



центр развития
перспективных технологий

ООО «Оператор ЦРПТ»

129090, Россия, Москва, Проспект Мира, 6

info@crpt.ru, www.crpt.ru

РУКОВОДСТВО ПО УСТАНОВКЕ И НАСТРОЙКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РАБОТЫ С ЭЛЕКТРОННОЙ ПОДПИСЬЮ НА ПОРТАЛЕ ГИС МТ

ООО «Оператор-ЦРПТ»
2020 г.

Оглавление

Список сокращений	3
Системные требования	4
Требования к криптографическому ПО	4
при использовании носителя РУТОКЕН ЭЦП 2.0 со встроенным криптопровайдером:.....	4
при использовании носителей без встроенного криптопровайдера:	4
Настройка для работы с носителем Рутокен ЭЦП 2.0.....	5
Установка комплекта "Драйверы Рутокен для Windows"	5
Установка Рутокен Плагин	6
Настройка рабочего места для работы с носителями без встроенного криптопровайдера	9
Установка криптопровайдера.....	9
КриптоПро CSP	9
VipNet CSP	11
Установка КриптоПро ЭЦП Browser plug-in	13
Выстраивание цепочки доверия личному сертификату	16
Установка корневого сертификата Минкомсвязи России в хранилище «Доверенные корневые центры».....	18
Установка сертификата Удостоверяющего Центра в хранилище «Промежуточные центры сертификации»	21
Установка сертификата в хранилище Личные	22
Техподдержка	25

Список сокращений

ГИС МТ	информационная система маркировки и оборота товаров
СКЗИ	программа (служба), которая обеспечивает шифрование и расшифровку документов, отвечает за работу с электронной подписью. СКЗИ может быть встроена в носитель или представлена как отдельный программный продукт
КСКПЭП	квалифицированный сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным 63-ФЗ и иными нормативно-правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи
КЭП	квалифицированная электронная подпись - уникальная последовательность символов, предназначенная для создания электронной подписи
УЦ	юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей

Системные требования

- ОПЕРАЦИОННАЯ СИСТЕМА:
Windows 7 и выше, Mac OS X 10.8 и выше
- БРАУЗЕР:
[Google Chrome 70](#), [Mozilla Firefox 60](#), [Internet Explorer 11](#), [Safari 12](#)

Требования к криптографическому ПО

при использовании носителя РУТОКЕН ЭЦП 2.0 со встроенным криптопровайдером:

- [Драйверы Рутокен](#)
- [Рутокен Плагин](#)

при использовании носителей без встроенного криптопровайдера:

- Криптопровайдер с поддержкой формирования и проверки подписи по ГОСТ Р 34.10-2012 ([КриптоПро CSP](#), [VipNet CSP](#) и пр.)
- [КриптоПро ЭЦП Browser plug-in](#)
- Построенная цепочка доверия личному сертификату пользователя

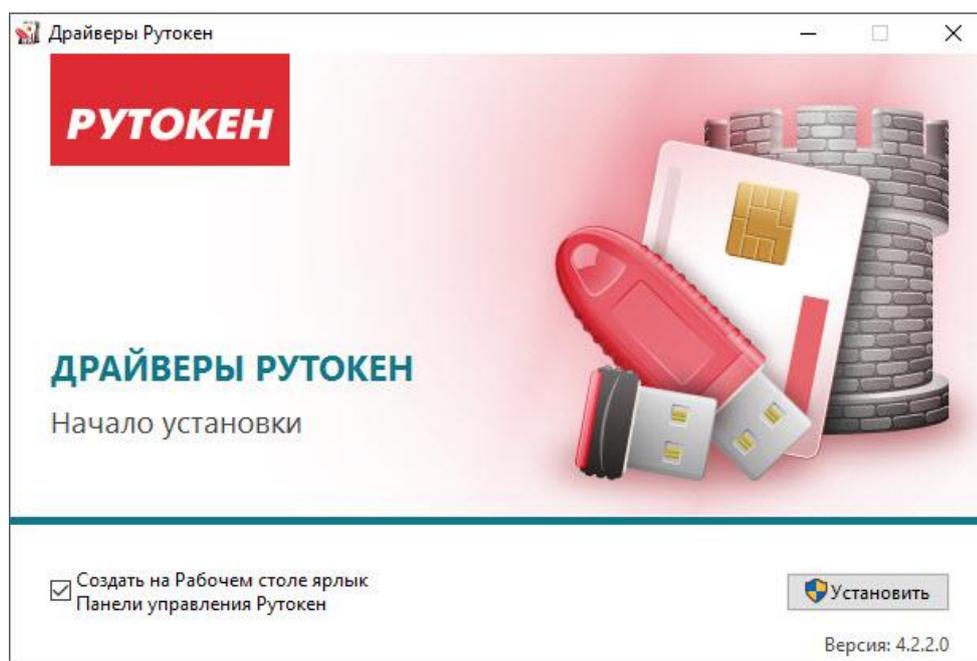
Настройка для работы с носителем Рутокен ЭЦП 2.0

Установка комплекта "Драйверы Рутокен для Windows"

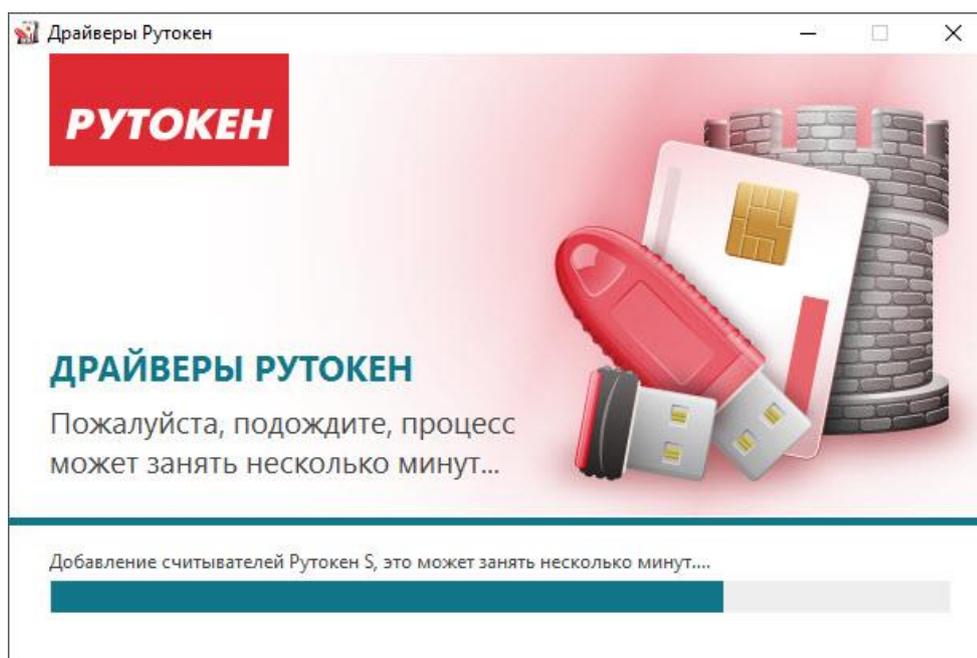
Для работы с носителями Рутокен установите комплект драйверов. Актуальная версия доступна на сайте производителя по [ссылке](#):

Для установки комплекта драйверов:

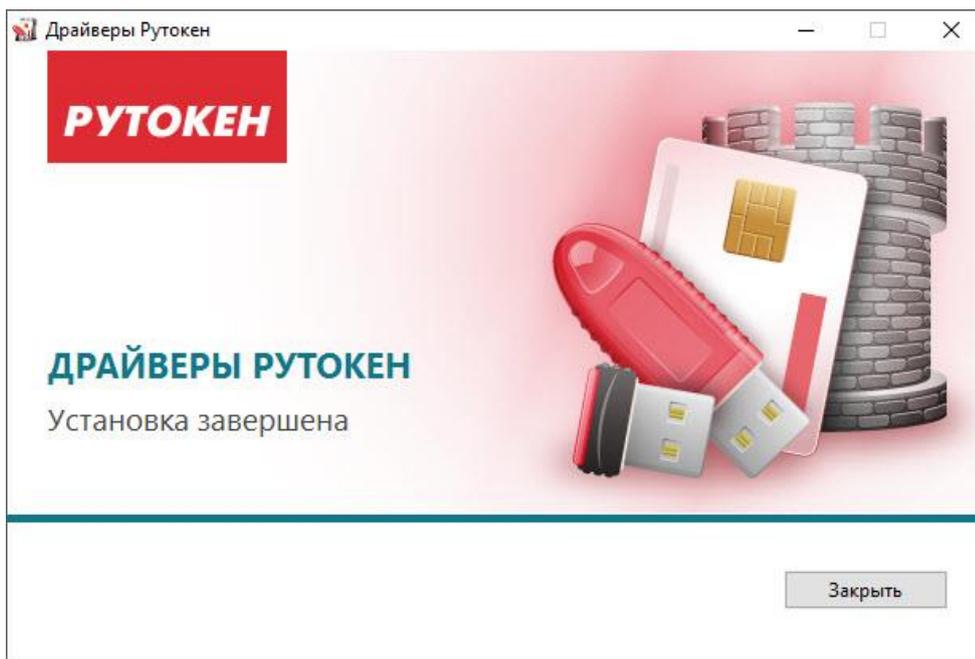
1. Запустите программу установки комплекта драйверов для Windows и нажмите на кнопку **[Установить]**.



