



---

Руководство пользователя  
по подготовке рабочего места для использования ЭП, выпущенных  
Новосибирским филиалом АО «ЦентрИнформ»

---

Новосибирск

2021

## Содержание

<a href="#">Введение</a> .....	3
<a href="#">1. Установка КриптоПро CSP</a> .....	4
<a href="#">2. Установка драйвера ключевого носителя</a> .....	8
<a href="#">2.1 Установка драйвера Rutoken</a> .....	9
<a href="#">2.2 Установка драйвера eToken</a> .....	11
<a href="#">2.3 Установка драйвера ESMART</a> .....	15
<a href="#">2.4 Установка драйвера Jacarta</a> .....	19
<a href="#">3. Загрузка и установка корневых сертификатов УЦ</a> .....	23
<a href="#">3.1 Автоматическая установка корневых сертификатов</a> .....	24
<a href="#">3.2 Ручная установка корневых сертификатов</a> .....	25
<a href="#">4. Установка Личного сертификата</a> .....	31
<a href="#">Заключение</a> .....	36

## Введение

Данное руководство содержит последовательное описание по подготовке персональных компьютеров (ПК) с операционными системами (ОС) семейства Windows (2003/XP/Vista/2008/7/8.1/10), которые будут использоваться в качестве рабочих мест для работы с использованием квалифицированных электронных подписей (ЭП).

---

**Примечание:** Подготовка ПК с ОС Windows более ранних версий (98/Me/NT/2000/2000Server) и UNIX-подобными ОС (Solaris/Linux FreeBSD и др.) в данной инструкции не рассматриваются и в качестве рабочих мест не рекомендуются.

---

Подготовка ПК для работы с ЭЦП выполняется в следующем порядке:

1. Установить КриптоПро CSP
2. Установить драйвер ключевого носителя
3. Установить корневые сертификаты УЦ
4. Установить Личный сертификат

### ВНИМАНИЕ!

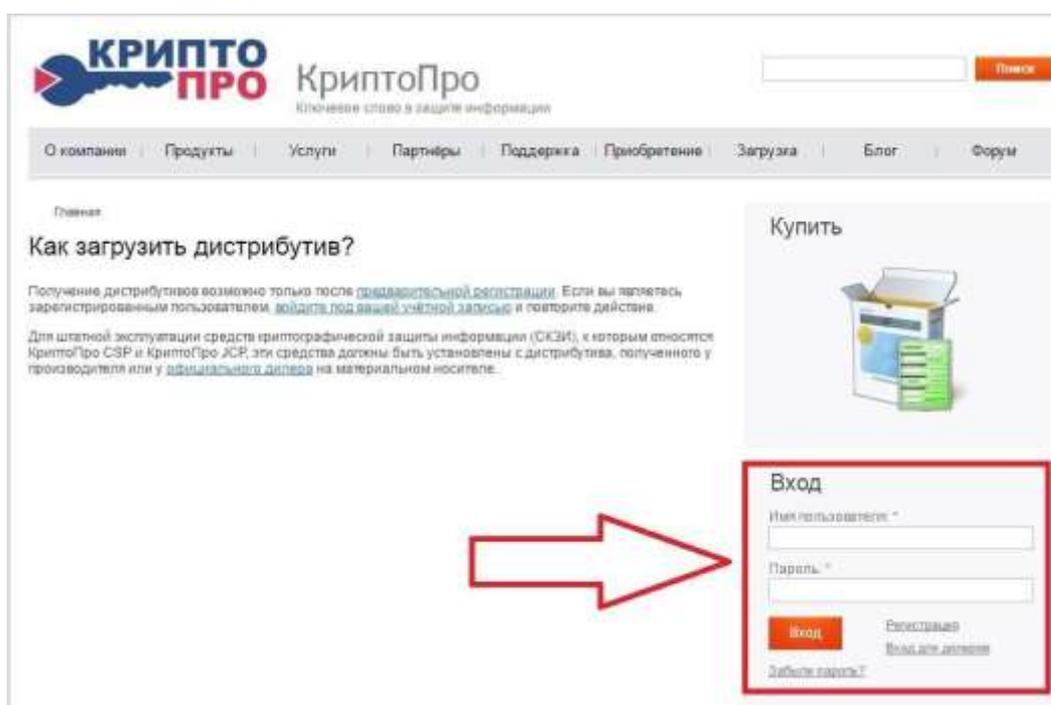
**ДО НАЧАЛА РАБОТ ПО ПОДГОТОВКЕ ВАШЕГО КОМПЬЮТЕРА ДЛЯ ИСПОЛЬЗОВАНИЯ ЭЦП УБЕДИТЕСЬ В ОТСУТСТВИИ ВИРУСОВ НА НЁМ И ОБЕСПЕЧЬТЕ НАДЕЖНУЮ АНТИВИРУСНУЮ ЗАЩИТУ ВАШЕГО ПК, ИНАЧЕ КОРРЕКТНАЯ РАБОТА С ЭЦП НЕ ГАРАНТИРУЕТСЯ.**

## 1. Установка КриптоПро CSP

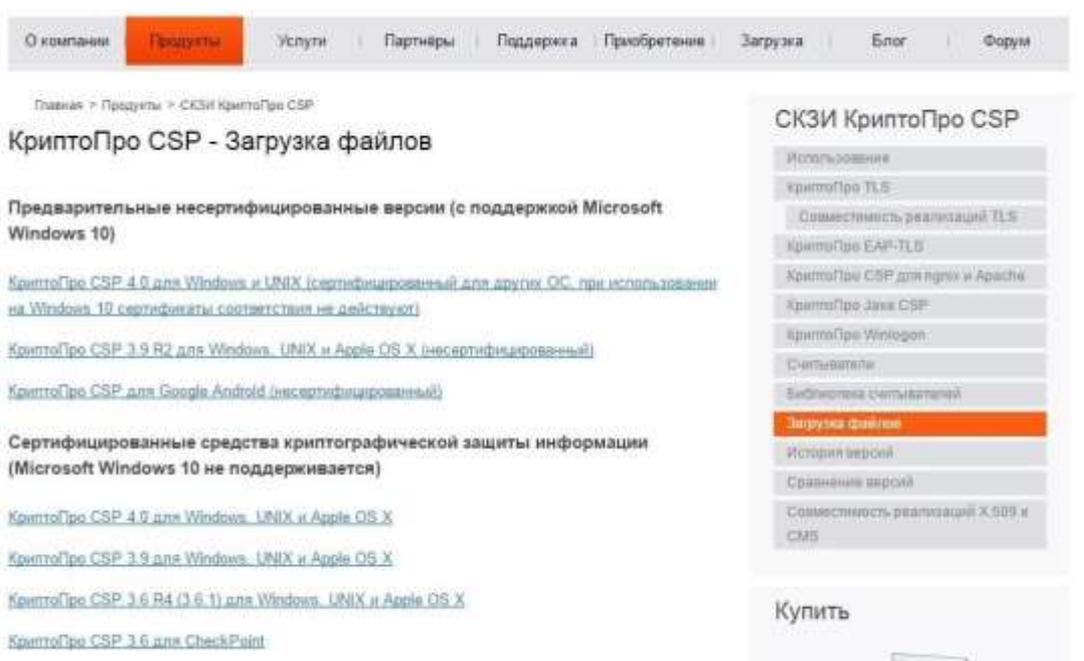
КриптоПро CSP — криптопровайдер (Cryptography Service Provider, CSP) — средство криптографической защиты информации (СКЗИ), представляющее собой независимый модуль, позволяющий осуществлять различные криптографические операции в ОС Windows и выполняющий взаимодействие с различными приложениями, работающими в этой среде.

Криптопровайдер КриптоПро CSP разработан компанией «КриптоПро» (<http://www.cryptopro.ru>) и используется для работы с ключами шифрования и ЭЦП, обеспечения целостности и подлинности информации, не содержащей сведений составляющих государственную тайну. КриптоПро CSP имеет [сертификаты соответствия](#) ФСБ России.

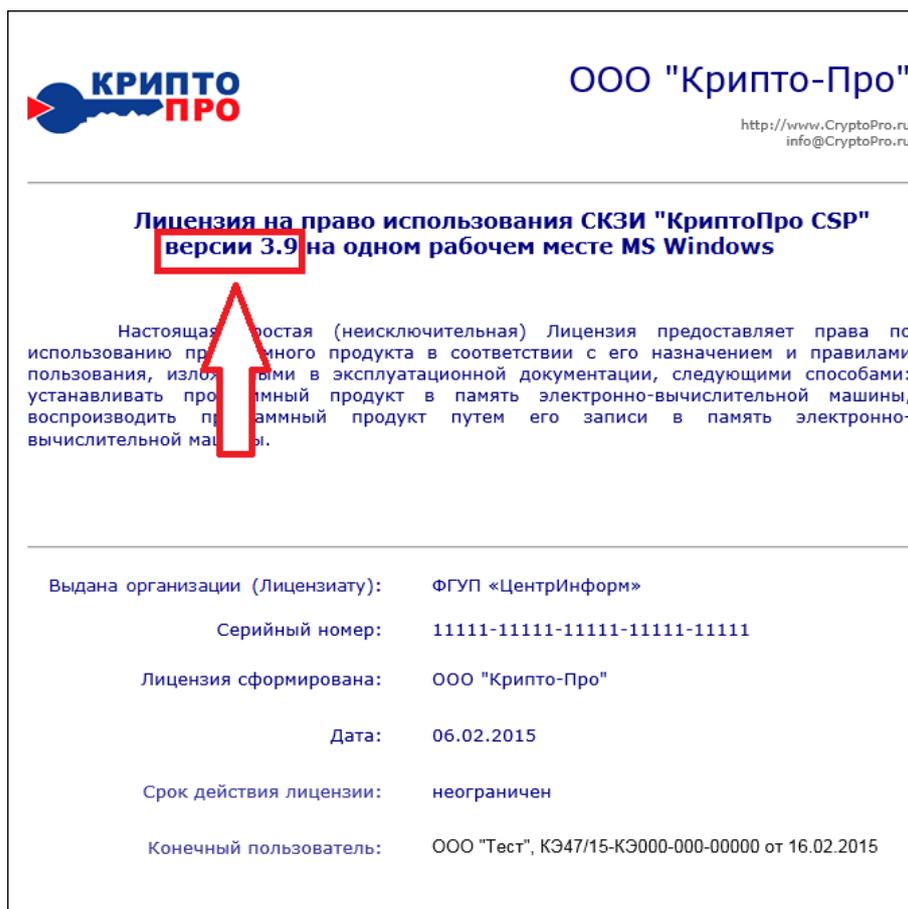
Дистрибутив КриптоПро CSP необходимо скачать с официального сайта «КриптоПро» <https://www.cryptopro.ru/products/csp/downloads>.



Чтобы дистрибутивы стали доступны для скачивания, нужно пройти регистрацию и авторизоваться по логину/паролю.



Скачать и установить нужно ту версию КриптоПРО CSP на которую была куплена лицензия. Версия лицензии указана в шапке бланка.



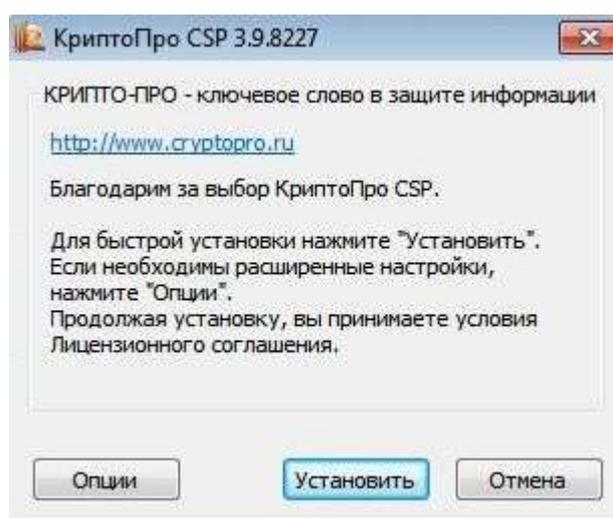
Ниже приведена последовательность установки КриптоПро CSP.

