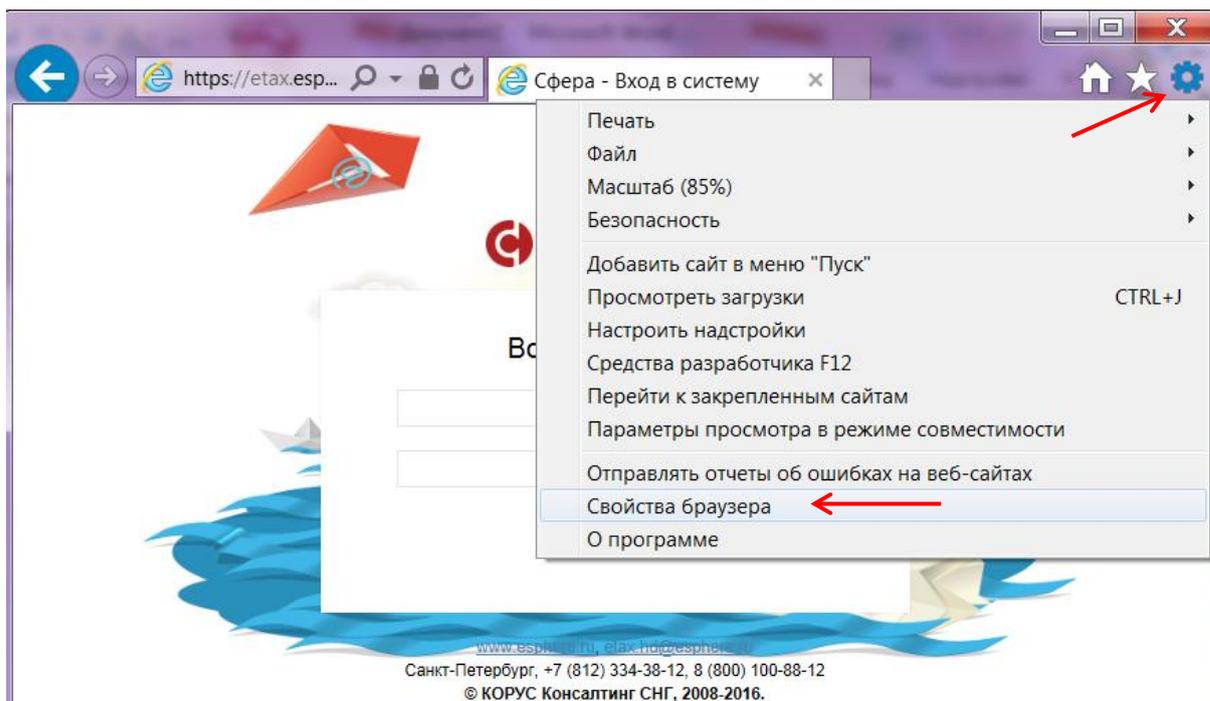


НАСТРОЙКА БРАУЗЕРА INTERNET EXPLORER

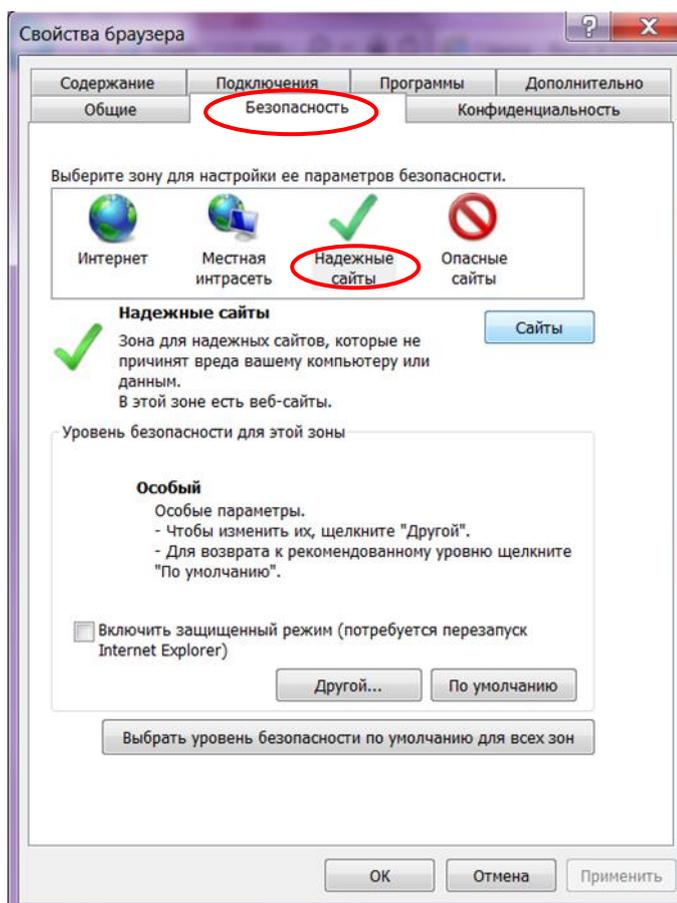
При работе с системой СФЕРА Отчетность используется только 32-разрядная версия Internet Explorer.

***Примечание:** Если у вас установлена 64-разрядная ОС Windows, убедитесь, что для работы с системой СФЕРА