2. В окне с запросом на разрешение изменений на компьютере нажмите на кнопку **[Да]**. В результате запустится процесс установки комплекта драйверов.



3. После завершения процесса установки нажмите на кнопку **[Заккрыть]**.

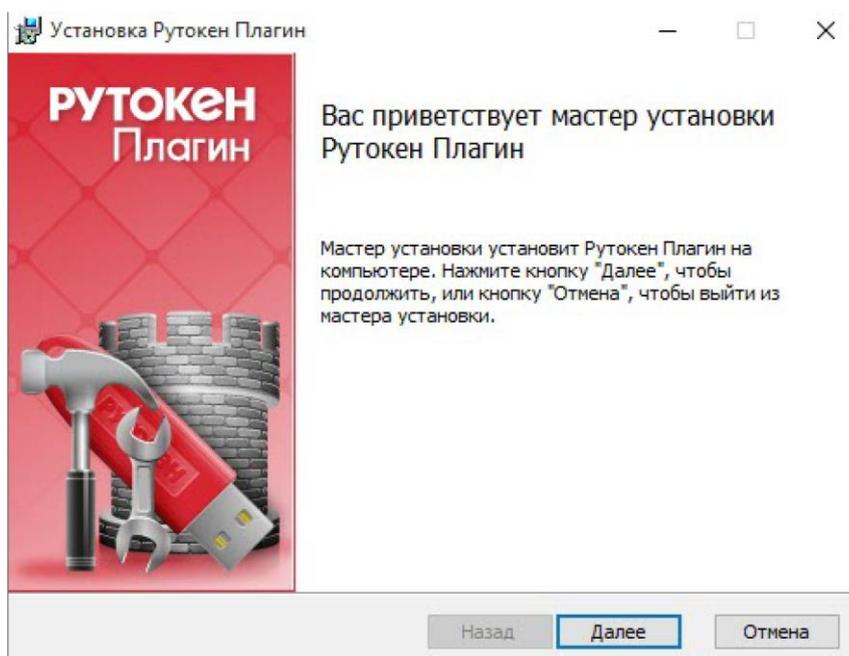


Установка Рутокен Плагин

Актуальная версия плагина доступна по [ссылке](#)

Установщик Рутокен Плагин не может автоматически добавить расширение Адаптер Рутокен Плагин в FireFox 74 и новее. Установите расширение [Адаптер Рутокен Плагин](#) из официального магазина расширений Mozilla.

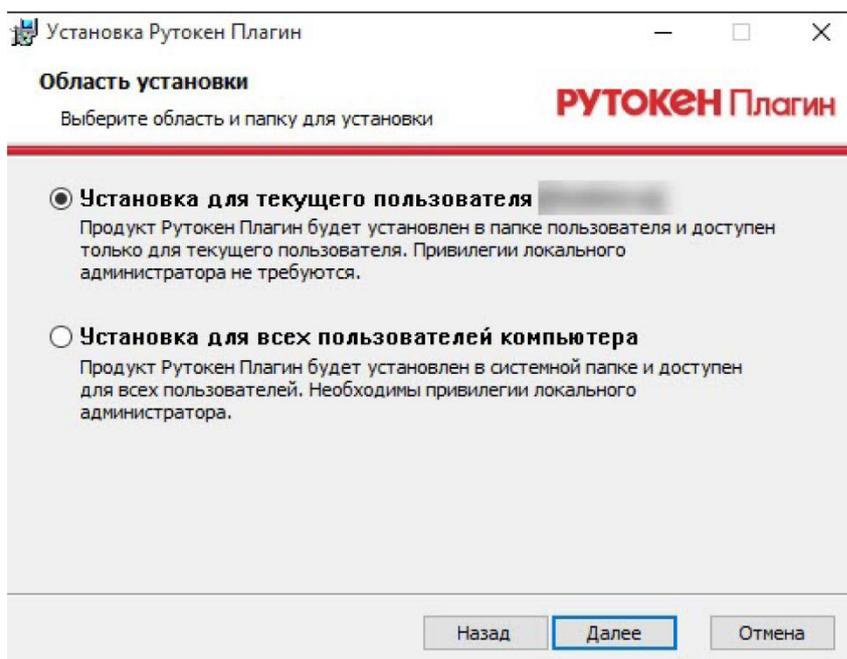
1. Запустите Рутокен Плагин для установки. Откроется окно Установка Рутокен Плагин.



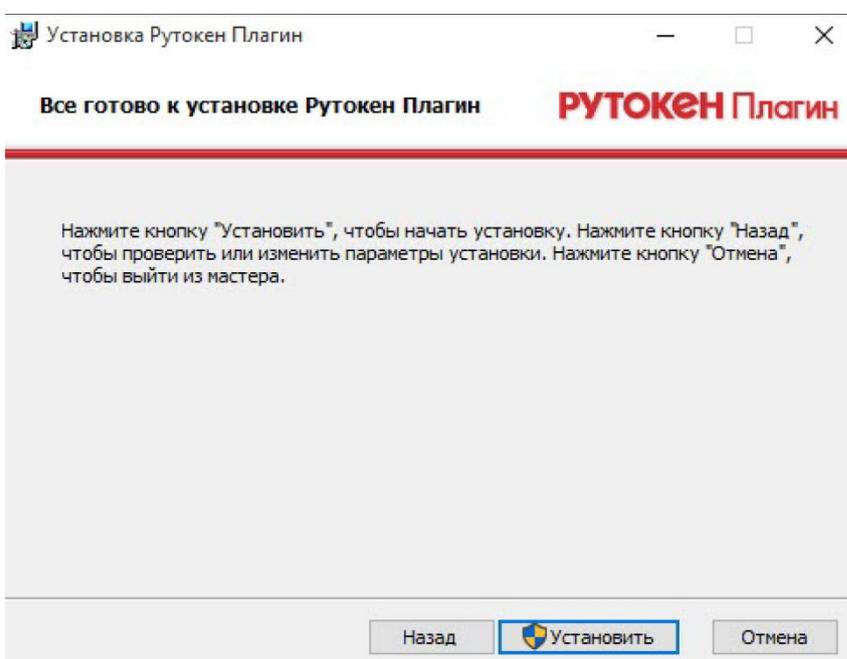
2. На следующем этапе установки выберите область установки Рутокен Плагина:

только текущему пользователю либо всем пользователям компьютера (доступно для пользователей с правами администратора).

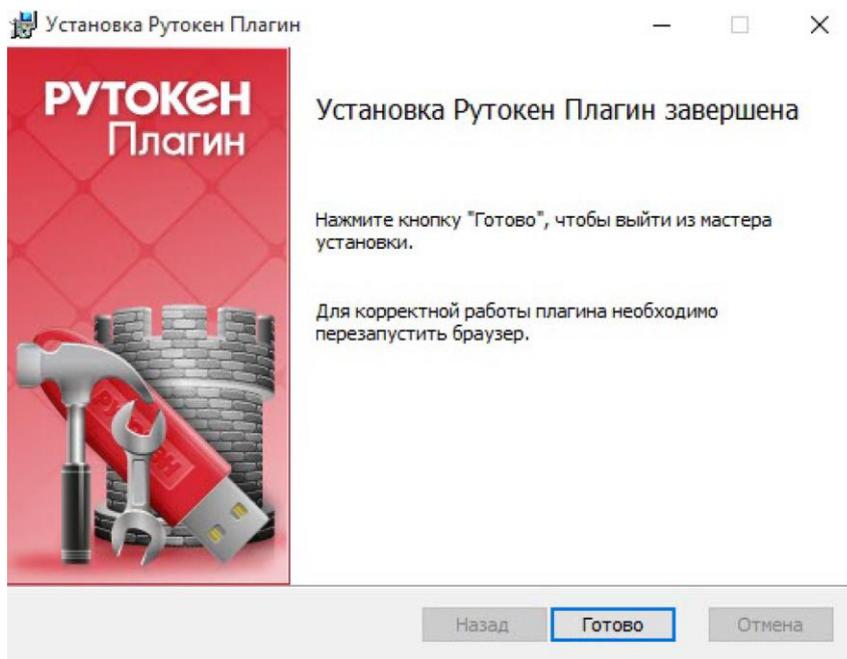
Нажмите на кнопку **[Далее]**.



3. Чтобы запустить процесс установки нажмите на кнопку **[Установить]**.



4. После завершения процесса установки нажмите на кнопку **[Готово]**.



5. Подключите устройство Рутокен к компьютеру.

Настройка рабочего места завершена.