---

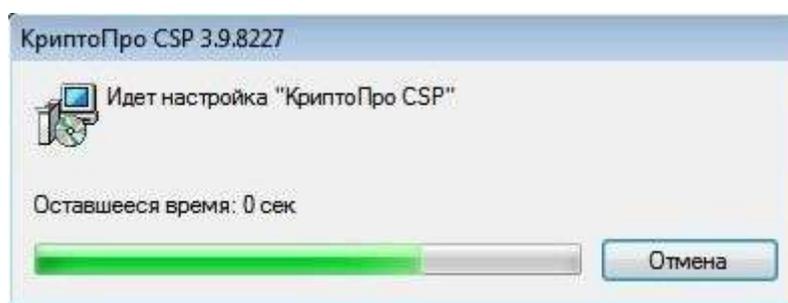
**ВНИМАНИЕ!** Установка КриптоПро CSP должна выполняться только с учетной записи пользователя имеющего права Администратора системы. До завершения установки не подключайте носитель электронных криптографических ключей с вашей ЭП к USB-порту компьютера.

---

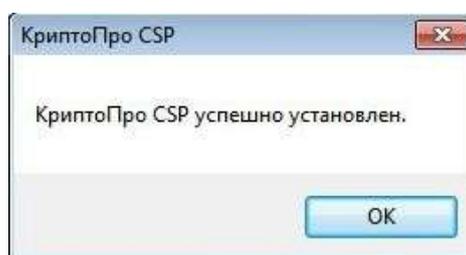
1.1) Запустите установочный пакет КриптоПро CSP. В открывшемся окне нажимаете кнопку «**Установить**»



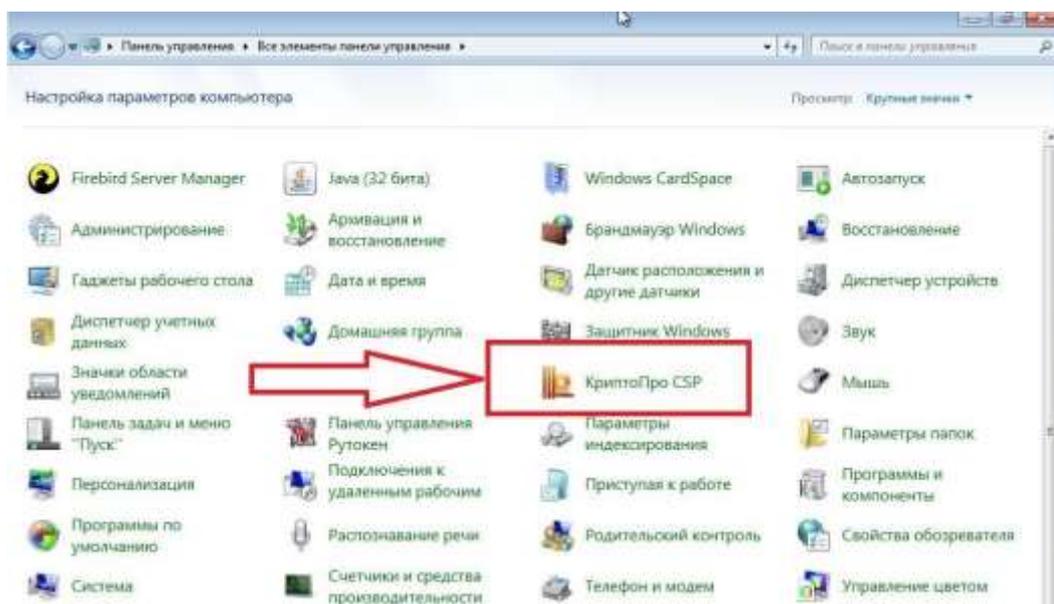
1.2) Дождитесь окончания процесса установки



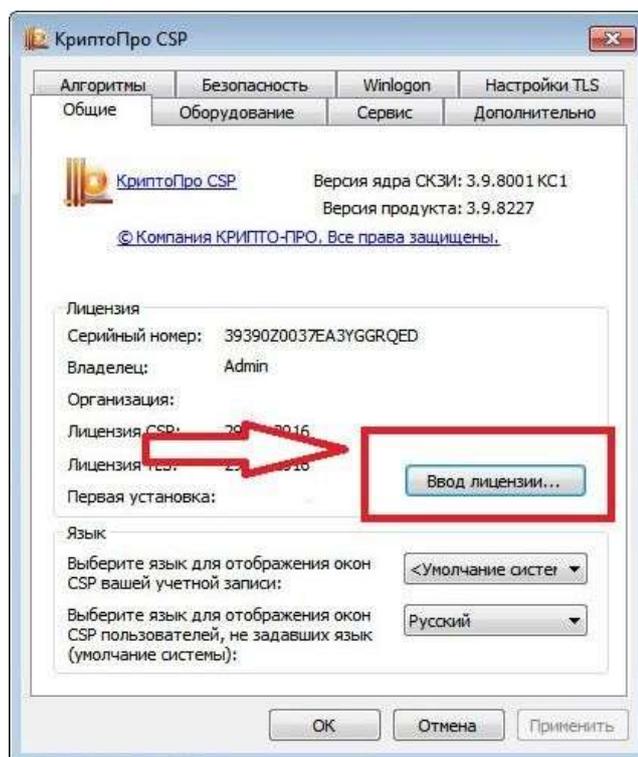
1.3) По окончании установки выйдет окно «КриптоПро CSP успешно установлен». Нажимаете «**Ок**»



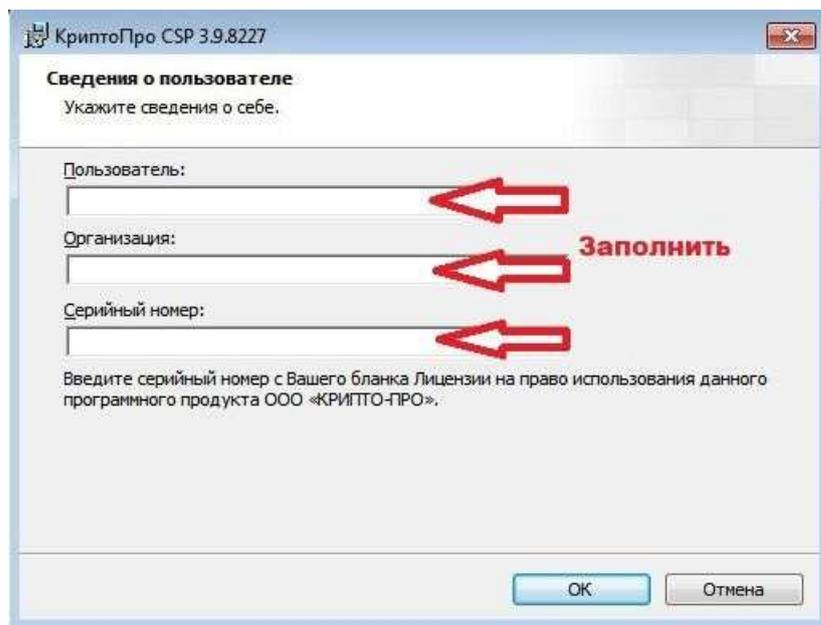
1.4) Зайдите в «**Панель управления**» Windows, откройте **КриптоПро CSP**



1.5) Нажмите кнопку «Ввод лицензии...»



1.6) В следующем окне необходимо указать сведения о пользователе, организации, а также ввести серийный номер с бланка



---

**Примечание:** Обязательным для заполнения является только поле «Серийный номер», в котором должны быть введен точный серийный номер вашей копии продукта, содержащий только цифры и заглавные буквы латинского алфавита. Кроме того, помните, что Лицензия выдается только на одну копию программы КриптоПро CSP строго в соответствии с её версией (серийные номера различных версий КриптоПро не совместимы). Если вы собираетесь работать с ЭЦП на нескольких ПК, то вам необходимо приобрести столько Лицензий на СКЗИ КриптоПро CSP, сколько ПК вы будете использовать для работы с ЭЦП.

---

## 2. Установка драйвера ключевого носителя

ЭП хранится на ключевом носителе Rutoken, Etoken, ESMART, Jacarta.



На ПК необходимо установить драйвер ключевого носителя.

Для ключевого носителя Rutoken драйвера скачиваются с сайта производителя <http://www.rutoken.ru/support/download/drivers-for-windows/>

Для ключевого носителя eToken драйвера скачиваются с сайта <http://nalog.ci54.ru/support/downloads>

Для ключевого носителя ESMART драйвера скачиваются с сайта производителя <https://esmart.ru/download/>

Для ключевого носителя Jacarta драйвера скачиваются с сайта производителя [https://www.aladdin-rd.ru/support/downloads/jacarta\\_client](https://www.aladdin-rd.ru/support/downloads/jacarta_client)

---

**ВНИМАНИЕ!** Установка драйвера ключевого носителя должна выполняться только с учетной записи пользователя имеющего права Администратора системы. До завершения установки не подключайте носитель электронных криптографических ключей с вашей ЭП к USB-порту компьютера.

---

Процесс установки для каждого из носителей представлен ниже.

## **2.1 Установка драйвера Rutoken**

---

**Примечание:** для ключевого носителя eToken установка драйвера показана в пункте 2.2.

Для ключевого носителя ESMART установка драйвера показана в пункте 2.3.

Для ключевого носителя Jacarta установка драйвера показана в пункте 2.4

---

2.1.1) На странице <http://www.rutoken.ru/support/download/drivers-for-windows/> нажмите на ссылку «Драйверы Рутокен для Windows (x86 и x64)»

**РУТОКЕН**

О компании / Контакты / Партнеры / Центр-сервис / Фирмы / Новости

Продукты ▾ Решения ▾ Технологии ▾ Поддержка ▾ Заказ ▾ Центр загрузки ▾ Разработка

Главная > Поддержка > Центр загрузки > Драйверы для Windows

## ДРАЙВЕРЫ ДЛЯ WINDOWS

**ВОПРОС-ОТВЕТ**

**ЦЕНТР ЗАГРУЗКИ**

- Драйверы для Windows
- Драйверы для ЕГАИС
- Рутокен для КриптоПро
- Рутокен для Signat.COM
- Рутокен Плагин
- Библиотека PKCS#11
- Драйверы для \*nix
- Драйверы для Mac
- ПО для Рутокен Web
- ПО для Рутокен PINPad

**Пользователям Рутокен**

Для того чтобы установить драйверы Рутокен для Windows, загрузите установочный файл, запустите его и следуйте указаниям установщика. После завершения процесса установки подключите Рутокен к компьютеру.

**Драйверы Рутокен для Windows (x86 и x64)**

Версия: v.4.0.5.0 от 30.12.2015, 99K3-certified

Объемы/форматы ОС: 32- и 64-разрядные MS Windows 10/8.1/2012R2/8/2012/7/XP/XP2/Vista/XP/XP/2003

**Системным администраторам**

**Утилиты**

**ИНСТРУКЦИИ**

- Настройка и эксплуатация Рутокен
- Установка драйверов при помощи групповых политик
- Справка от ITСет.к работе с Панелью управления Рутокен

**ДРАЙВЕРЫ ДЛЯ ЕГАИС**

Специально для стабильных версий

2.1.2) Поставьте флаг, что Вы принимаете условия лицензионного соглашения и нажмите кнопку «Условия приняты». После этого начнется загрузка установочного файла

**ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ**

**ВОПРОС-ОТВЕТ**

**ЦЕНТР ЗАГРУЗКИ**

- Драйверы для Windows
- Драйверы для ЕГАИС
- Рутокен для КриптоПро
- Рутокен для Signat.COM
- Рутокен Плагин
- Библиотека PKCS#11
- Драйверы для \*nix
- Драйверы для Mac
- ПО для Рутокен Web
- ПО для Рутокен PINPad

Перед использованием программного продукта и/или онлайн-сервисов Рутокен (Rutoken), ознакомьтесь с условиями Лицензионного соглашения. Любое использование программного продукта и/или онлайн-сервисов Рутокен (Rutoken) означает согласие и безоговорочное принятие его условий.