Отчетность вы используете 32-разрядную версию браузера.*

1. Для настройки **Internet Explorer**, необходимо войти в меню «Сервис» -> «Свойства браузера».

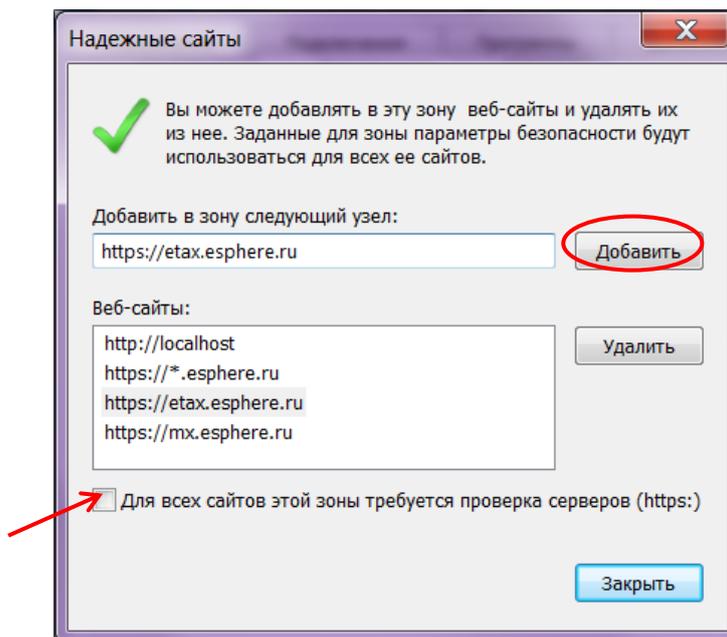


- В открывшемся окне «Свойства браузера» перейдите на вкладку «Безопасность». Выберите пункт «Надежные сайты» и нажмите кнопку **Сайты**.