Настройка рабочего места для работы с носителями без встроенного криптопровайдера

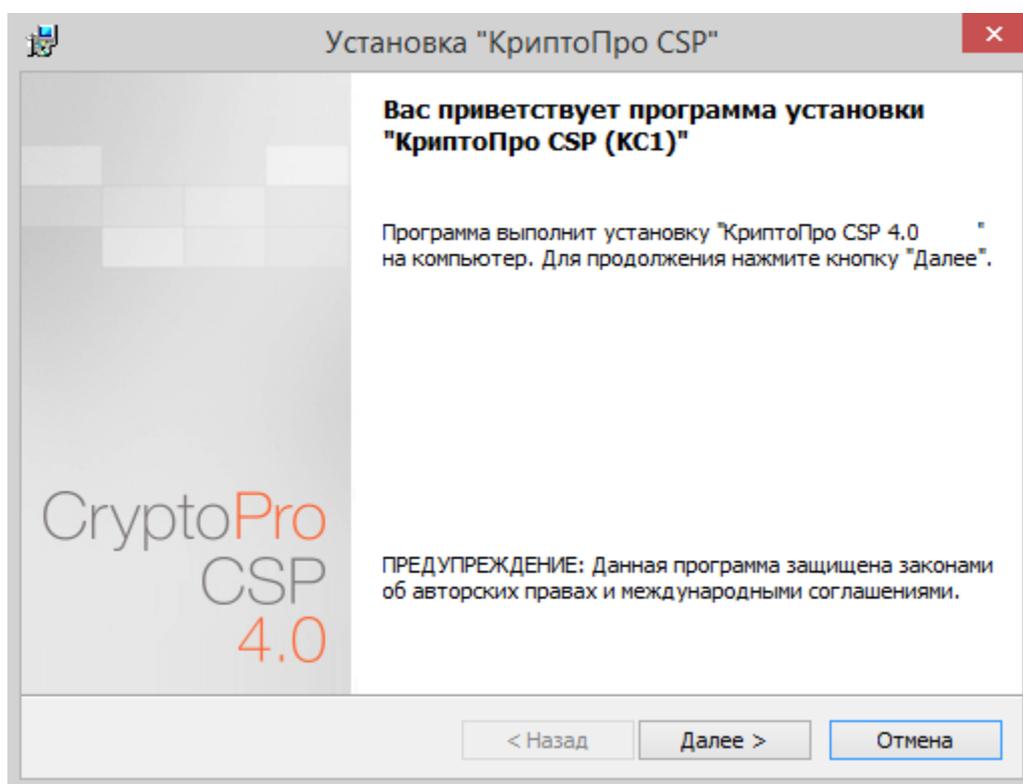
Установка криптопровайдера

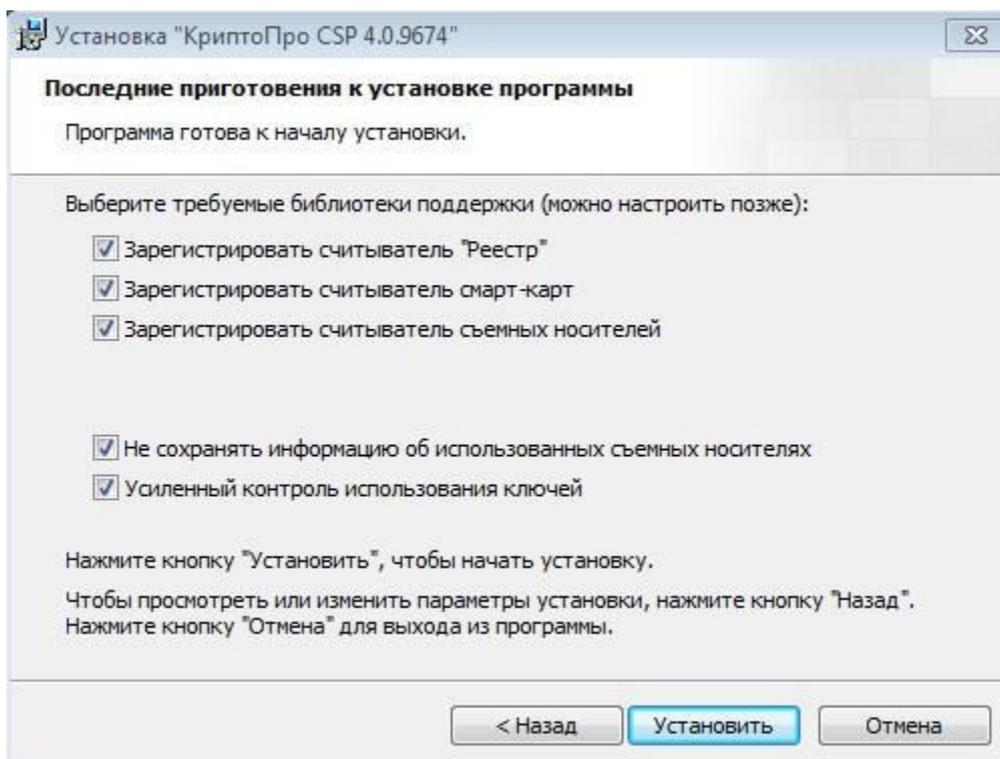
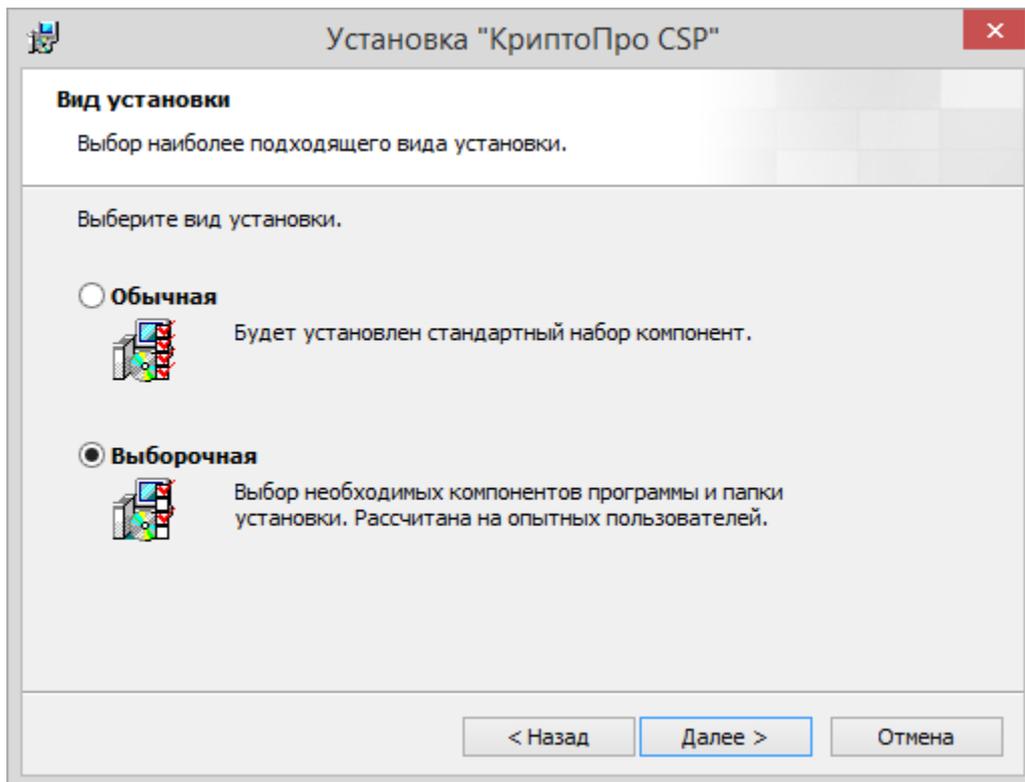
КриптоПро CSP

Пройдите процедуру регистрации и загрузите дистрибутив КриптоПро CSP с официального сайта разработчика по [ссылке](#)

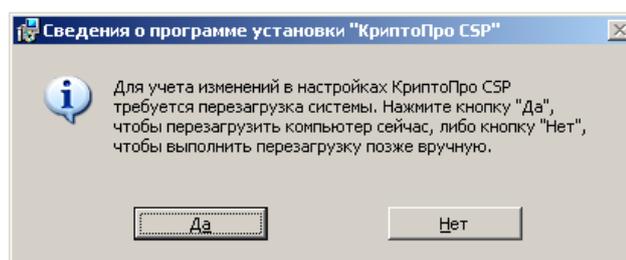
Внимание! Установка дистрибутива СКЗИ КриптоПро CSP должна производиться пользователем, имеющим права администратора.

При установке КриптоПро CSP следуйте инструкциям мастера установки





После завершения установки перезагрузите компьютер.