[Загрузить Лицензионное соглашение в виде отдельного PDF-документа](#)

### Лицензионное соглашение на использование программных продуктов и/или онлайн-сервисов Рутокен (Rutoken)

Редакция №1 от 31.08.2012 г.

Настоящий документ представляет собой предложение Закрытого акционерного общества «АктивСофт» (далее – «Правообладатель») заключить соглашение на условиях, указанных ниже.

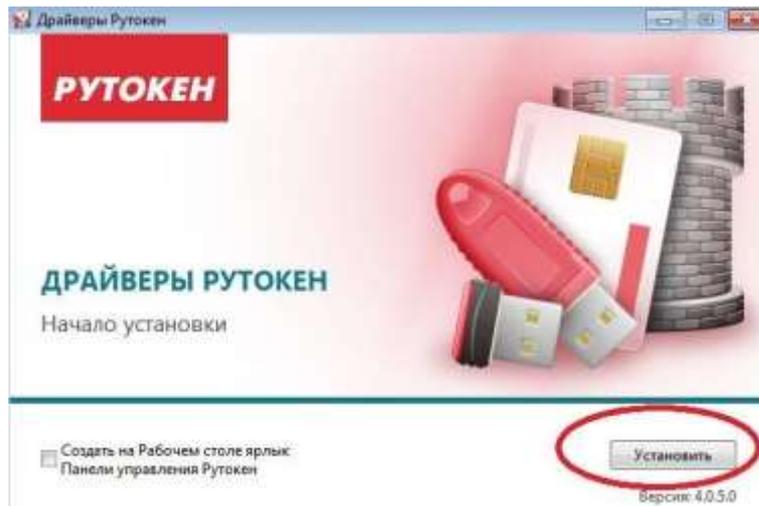
Прежде чем начать работу с программным продуктом и/или использовать его содержание, и/или прежде чем загрузить или устанавливать программный продукт и/или онлайн-сервис Рутокен (Rutoken), пожалуйста, внимательно прочтите данное лицензионное соглашение.

Все уведомления по использованию программных продуктов и/или онлайн-сервисов Рутокен (Rutoken)

Условия Лицензионного соглашения прочитаны и приняты в полном объеме.

**УСЛОВИЯ ПРИНЯТЫ**

2.1.3) Запустите установочный файл. Нажмите кнопку «Установить»



2.1.4) Дождитесь окончания установки и нажмите на кнопку «Закреть»

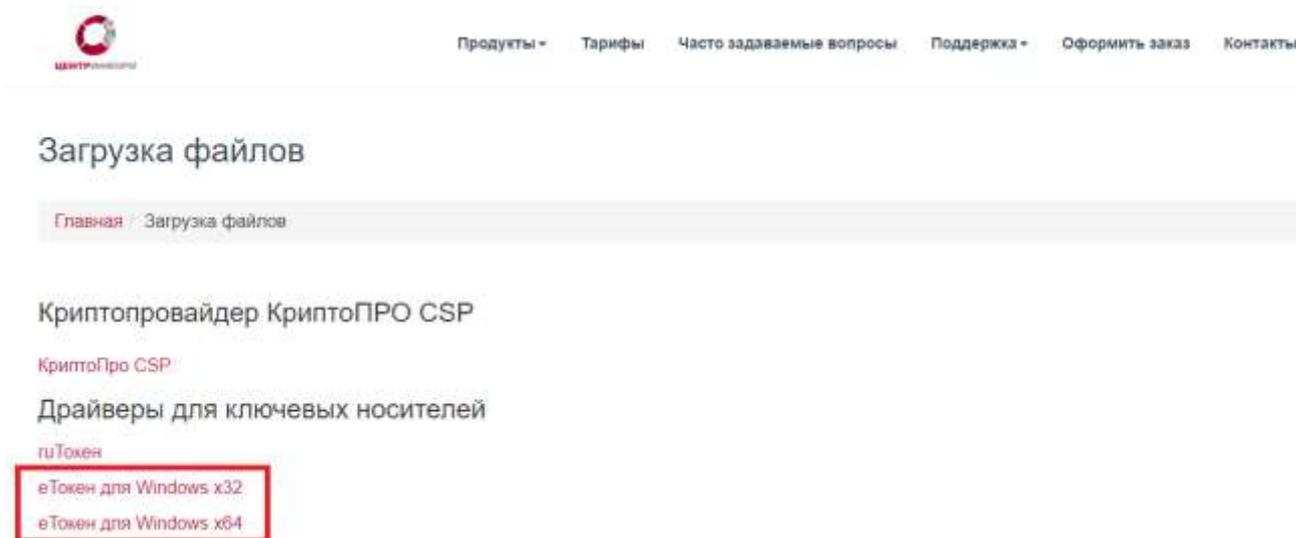


2.1.5) Вставьте в USB порт Rutoken.Windows должен определить его как новое устройство.

2.1.6) Перейдите к разделу 3 данной инструкции

## 2.2 Установка драйвера eToken

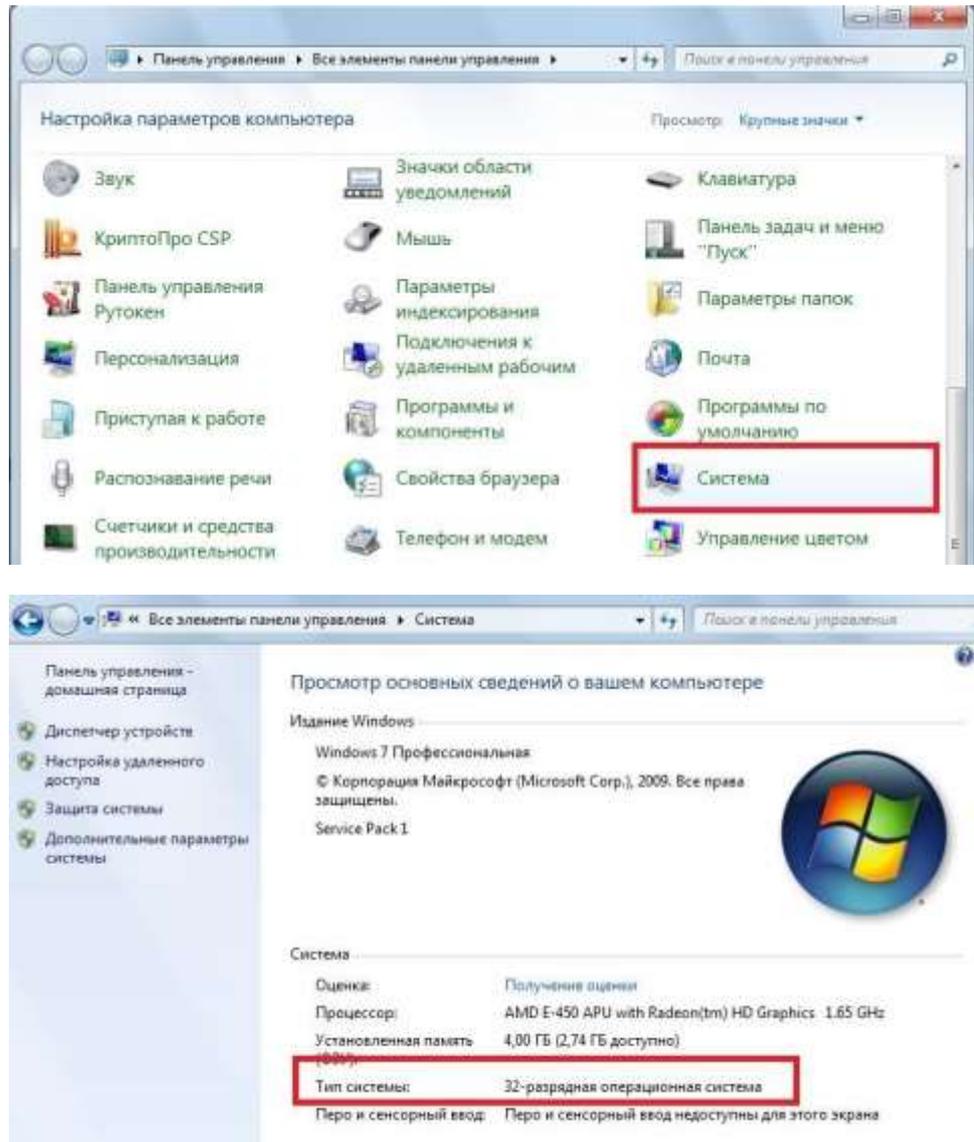
2.2.1) Зайдите на страницу <http://nalog.ci54.ru/support/downloads>. Скачайте и запустите установочный файл в зависимости от разрядности операционной системы



2.2.2) Запустите

- [PKIClient\\_x32\\_5.1\\_SP1.msi](#), есть у Вас Windows разрядности x32
- [PKIClient\\_x64\\_5.1\\_SP1.msi](#), есть у Вас Windows разрядности x64.

**Примечание:** Разрядность Windows можно определить, если зайти в «Панель управления» Windows в меню «Система»



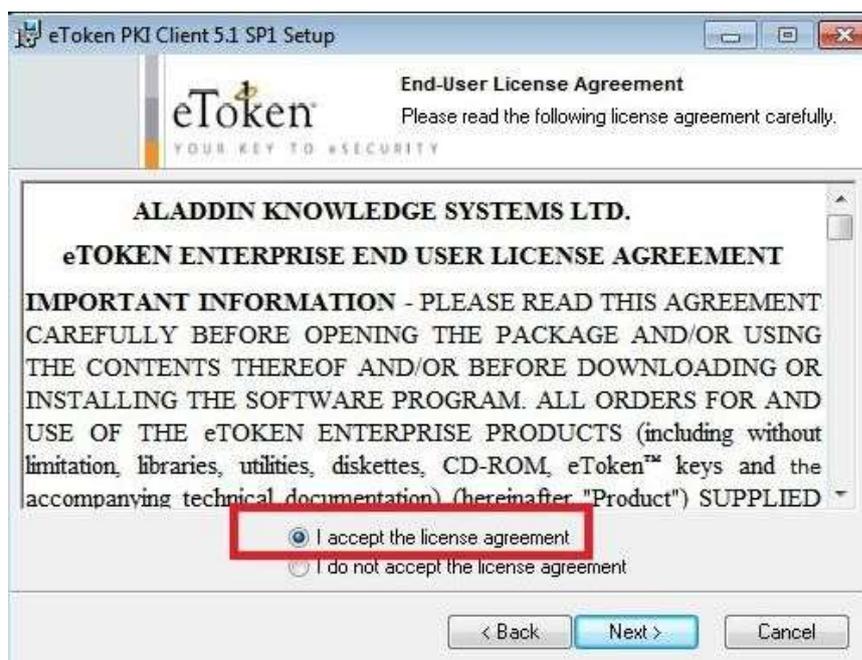
2.2.1) В открывшемся окне приветствия мастера установки нажмите кнопку «Next»:



2.2.2) В следующем окне выберите язык «Russia» и нажмите «Next»:



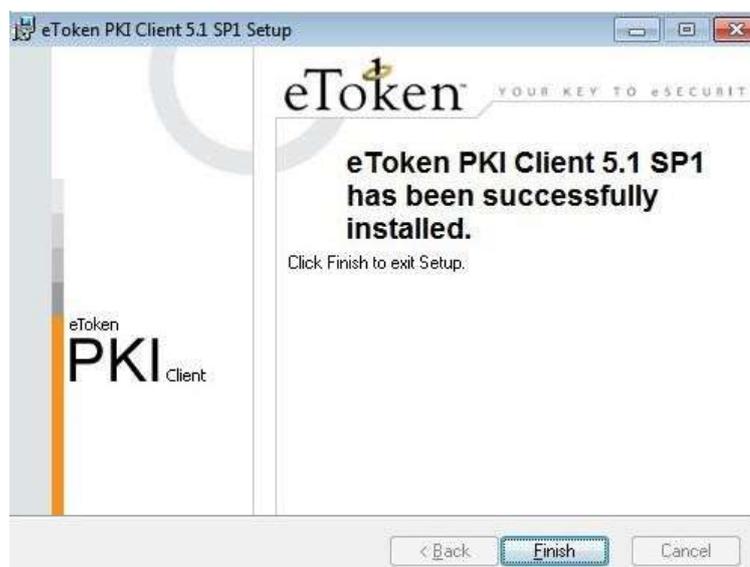
2.2.3) Согласитесь с условиями лицензионного соглашения, выбрав «I accept the license agreement». Нажмите «Next»:



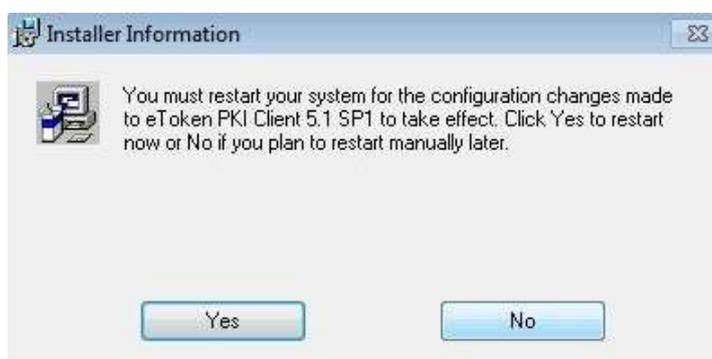
2.2.4) Откроется окно выбора папки для установки. Оставьте папку по умолчанию, нажмите «**Next**»:



2.2.5) Начнется установка драйвера. По окончании выйдет окно «eToken PKI Client 5.1 SP1 has been successfully installed», Нажимаете кнопку «**Finish**»



2.2.6) Выйдет окно с предложением перезагрузить компьютер



---

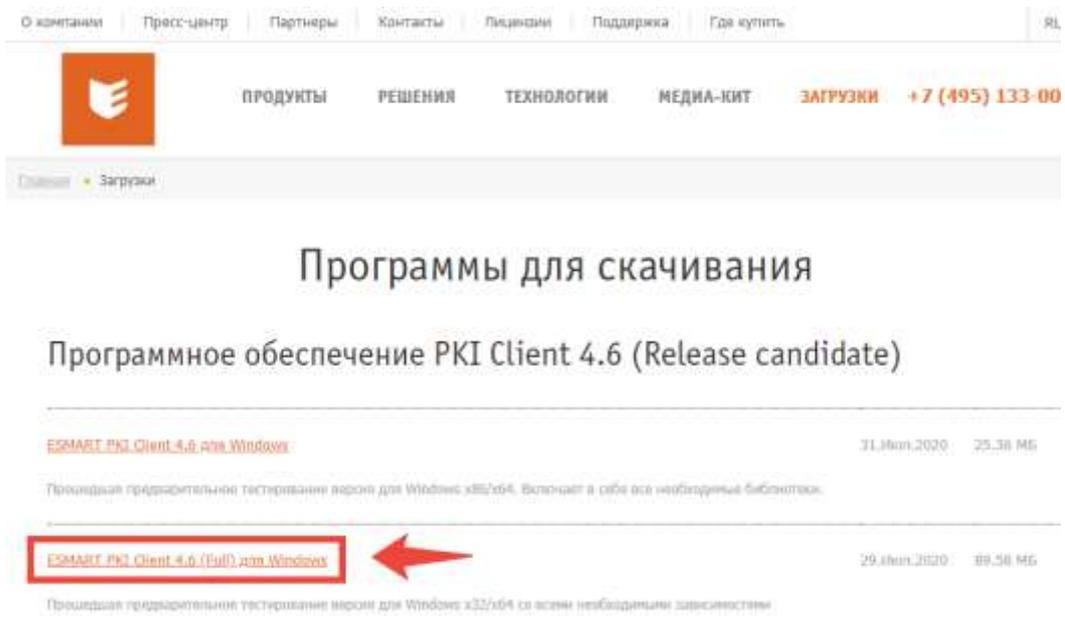
**Примечание:** Перезагрузка ОС не является обязательным условием правильного функционирования драйвера eToken, поэтому можете отказаться от её выполнения.

---

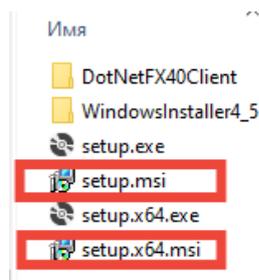
9) Вставьте в USB порт eToken. Windows должен определить его как новое устройство.

### 2.3 Установка драйвера ESMART

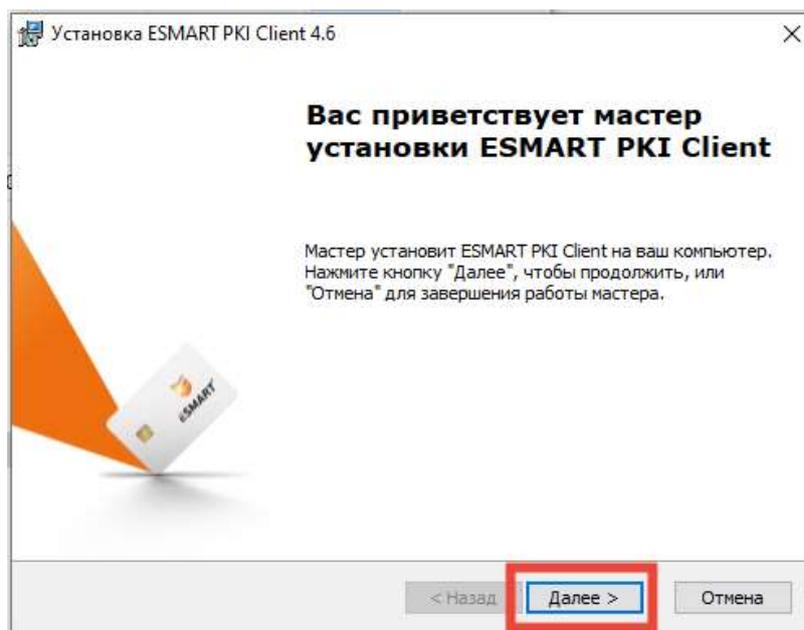
Откройте страницу <https://esmart.ru/download/> и загрузите файл «*ESMART PKI Client 4.6 (Full) для Windows*».



В загруженном архиве запустите файл *setup.msi* или *setup.x64.msi* в зависимости от разрядности операционной системы.

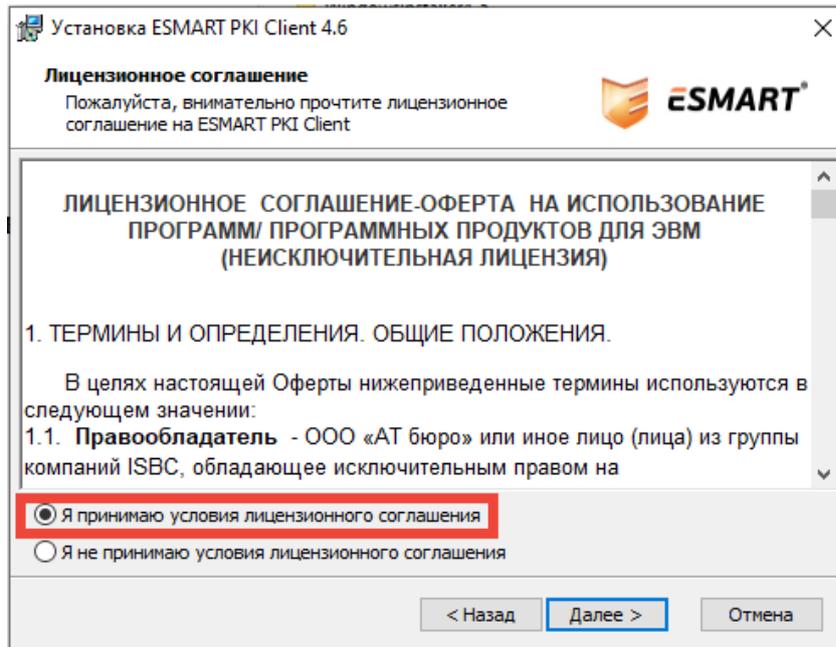


В открывшемся окне нажмите *Далее*

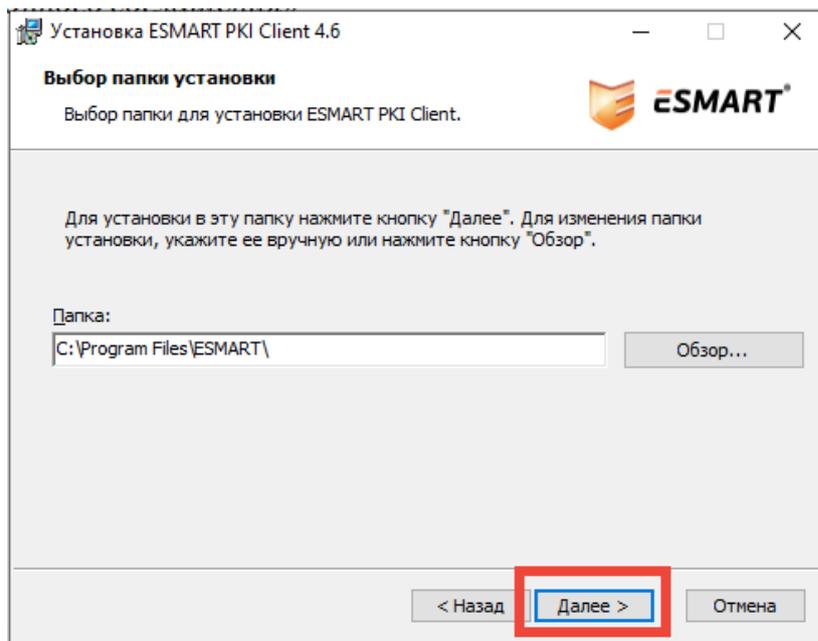


Поставьте переключатель в положение «Я принимаю условия»

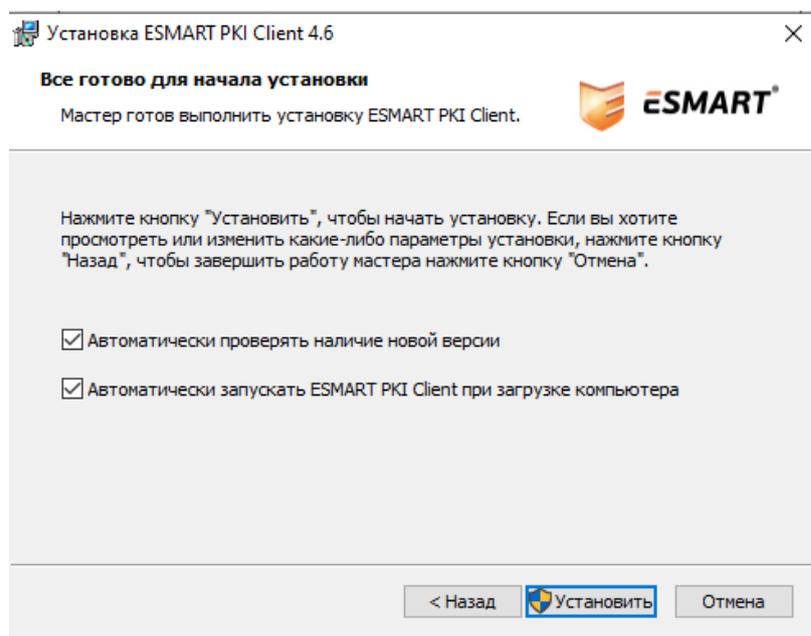
лицензионного соглашения»