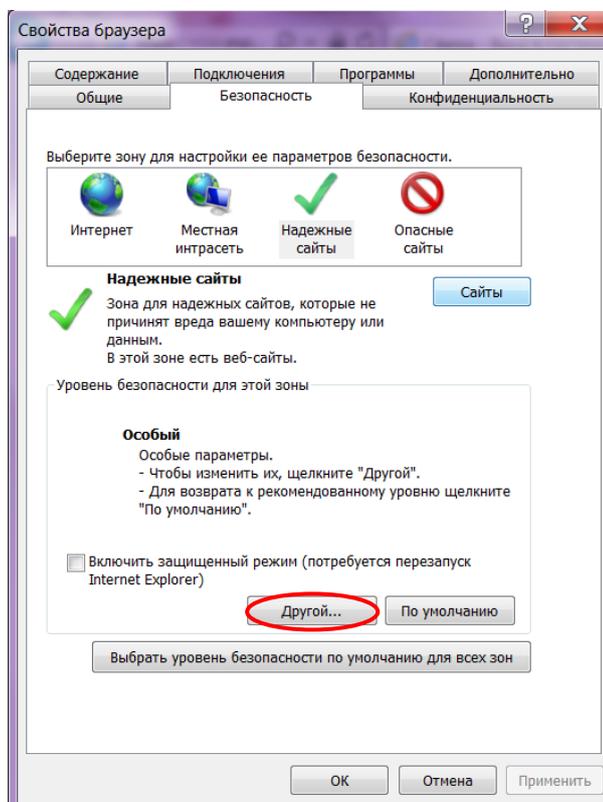


- В открывшемся окне «Надежные сайты» в поле «Добавить в зону следующий узел» введите адрес <https://etax.esphere.ru> и нажмите

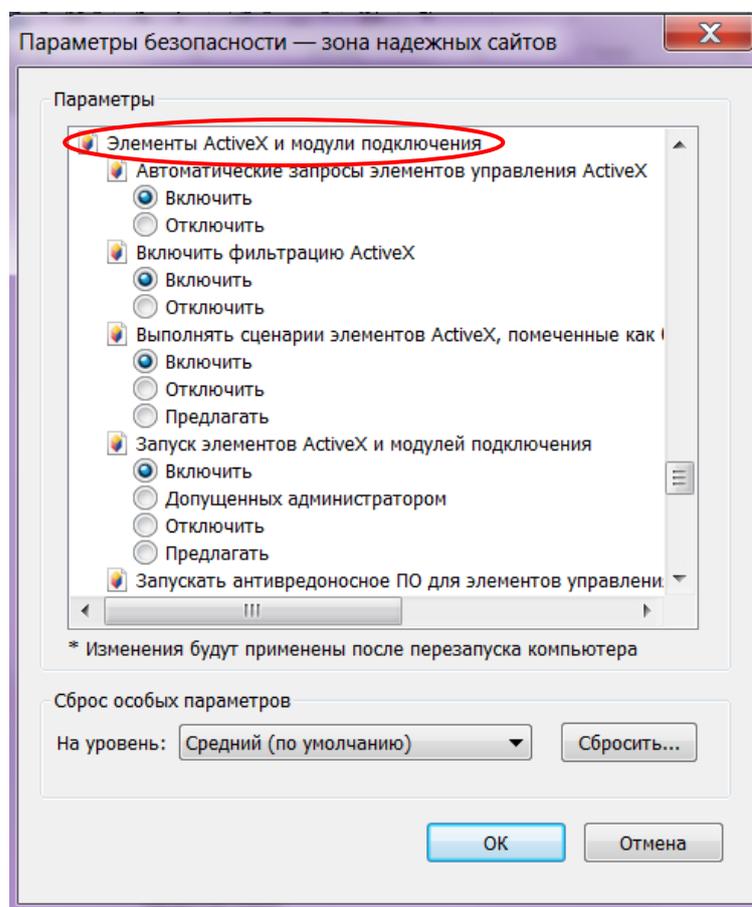
Добавить. Снимите флаг «Для всех узлов этой зоны требуется проверка серверов», если он установлен.



4. Адрес системы СФЕРА Отчетность будет добавлен в список надежных сайтов. Нажмите кнопку **Заккрыть**.
5. После добавления адреса системы СФЕРА Отчетность в надежные узлы во вкладке «Безопасность» нажмите кнопку **Другой**, откроется окно «Параметры безопасности – зона надежных сайтов».



6. В открывшемся окне в настройках безопасности найдите раздел «Элементы ActiveX и модули подключения» и включите следующие настройки:
- Автоматические запросы элементов управления ActiveX;
 - Выполнять сценарии элементов ActiveX, помеченные как безопасные;
 - Загрузка неподписанных элементов ActiveX;
 - Загрузка подписанных элементов ActiveX;
 - 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.
7. Нажмите кнопку **Ок** и перезапустите браузер.



*Поздравляем! Ваше программное обеспечение готово к работе с системой
СФЕРА Отчетность.*