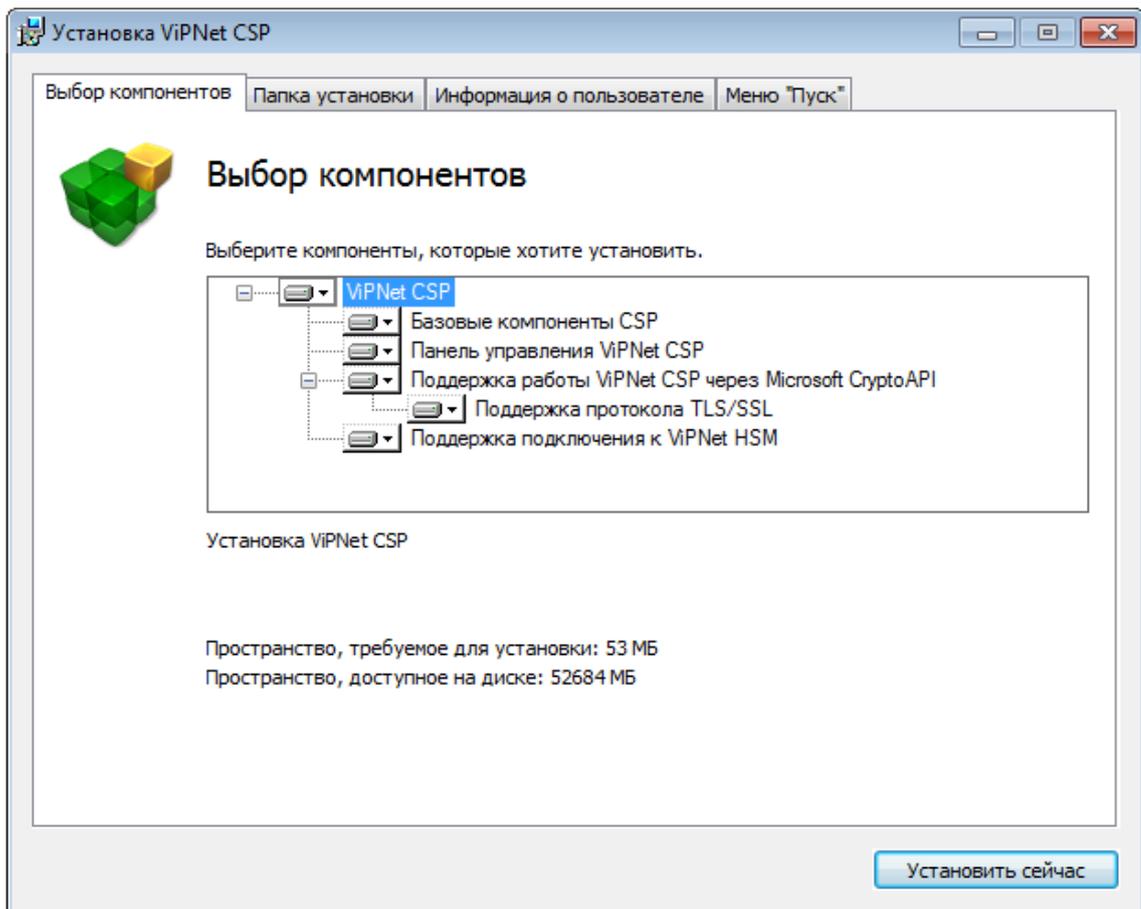
VipNet CSP

Пройдите процедуру регистрации и загрузите дистрибутив VipNet CSP с официального сайта разработчика по [ссылке](#)

Для установки программы ViPNet CSP вы должны обладать правами администратора операционной системы.

Чтобы установить программу ViPNet CSP, выполните следующие действия:

1. Запустите установочный файл.
2. На странице Лицензионное соглашение мастера установки ViPNet CSP ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку Продолжить.
3. Чтобы после завершения установки компьютер перезагрузился автоматически, на странице Способ установки установите флажок Автоматически перезагрузить компьютер после завершения.
4. Если вы хотите настроить параметры установки, на странице Способ установки нажмите кнопку Настроить и укажите следующее:
 - компоненты программы, которые хотите установить;
 - путь к папке установки программы на компьютере;
 - имя пользователя и название организации;
 - название папки программы в меню Пуск. Вы можете выбрать или отключить следующие компоненты для установки:
 - Панель управления ViPNet CSP — если отключить этот компонент, будут установлены лишь библиотеки криптопровайдера без исполняемого файла ViPNet CSP. Такой способ установки может быть использован разработчиками.
 - Поддержка работы ViPNet CSP через Microsoft CryptoAPI — добавляет функции, позволяющие использовать криптопровайдер ViPNet CSP в сторонних приложениях, например в приложениях Microsoft Office. Компонент включен по умолчанию при отдельной установке ViPNet CSP.
 - Поддержка протокола TLS/SSL — добавляет функции, позволяющие организовать защищенное соединение по протоколу TLS. При установке ViPNet CSP на компьютер, работающий под управлением ОС Windows 10, компонент по умолчанию отключен.
 - Поддержка подключения к ViPNet HSM — добавляет функции, позволяющие организовать подключение к серверу ViPNet HSM и работать с ключами, хранящимися на этом сервере.



5. Чтобы начать установку, нажмите кнопку **Установить сейчас**.
6. Если ранее на странице **Способ установки** вы установили флажок **Автоматически перезагрузить компьютер после завершения**, по окончании установки компьютер перезагрузится автоматически. В противном случае по окончании установки программа предложит перезагрузить компьютер. В окне сообщения о перезагрузке нажмите кнопку **Да**.

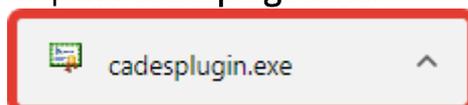
В результате выбранные компоненты будут установлены. В процессе установки также будет создана точка восстановления системных файлов и параметров.

Установка КриптоПро ЭЦП Browser plug-in

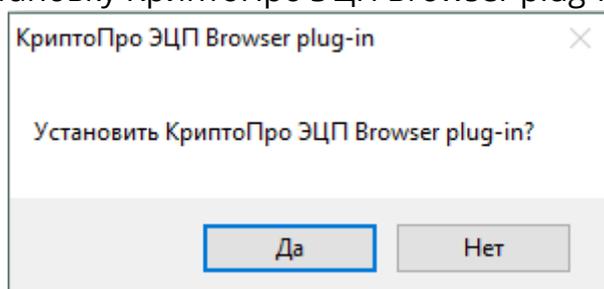
Для корректного функционирования веб-страниц, использующих КриптоПро ЭЦП Browser plug-in, недостаточно расширения для браузера. Сначала необходимо скачать установочный файл и установить его, соблюдая настоящую Инструкцию.

Дистрибутив и инструкцию по установке можно получить по [ссылке](#)

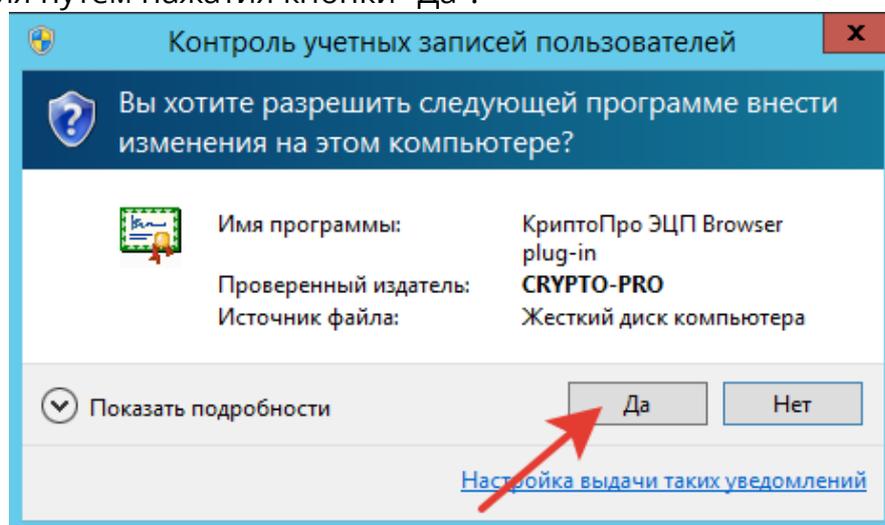
1. Скачайте программу установки. КриптоПро ЭЦП Browser plug-in доступен по [ссылке](#).
2. Запустите исполняемый файл **ca desplugin.exe**.



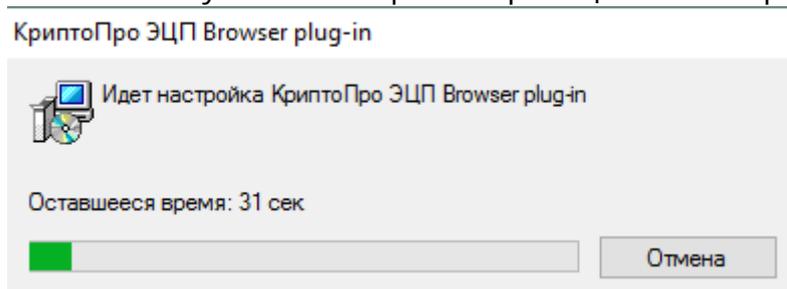
3. Подтвердите установку КриптоПро ЭЦП Browser plug-in.



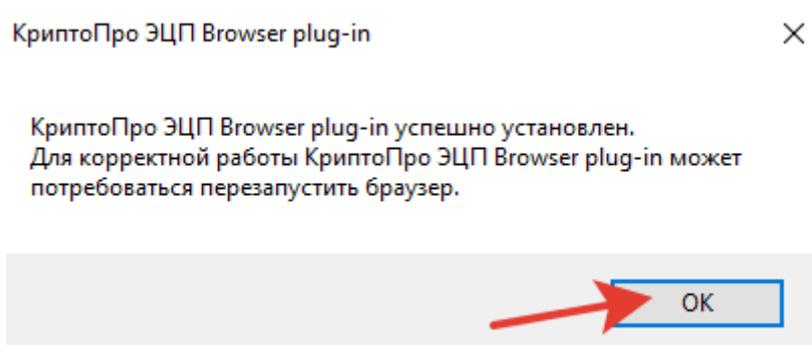
4. Если потребуется, разрешите КриптоПро ЭЦП Browser plug-in внести изменения путем нажатия кнопки "Да".



5. Дождитесь окончания установки КриптоПро ЭЦП Browser plug-in.

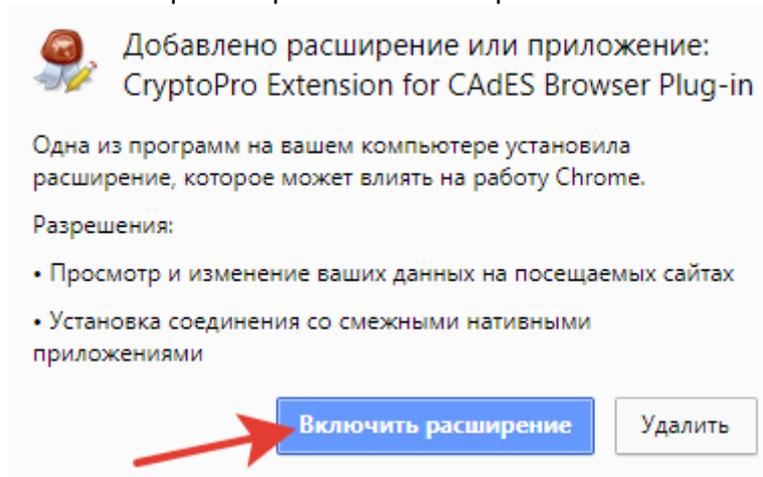


6. После окончания установки КристоПро ЭЦП Browser plug-in нажмите ОК.