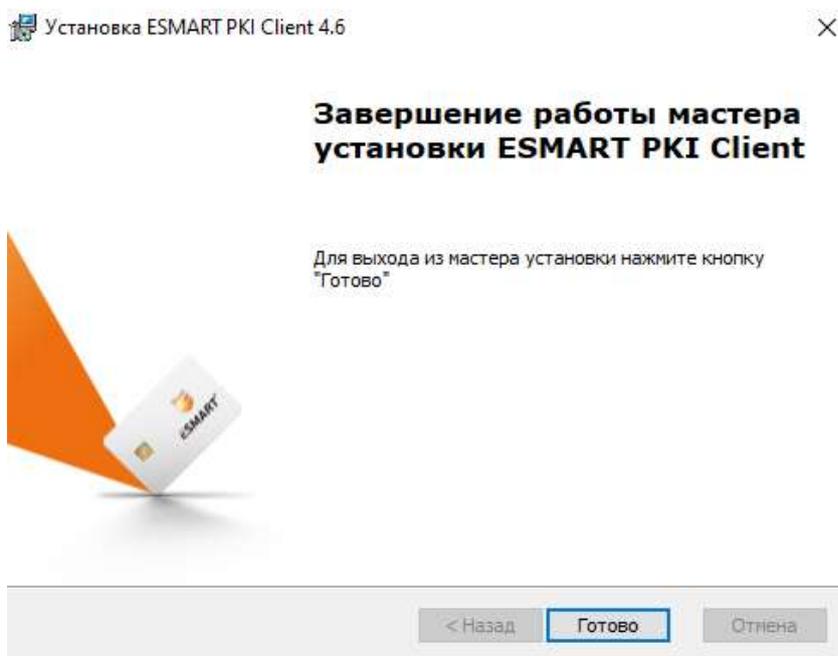
Папку установки оставьте по умолчанию



На следующем шаге поставьте все флаги и нажмите *Установить*



Дождитесь окончания установки и нажмите *Готово*



## 2.4 Установка драйвера Jacarta

Откройте страницу [https://www.aladdin-rd.ru/support/downloads/jacarta\\_client](https://www.aladdin-rd.ru/support/downloads/jacarta_client) и загрузите файл

«ПК "Единый Клиент JaCarta 2.13" (версия для 32-битных систем)»

или

«ПК "Единый Клиент JaCarta 2.13" (версия для 64-битных систем)»

## Центр загрузки

### Единый Клиент JaCarta 2.13

ПК "Единый Клиент JaCarta" — программный комплекс, предназначенный для поддержки функций строгой двухфакторной аутентификации, настройки и работы с моделями USB-токенов и смарт-карт JaCarta, генерации запросов на сертификаты. Версия для Microsoft Windows включает в себя компонент JaCarta SecurLogon.

Внимание пользователям ЕГАИС, работающим с JaCarta на компьютерах под управлением ОС Microsoft Windows! В случае установки ПК "Единый Клиент JaCarta" 2.13 необходимо дополнительно установить [Модуль поддержки устройств JaCarta для ЕГАИС](#).

#### Microsoft Windows

##### Дистрибутивы

 [ПК "Единый Клиент JaCarta 2.13" \(версия для 32-битных систем\)](#)

 [ПК "Единый Клиент JaCarta 2.13" \(версия для 64-битных систем\)](#)



##### Документация

 [ПК "Единый Клиент JaCarta" 2.13. Руководство пользователя для Windows](#)

 [ПК "Единый Клиент JaCarta" 2.13. Руководство администратора для Windows](#)

 [ПК "Единый Клиент JaCarta" 2.13. Инструкция по сбору диагностической информации](#)

#### Техническая поддержка

[Мои обращения](#)

[Создать новое обращение](#)

[Комплекты разработчика](#)

[Центр загрузки](#)

[Обучение и сертификация](#)

#### Полезные ресурсы

[База знаний](#)

[Интеграционные инструкции](#)

[Продукты, снятые с продаж](#)

[Правила оказания услуг](#)

На следующей странице нажимаете кнопку «Скачать»

## Центр загрузки

### ПК "Единый Клиент JaCarta 2.13" (версия для 64-битных систем)

ИМЯ ФАЙЛА	РАЗМЕР	
JaCartaUnifiedClient_2.13.3.3108_win-x64_ru-Ru.msi	43 MB	<a href="#">Скачать</a>



ПК "Единый Клиент JaCarta" — программный комплекс, предназначенный для поддержки функций строгой двухфакторной аутентификации, настройки и работы с моделями USB-токенов и смарт-карт JaCarta, генерации запросов на сертификаты.

Актуальная информация по продукту [ПК "Единый Клиент JaCarta"](#).

[← Единый Клиент JaCarta 2.13](#)

[← Центр загрузки](#)

#### Техническая поддержка

[Мои обращения](#)

[Создать новое обращение](#)

[Комплекты разработчика](#)

[Центр загрузки](#)

[Обучение и сертификация](#)

#### Полезные ресурсы

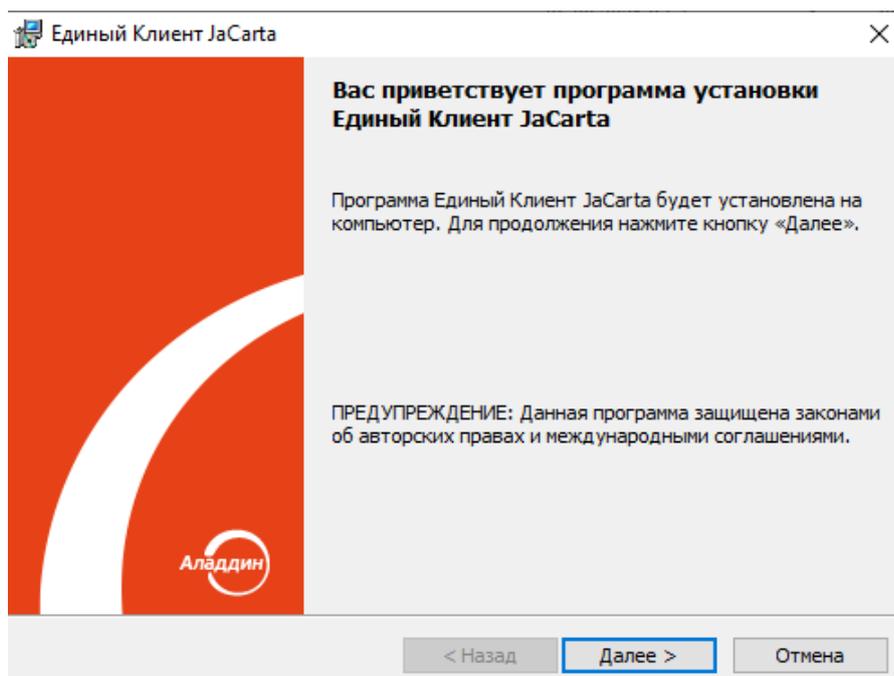
[База знаний](#)

[Интеграционные инструкции](#)

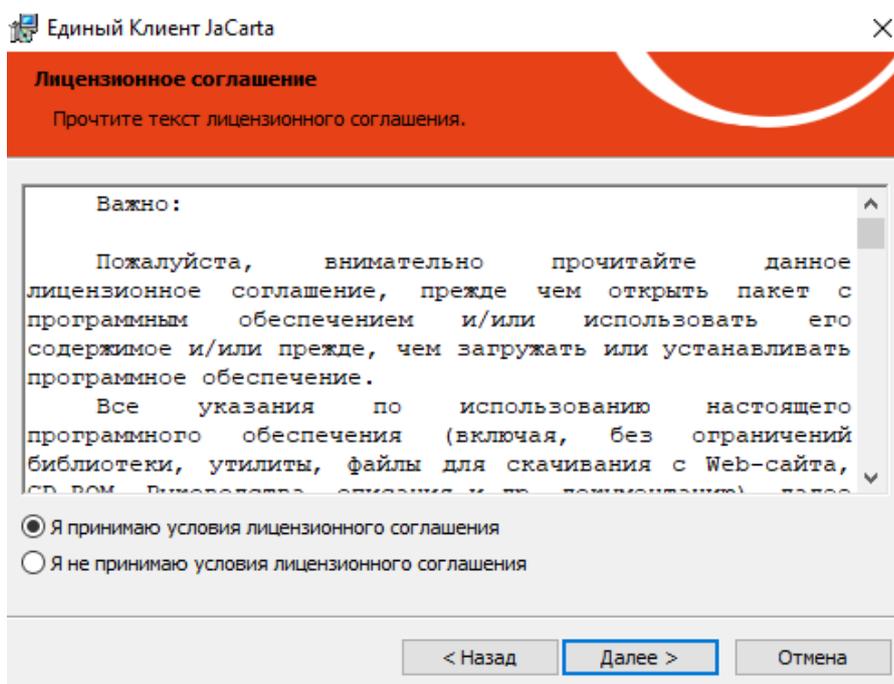
[Продукты, снятые с продаж](#)

[Правила оказания услуг](#)

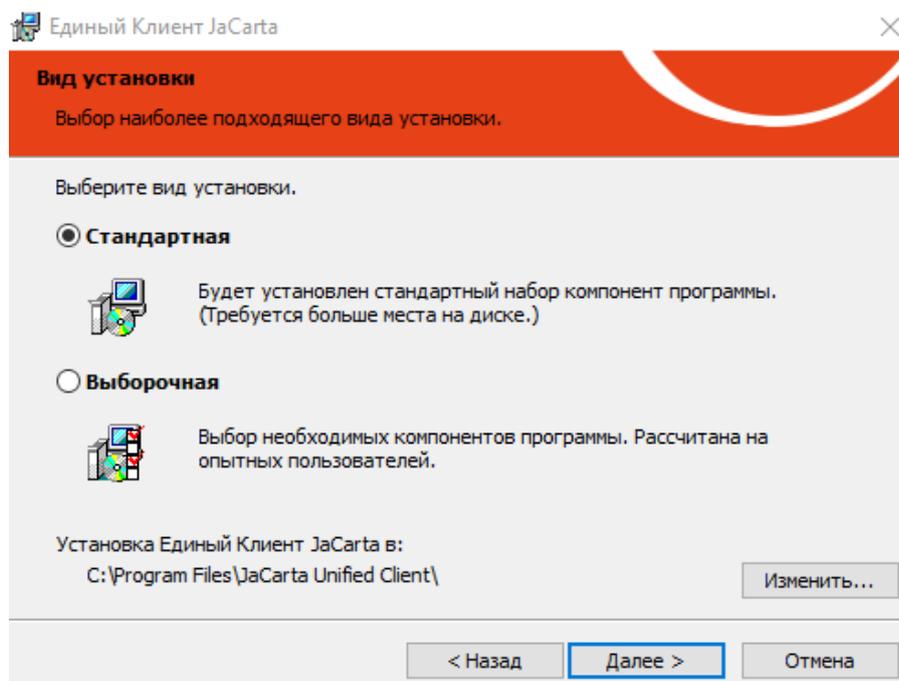
Запускаете загруженный файл и нажимаете «Далее»



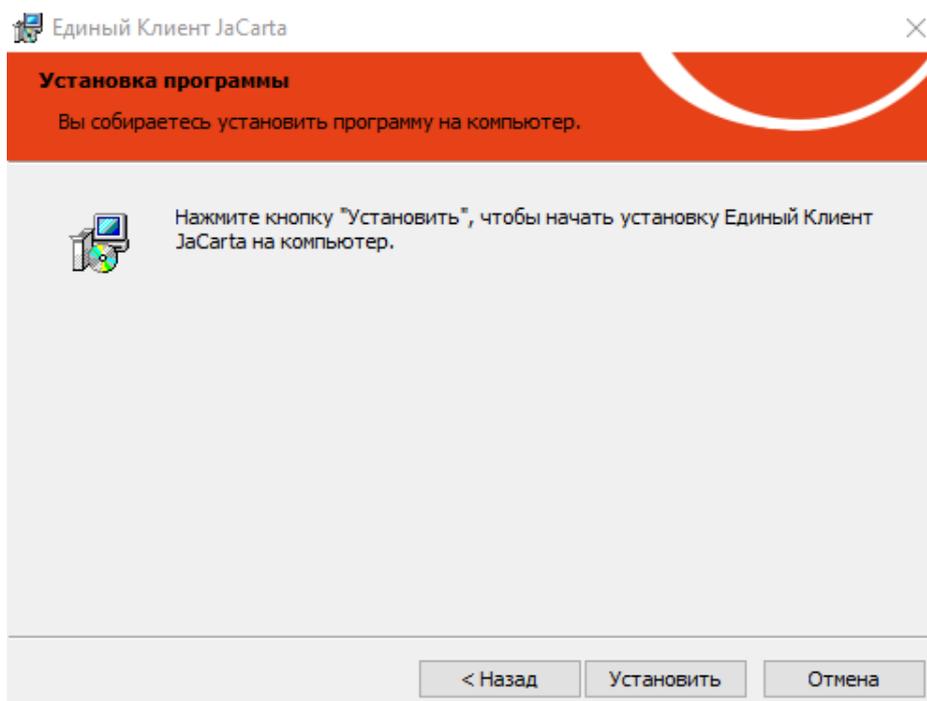
Принимаете условия лицензионного соглашения, нажимаете «Далее»



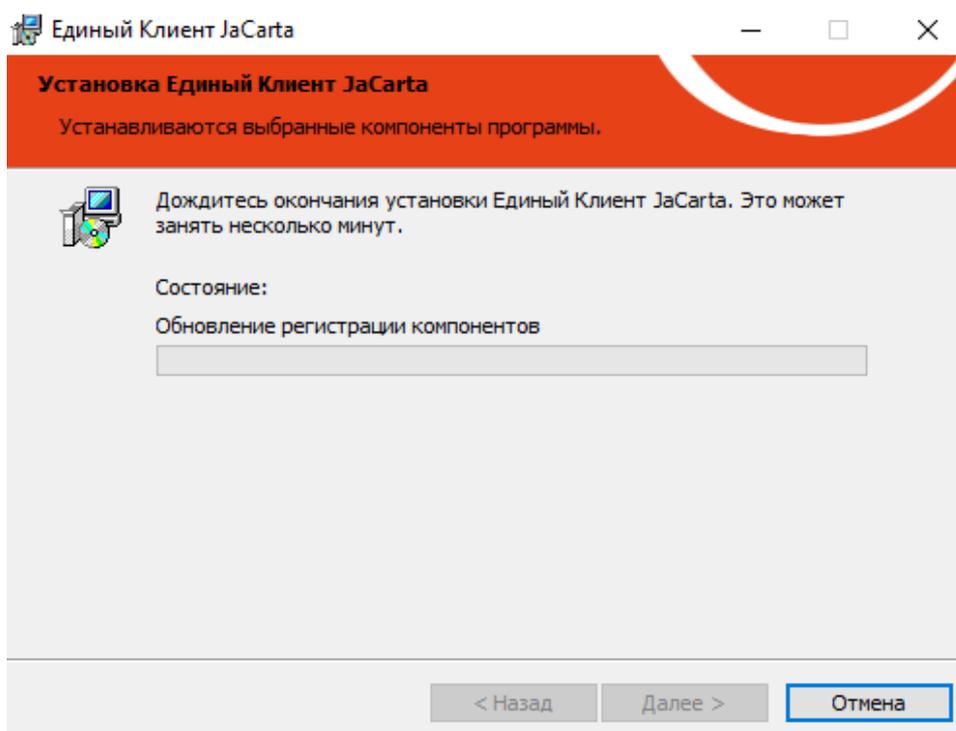
Выбираете стандартную установку, нажимаете «Далее»



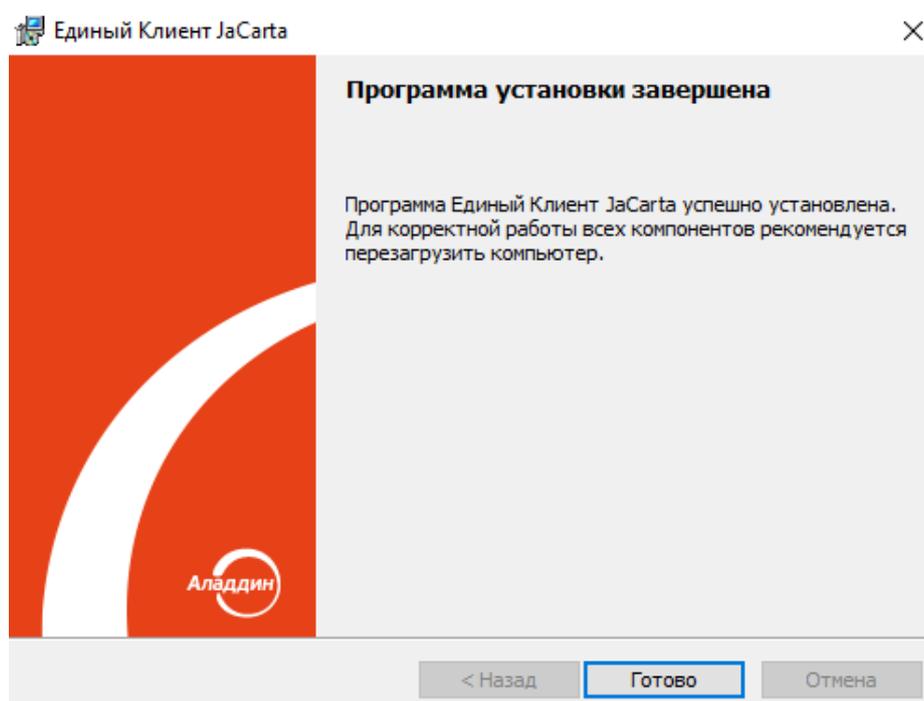
Нажимаете «Установить»



Дождитесь окончания установки



Нажимаете «Готово»



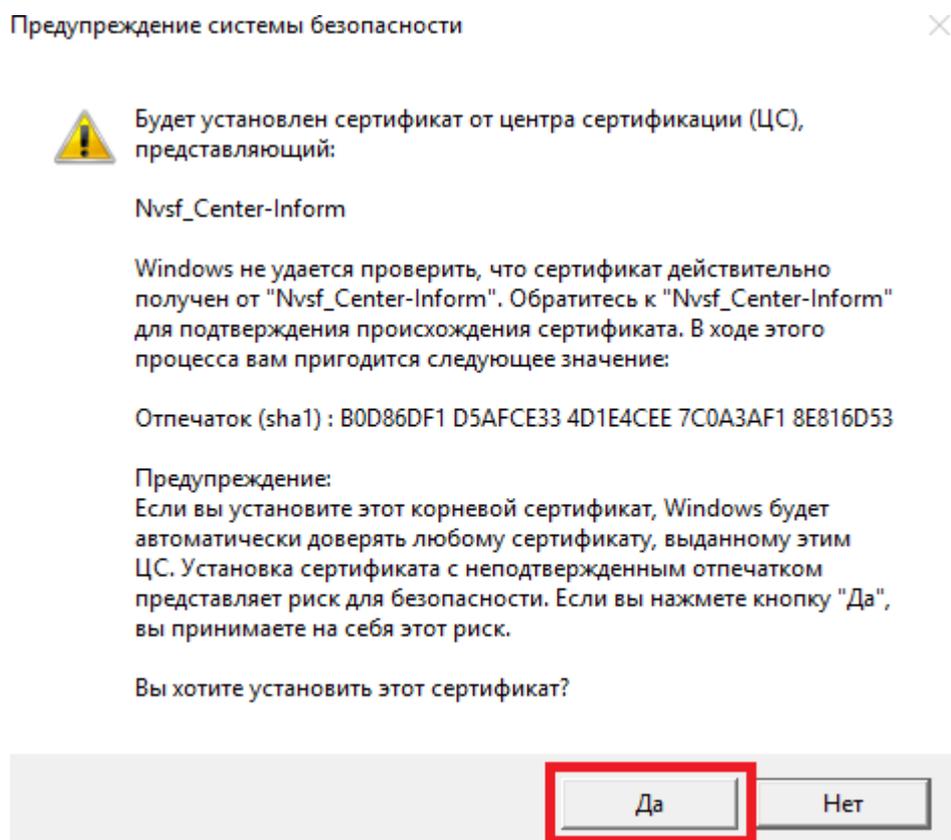
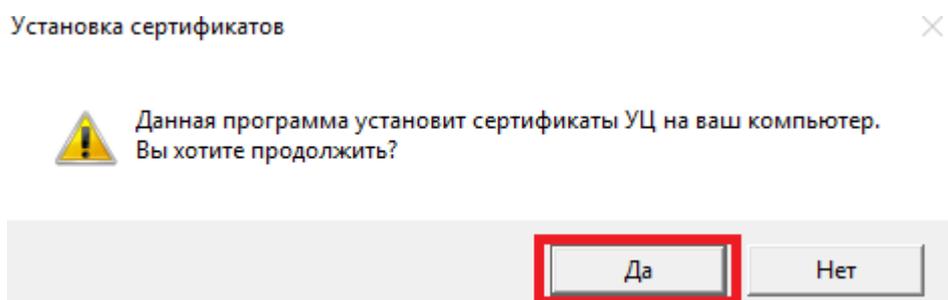
### 3. Загрузка и установка корневых сертификатов УЦ

Важным элементом любых криптографических ключей является сертификат или набор сертификатов поставщика (УЦ), выпустивших эти ключи и содержащих сведения для идентификации поставщика и цифровую

подпись поставщика, заверяющую действительность связи между ключом субъекта и сведениями для его идентификации. Такой сертификат или набор сертификатов поставщика принято называть «Корневыми сертификатами»

### 3.1 Автоматическая установка корневых сертификатов

Скачайте утилиту установки корневых сертификатов по ссылке [http://ci54.ru/files/xinstall\\_cert.exe](http://ci54.ru/files/xinstall_cert.exe). Запустите и разрешите установку всех предложенных сертификатов.



## 3.2 Ручная установка корневых сертификатов

**Примечание:** Если Вы выполнили автоматическую установку корневых сертификатов в пункте 3.1, то ручную установку корневых сертификатов выполнять **не нужно**, переходите к разделу 4.

### 3.2.1 Установка в доверенные корневые центры сертификации

Скачайте со страницы <https://e-trust.gosuslugi.ru/MainCA> сертификаты

[ПАК "Головной удостоверяющий центр" \(действует с 20.07.2012 по 17.07.2027\)](#)

Портал уполномоченного федерального органа в области использования электронной подписи [Вход через ЕСИА](#)

ГЛАВНАЯ | АККРЕДИТАЦИЯ | ГОЛОВНОЙ УЦ | РЕЕСТРЫ | ОБЪЕКТНЫЕ ИДЕНТИФИКАТОРЫ РФ | МОНИТОРИНГ УЦ

НОРМАТИВНЫЕ ДОКУМЕНТЫ | КОНТАКТЫ

Данный раздел содержит информацию о головном удостоверяющем центре

В соответствии с [Постановлением Правительства РФ от 28.11.2011 №975](#) «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи» функция **головного удостоверяющего центра** в отношении аккредитованных удостоверяющих центров осуществляет **Министерство связи и массовых коммуникаций Российской Федерации**.