7. Дальнейшие настройки различаются в зависимости от используемого браузера.

- **Браузер Chrome:** запустите Chrome и дождитесь оповещения об установленном расширении "CryptoPro Extension for CADES Browser Plug-in". Включите это расширение. Если на Вашем компьютере ранее уже выполнялась установка КристоПро ЭЦП Browser plug-in, а потом он был удален, потребуется отдельно установить расширение. Для этого перейдите по [ссылке](#) и установите расширение из интернет-магазина Chrome.



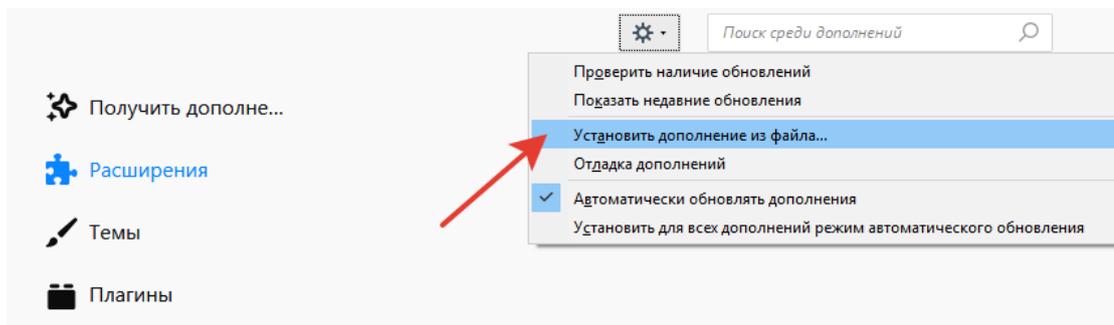
- **Браузер Opera или Яндекс.Браузер:** расширение доступно по [ссылке](#).

Снимок экрана

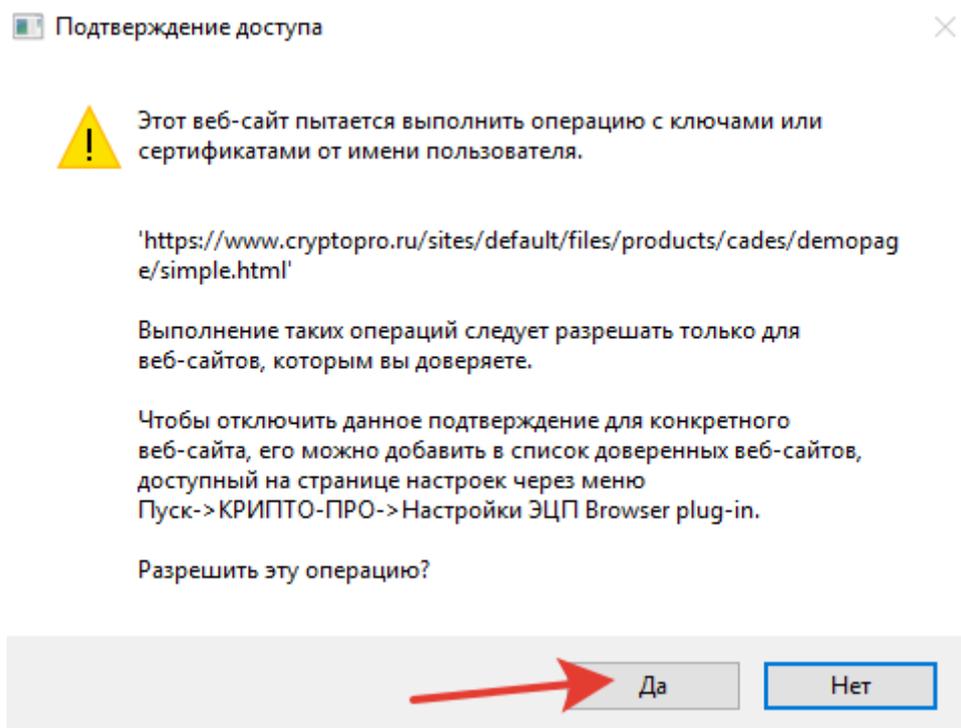
О расширениях

Загрузки: 435 076
Категория: [Инструменты разработчик](#)
Версия: 1.2.5
Размер: 60,2 КБ
Обновлено: 27 ноября 2017 г.
Лицензионное соглашение: Copyright

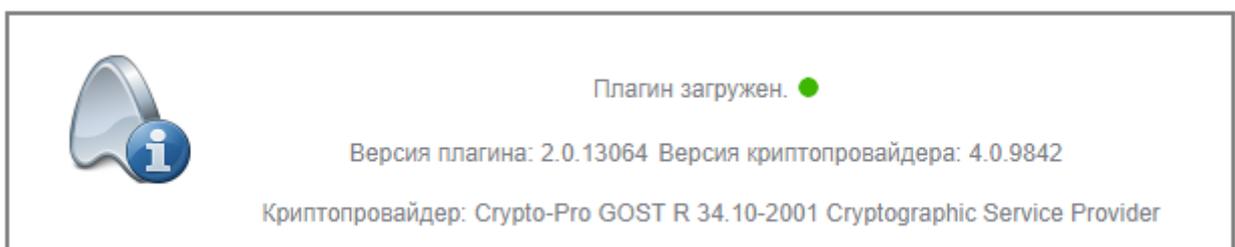
- **Браузер Firefox:** скачайте расширение по [ссылке](#) и установите в браузер самостоятельно.
- **Браузер Microsoft Internet Explorer:** не требуется дополнительных настроек.



8. Проверьте корректность установки на [странице проверки плагина](#). Для этого в открывшемся окне подтвердите доступ путем нажатия кнопки "Да".



Если установка КриптоПро ЭЦП Browser plug-in прошла успешно, появится окно с надписью "Плагин загружен", указанием его версии и используемой Вами версии КриптоПро CSP.

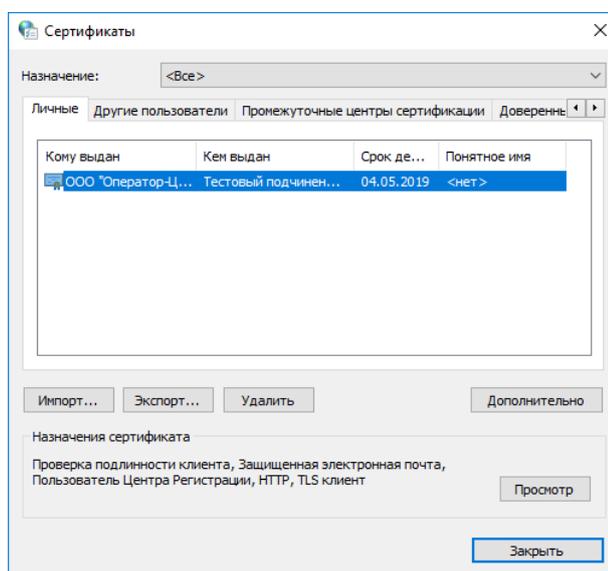


Выстраивание цепочки доверия личному сертификату

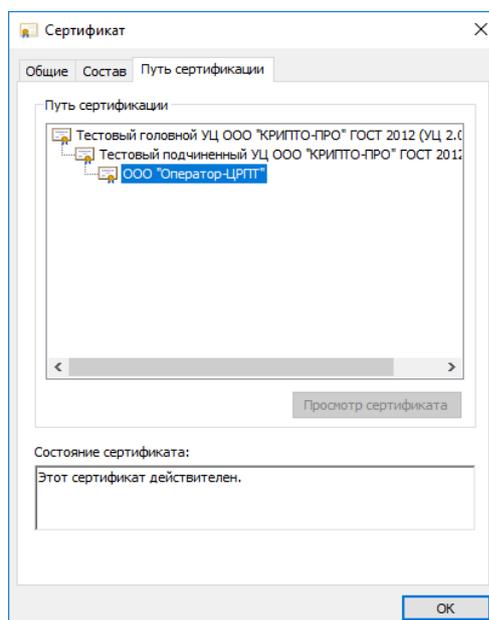
Необходимо установить сертификаты ключей проверки электронной подписи:

- корневой сертификат [Минкомсвязи России](#) - в хранилище сертификатов «Доверенные корневые центры сертификации»;
- сертификат Удостоверяющего Центра, выдавшего ЭП - в хранилище сертификатов «Промежуточные центры сертификации».
- сертификат, выданный юридическому лицу или индивидуальному предпринимателю удостоверяющим центром, аккредитованным в соответствии с требованиями Федерального закона № 63-ФЗ – в хранилище сертификатов «Личные».

В меню «Пуск» выберите Панель управления -> Свойства браузера -> вкладка Содержание -> Сертификаты. Откройте вкладку Личные:



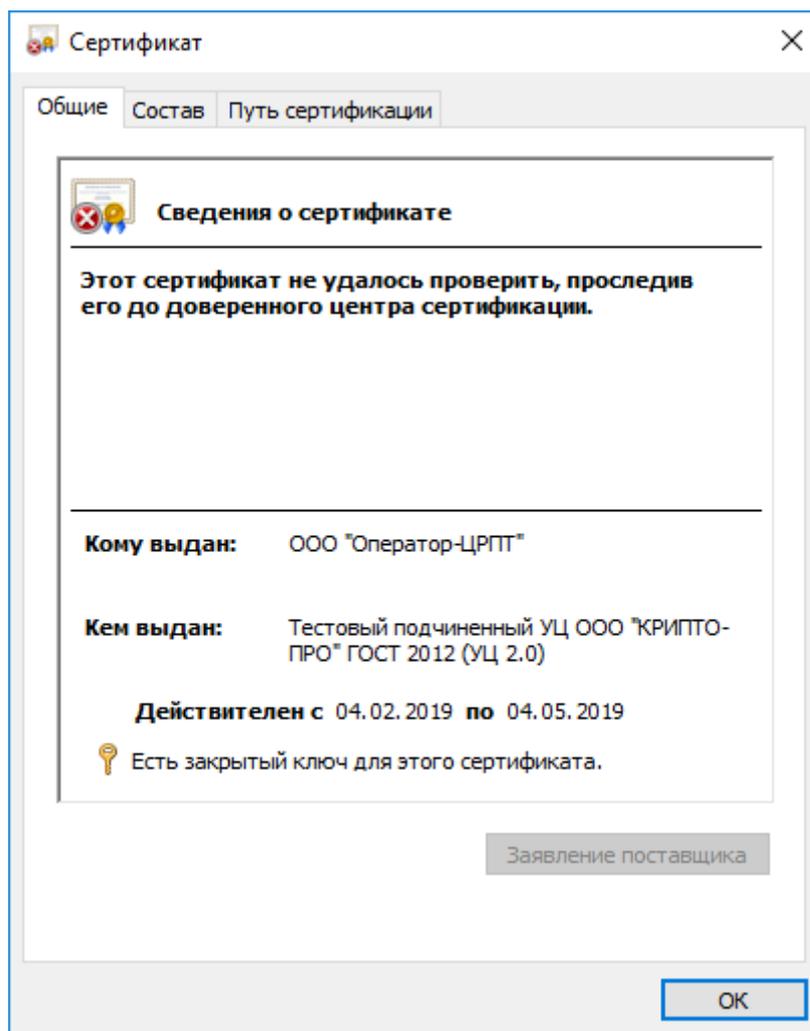
Выберите установленный сертификат, кликнув по нему два раза левой кнопкой мыши. Перейдите на вкладку «Путь сертификации»:



На вкладке «Путь сертификации» должна отображаться цепочка сертификатов, с помощью которых устанавливается доверие.

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

В случае если во вкладке «Общие» Сведения о сертификате отображается «Этот сертификат не удалось проверить, проследив его до доверенного центра сертификации» – необходимо установить корневой сертификат Минкомсвязи и Удостоверяющего Центра, выдавшего вашу электронную подпись.



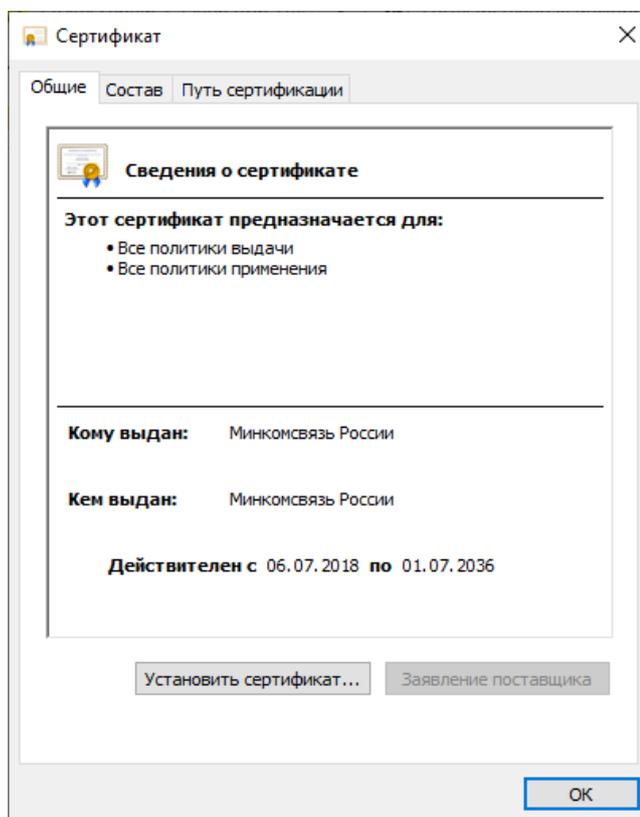
Сертификат Минкомсвязи должен размещаться в хранилище сертификатов «Доверенные корневые центры сертификации»:

Сертификат Удостоверяющего Центра, выдавшего КСКПЭП, будет размещаться в хранилище сертификатов «Промежуточные центры сертификации».

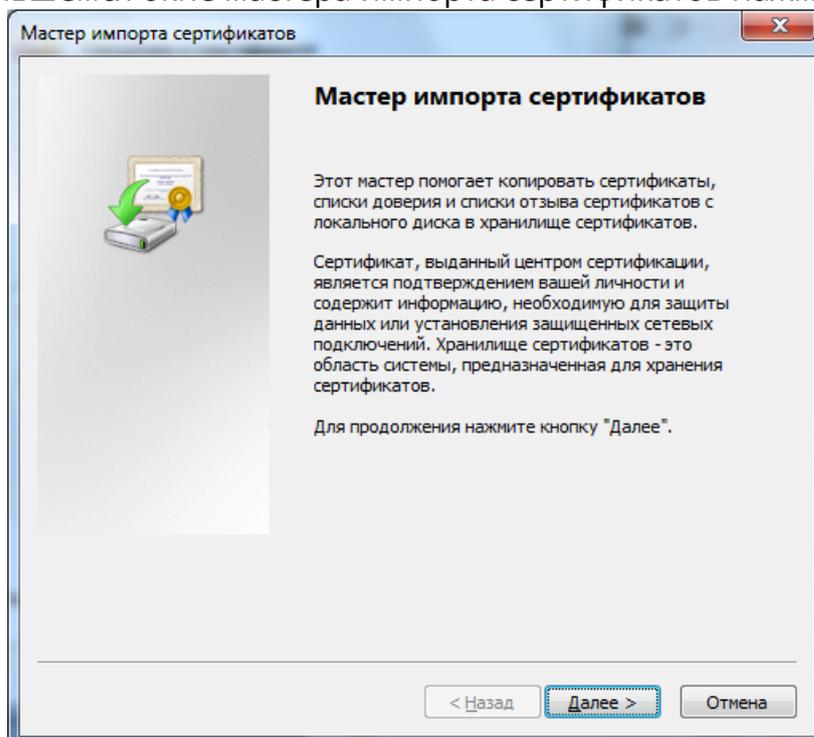
Установка корневого сертификата Минкомсвязи России в хранилище «Доверенные корневые центры»

Для установки сертификата вам потребуется перейти по [ссылке](#) и открыть загруженный сертификат.

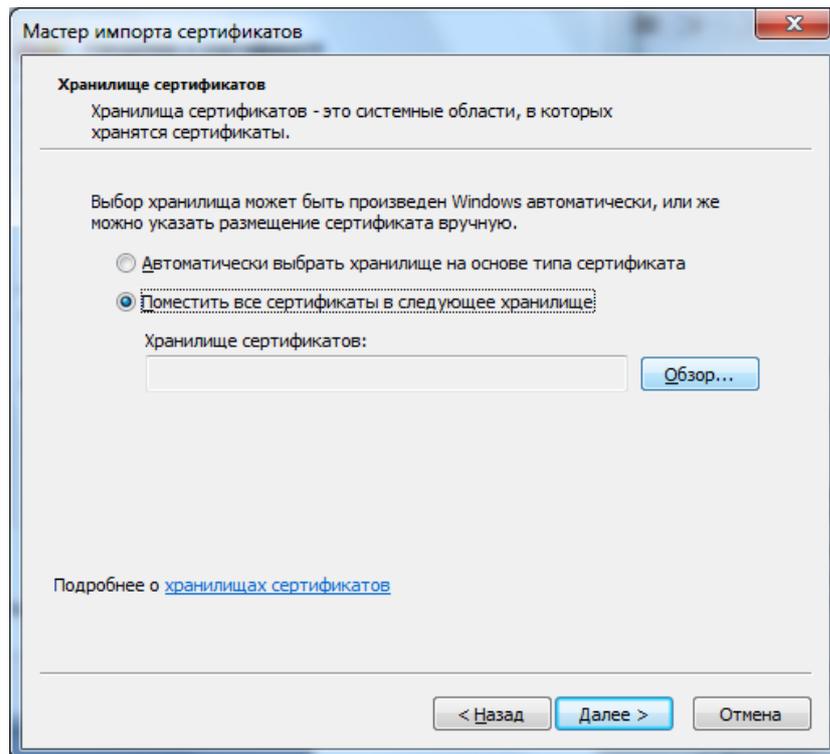
Далее нажмите «Установить сертификат»



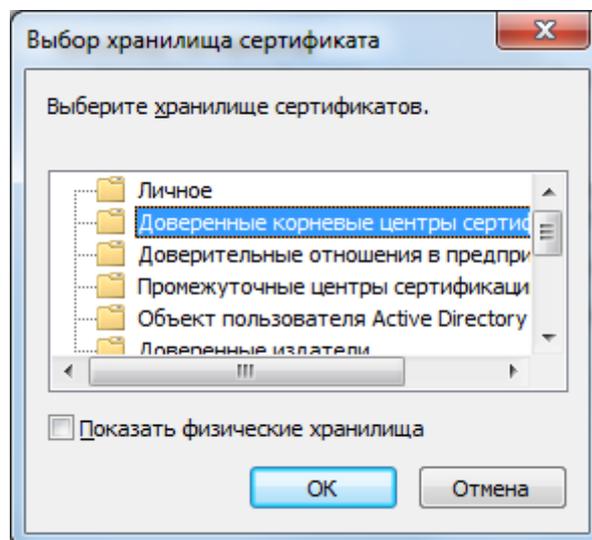
В открывшемся окне мастера импорта сертификатов нажмите «Далее».



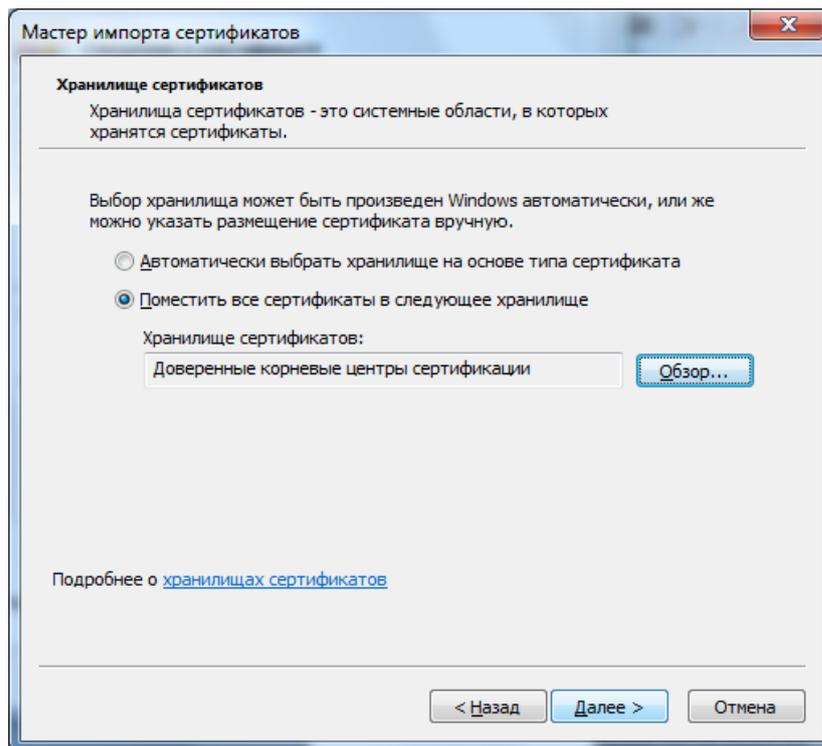
Выберите «Поместить все сертификаты в следующее хранилище», после чего нажмите «Обзор...»



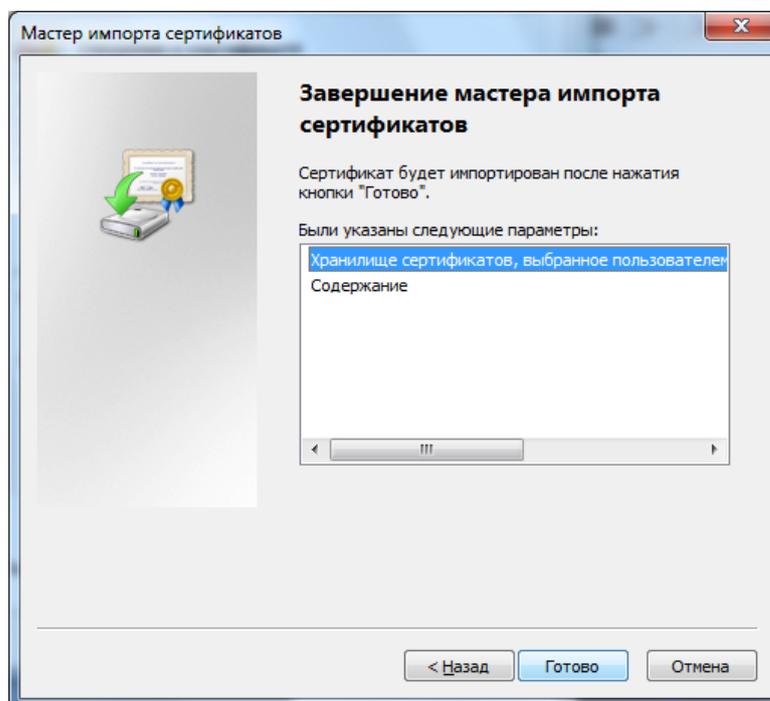
Укажите «Доверенные корневые центры сертификации», нажмите «ОК»



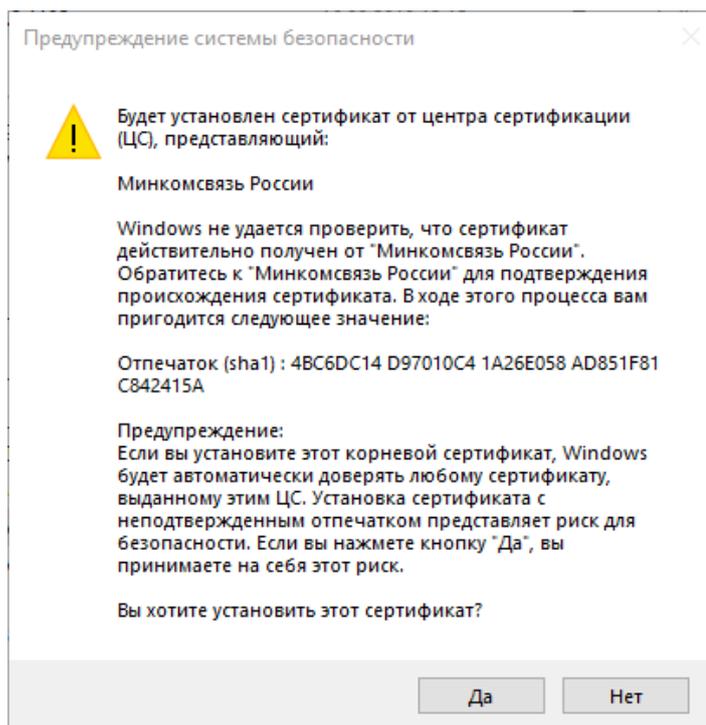
Нажмите «Далее»



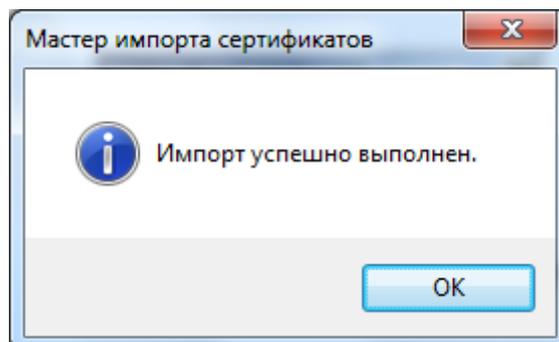
Для завершения работы мастера импорта сертификатов нажмите «Готово»



Подтвердите установку сертификата, нажав кнопку «Да»



Установка сертификата завершена, нажмите «ОК»

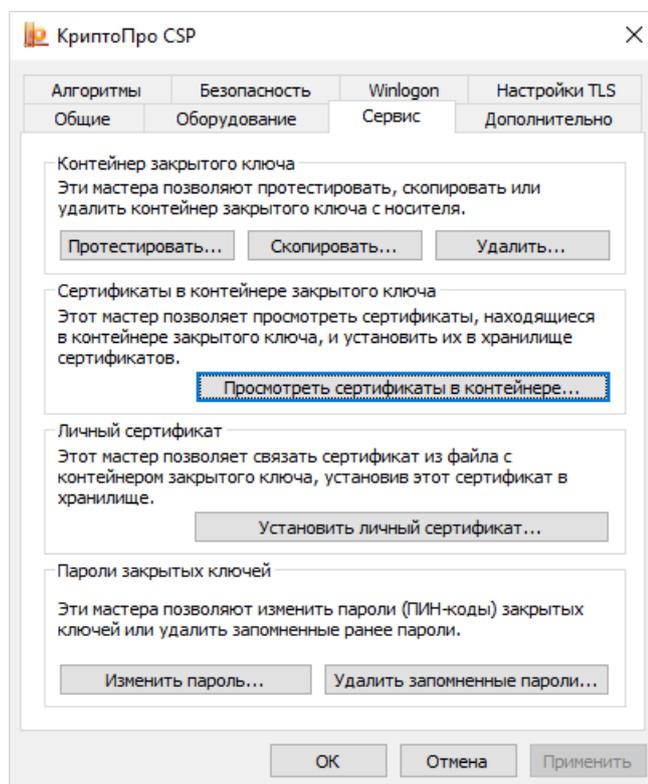


Установка сертификата Удостоверяющего Центра в хранилище «Промежуточные центры сертификации»

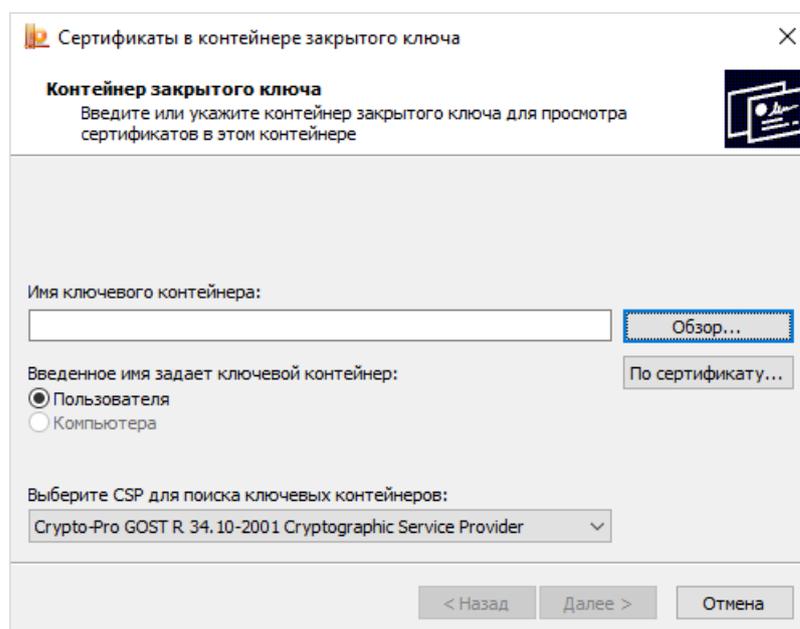
Произведите установку сертификата Удостоверяющего Центра, выдавшего вашу электронную подпись, в **Промежуточные центры сертификации**, аналогично установки корневого сертификата Минкомсвязи России. За сертификатом следует обратиться на сайт УЦ.

Установка сертификата в хранилище Личные Криптопровайдер КриптоПро CSP

Для того чтобы просмотреть сертификат, хранящийся в контейнере закрытого ключа, откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис**

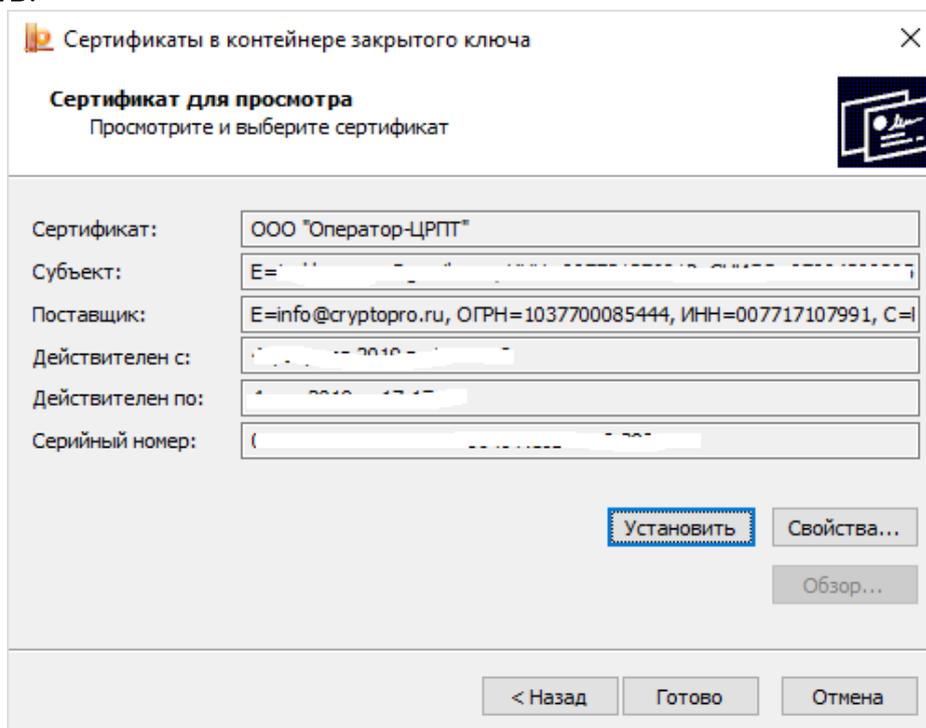


Нажмите кнопку **Просмотреть сертификаты в контейнере**. Откроется окно «Сертификаты в контейнере закрытого ключа»



На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**) или сертификатов (кнопка **По сертификату**). Если сертификат в выбранном контейнере имеется, откроется окно «Сертификат для просмотра»

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



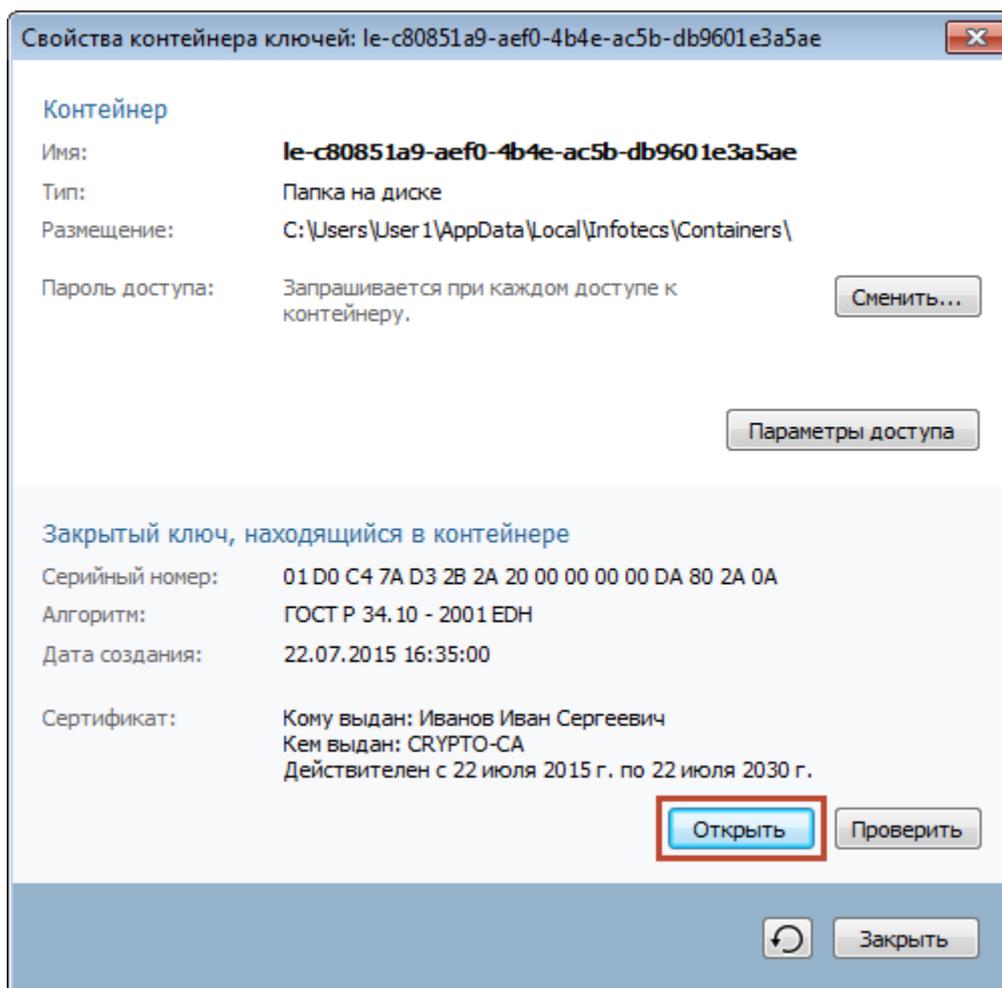
Криптопровайдер VipNet CSP

Чтобы использовать сертификат в различных приложениях, следует установить его в одно из следующих хранилищ сертификатов операционной системы Windows:

- Хранилище текущего пользователя (Current User), раздел **Личное > Сертификаты** — сертификат следует установить в это хранилище в целях шифрования, расшифрования, создания и проверки электронной подписи файлов, а также для доступа к защищенным ресурсам через веб-браузер.
- Хранилище компьютера (Local Machine), раздел **Личное > Сертификаты** — сертификат следует установить в это хранилище при использовании VipNet CSP на веб-сервере для организации доступа к защищенным ресурсам. Также в хранилище компьютера следует устанавливать сертификаты, которые будут использоваться службами данного компьютера.

Для установки сертификата в системное хранилище из контейнера ключей выполните следующие действия:

1. В окне **ViPNet CSP** в разделе **Контейнеры ключей** выберите контейнер ключей, сертификат из которого требуется установить.
2. Нажмите кнопку **Свойства** либо дважды щелкните нужный контейнер ключей.
3. Если вы хотите установить сертификат в хранилище ключей текущего пользователя, выполните следующие действия:
 - В окне **Свойства контейнера ключей** нажмите кнопку **Открыть**.



- В окне **Сертификат** на вкладке **Общие** нажмите кнопку **Установить сертификат**. Будет запущен мастер импорта сертификатов.
- На странице приветствия мастера импорта сертификатов нажмите кнопку **Далее**.
- На странице **Хранилище сертификатов** выберите вариант **Поместить все сертификаты в следующее хранилище** и нажмите кнопку **Обзор**.
- В окне **Выбор хранилища сертификатов** выберите хранилище **Личное**.
- На странице **Завершение мастера импорта сертификатов** нажмите кнопку **Готово**.

Настройка рабочего места завершена.

Техподдержка

Если у вас остались нерешенные вопросы, обратитесь к нам по следующим каналам связи:

support@crpt.ru

+7 800 222-15-23

через обращение на сайте <https://честныйзнак.рф>