**Общие сведения**

ИНН: 7710474375  
ОГРН: 1047702026701  
Эл. почта: dtj@minsvyaz.ru  
Web-сайт УЦ: <http://minsvyaz.ru>  
Адрес: Москва, ул. Тверская, д. 7

**ПАК "Головной удостоверяющий центр"**

Класс средств ЭП: КВ2  
Средства УЦ: ПАК «Головной УЦ»  
Адрес: Москва, ул. Тверская, д. 7

Ключи проверки ЭП уполномоченных лиц:

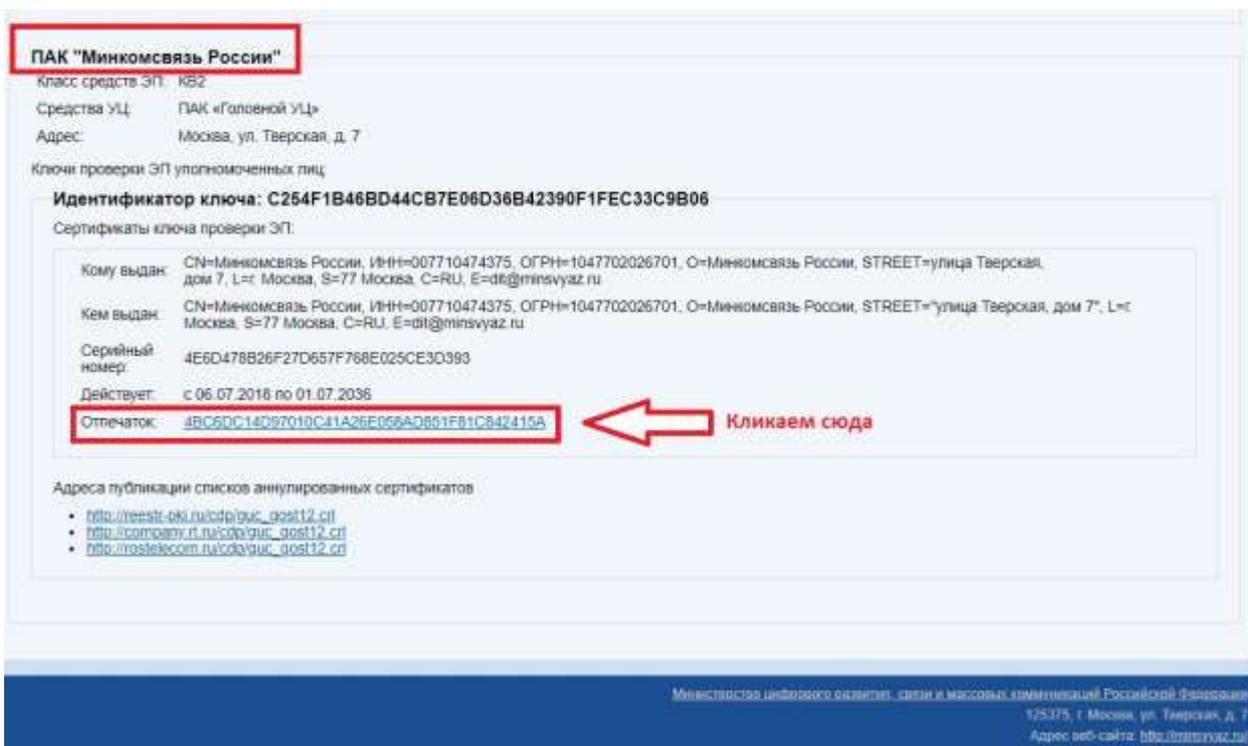
**Идентификатор ключа: 8B983B891851E8EF9C0278B8EAC8D420B255C95D**

Сертификаты ключа проверки ЭП

Кому выдан:	CN=Головной удостоверяющий центр, ИНН=007710474375, ОГРН=1047702026701, O=Минкомсвязь России, STREET="125375 г. Москва, ул. Тверская, д. 7", L=Москва, S=77 г. Москва, C=RU, E=dtj@minsvyaz.ru
Кем выдан:	CN=Головной удостоверяющий центр, ИНН=007710474375, ОГРН=1047702026701, O=Минкомсвязь России, STREET="125375 г. Москва, ул. Тверская, д. 7", L=Москва, S=77 г. Москва, C=RU, E=dtj@minsvyaz.ru
Серийный номер:	34681E40CB41EF33A9A0B7C876929A29
Действует:	с 20.07.2012 по 17.07.2027
Отпечаток:	8CAE8888ED40467AC0630854F81136D6E1DC40E2

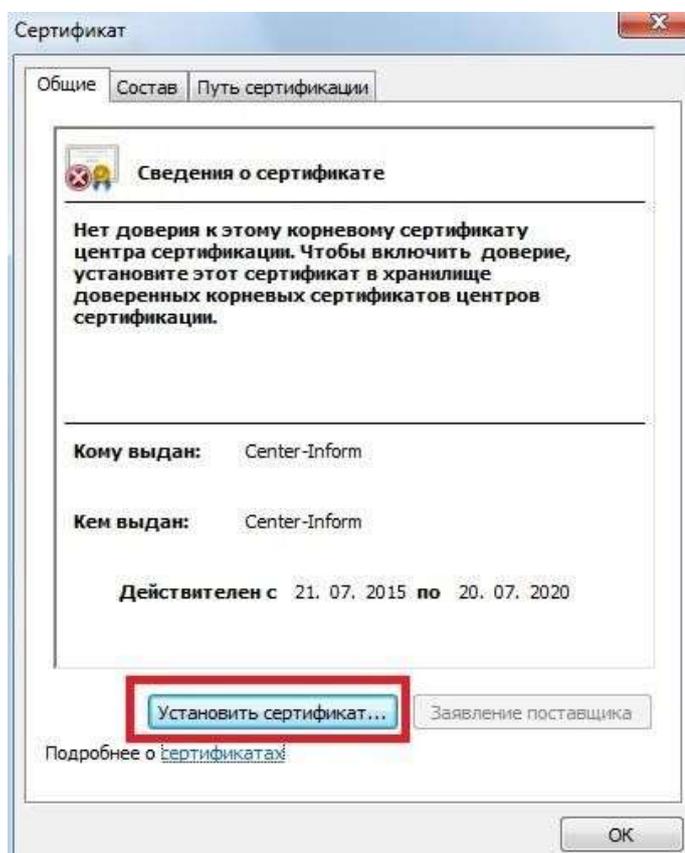
Кликаем сюда

[ПАК "Минкомсвязь России" \(действует с 06.07.2018 по 01.07.2036\)](#)

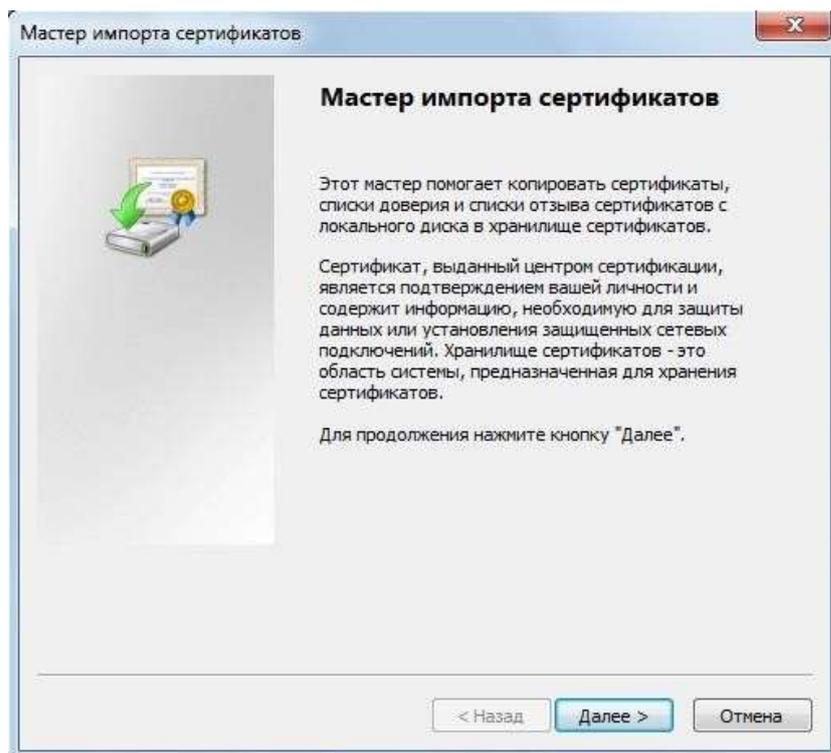


Поочередно установите сертификаты в доверенные корневые центры сертификации:

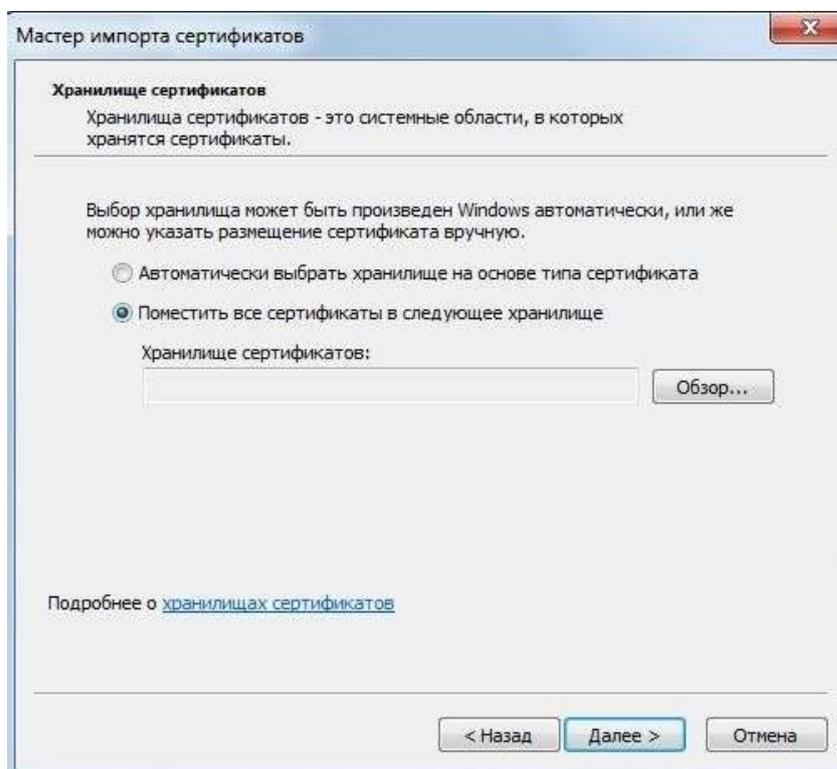
двойным щелчком мыши откройте скачанный файл и в открывшемся окне сертификата нажмите кнопку «**Установить сертификат**»:



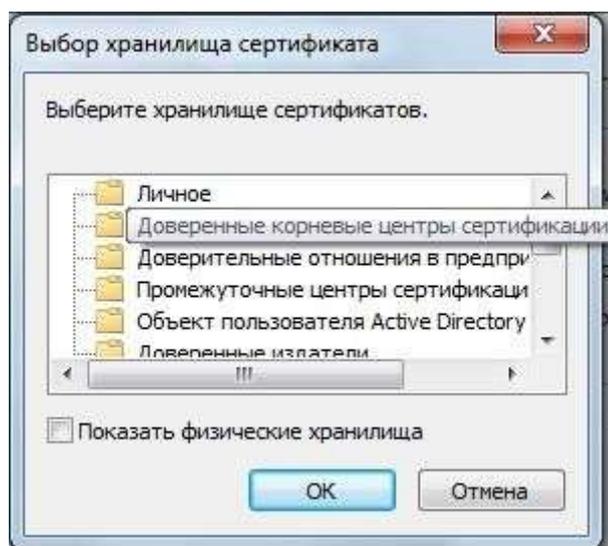
Откроется Мастер импорта сертификатов. Нажмите кнопку «Далее»:



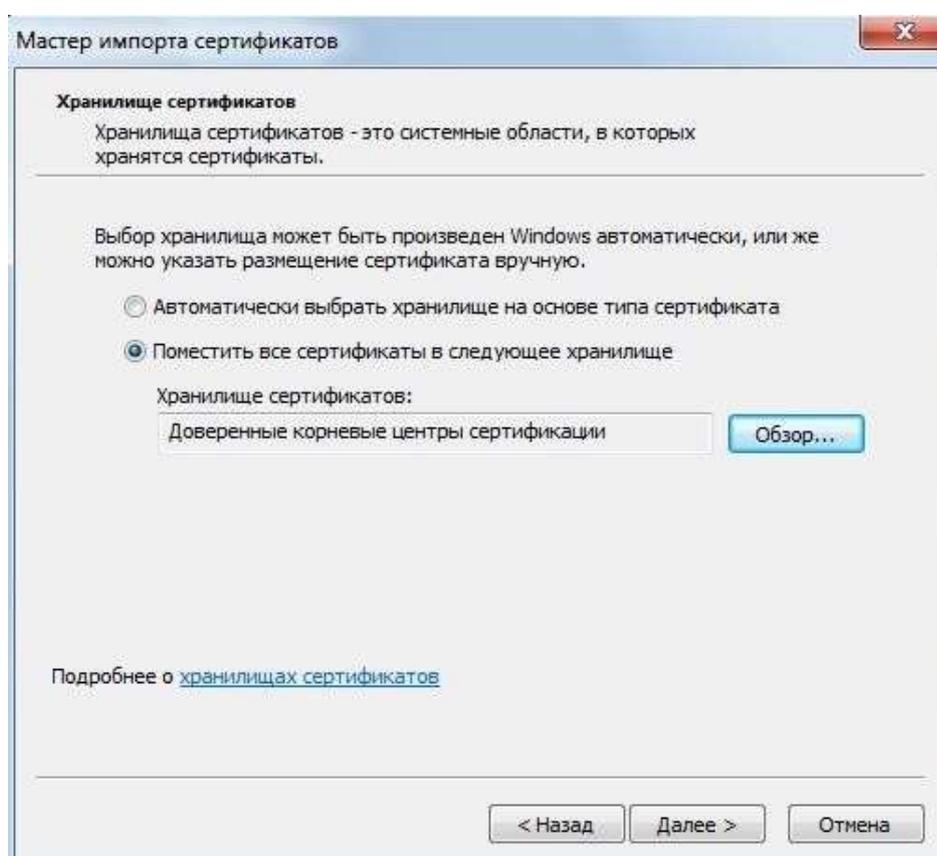
Выберите пункт «Поместить все сертификаты в следующее хранилище» и нажмите кнопку «Обзор».



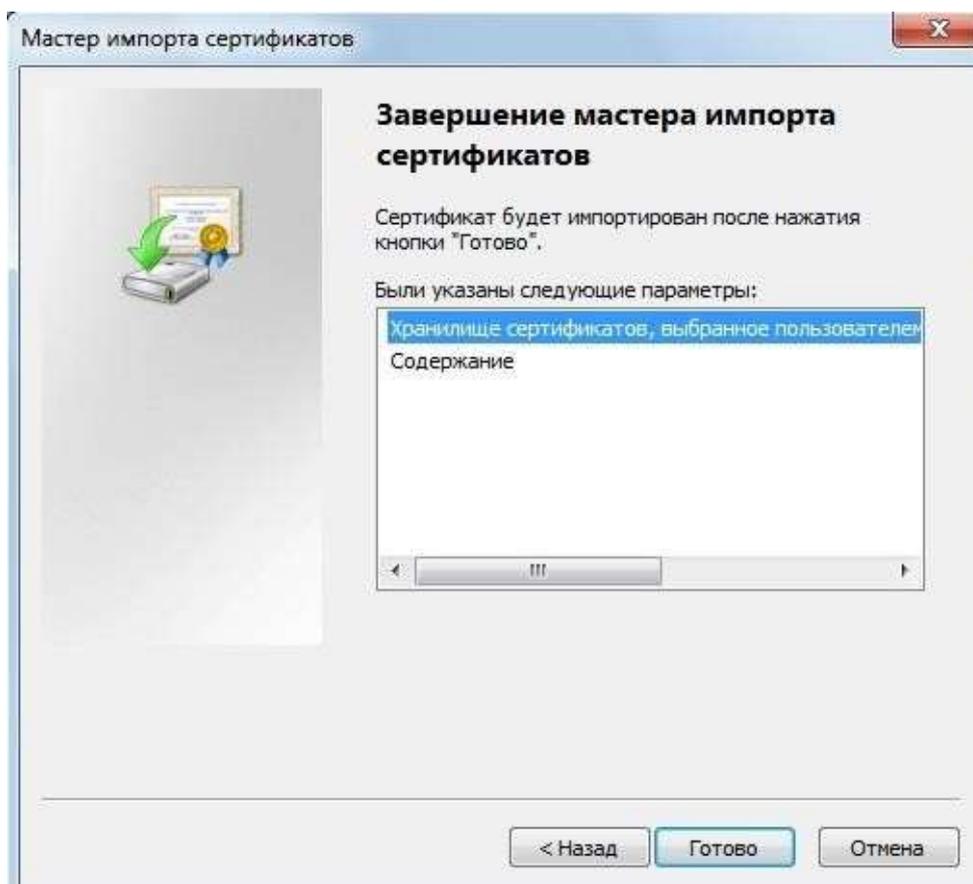
В окне «Выбор хранилища сертификата» выберите папку «Доверенные корневые центры сертификации» и нажмите кнопку «ОК»:



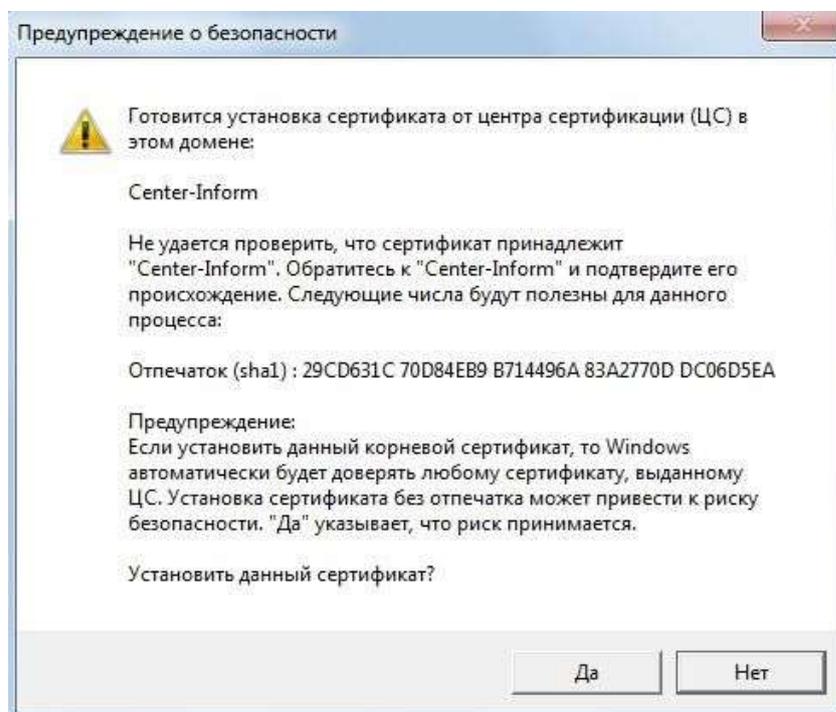
Указав хранилище сертификата, нажмите кнопку «Далее»:



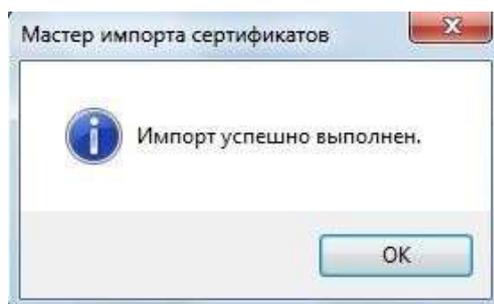
Для завершения установки сертификата нажмите кнопку «Готово»:



Появится «Предупреждение системы безопасности»:



Подтвердите установку сертификата нажатием кнопки «Да». Мастером будет выдано сообщение об успешном импорте сертификата:



Нажатием кнопок «ОК» закройте окна сообщения и сертификата.

### 3.2.2 Установка в промежуточные центры сертификации

Скачайте со страницы <http://www.ci54.ru/index.php?id=73> следующие сертификаты

- [Корневой сертификат ПУЦ аккредитованного в МКС Новосибирского филиала АО «ЦентрИнформ» в соответствии с 63-ФЗ от 31.07.2018 \(ГОСТ 34.10-2012\)](#)

- [Корневой сертификат ПУЦ аккредитованного в МКС Новосибирского филиала АО «ЦентрИнформ» в соответствии с 63-ФЗ от 15.11.2017](#)

ЦЕНТРИНФОРМ

Главная Услуги Партнеры Публичная оферта Поддержка Контакты

## СЕРТИФИКАТЫ

Аккредитованный в Минкомсвязи удостоверяющий центр для выпуска квалифицированных сертификатов ЭП

Корневой сертификат ПУЦ аккредитованного в МКС Новосибирского филиала АО «ЦентрИнформ» в соответствии с 63-ФЗ от 10.09.2019 (ГОСТ 34.10-2012) (Скачать).

Список отозванных сертификатов ПУЦ аккредитованного в МКС Новосибирского филиала АО «ЦентрИнформ» в соответствии с 63-ФЗ (ГОСТ 34.10-2012) (Скачать) (Скачать).

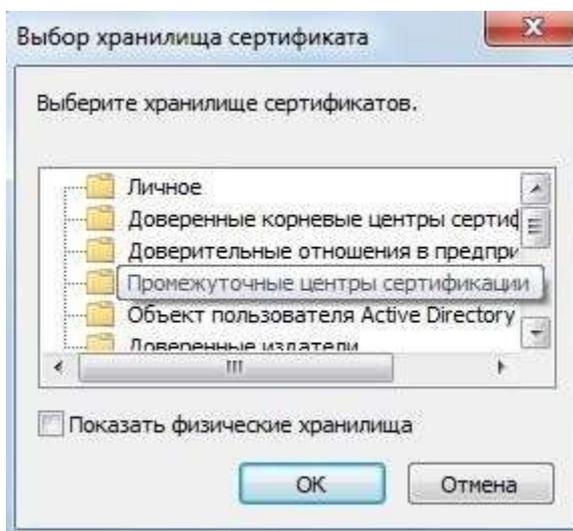
Корневой сертификат ПУЦ аккредитованного в МКС Новосибирского филиала АО «ЦентрИнформ» в соответствии с 63-ФЗ от 31.07.2018 (ГОСТ 34.10-2012) (Скачать).

Список отозванных сертификатов ПУЦ аккредитованного в МКС Новосибирского филиала АО «ЦентрИнформ» в соответствии с 63-ФЗ (ГОСТ 34.10-2012) (Скачать) (Скачать).

Формы заявлений на ОТЗЫВ, ПРИОСТАНОВЛЕНИЕ и ВОЗОБНОВЛЕНИЕ сертификатов.

Утилита для установки корневых сертификатов

Установка корневых сертификатов в промежуточные центры сертификации выполняется аналогично установке сертификатов в доверенные корневые центры, с той лишь разницей, что в качестве хранилища сертификата необходимо указать **«Промежуточные центры сертификации»**:



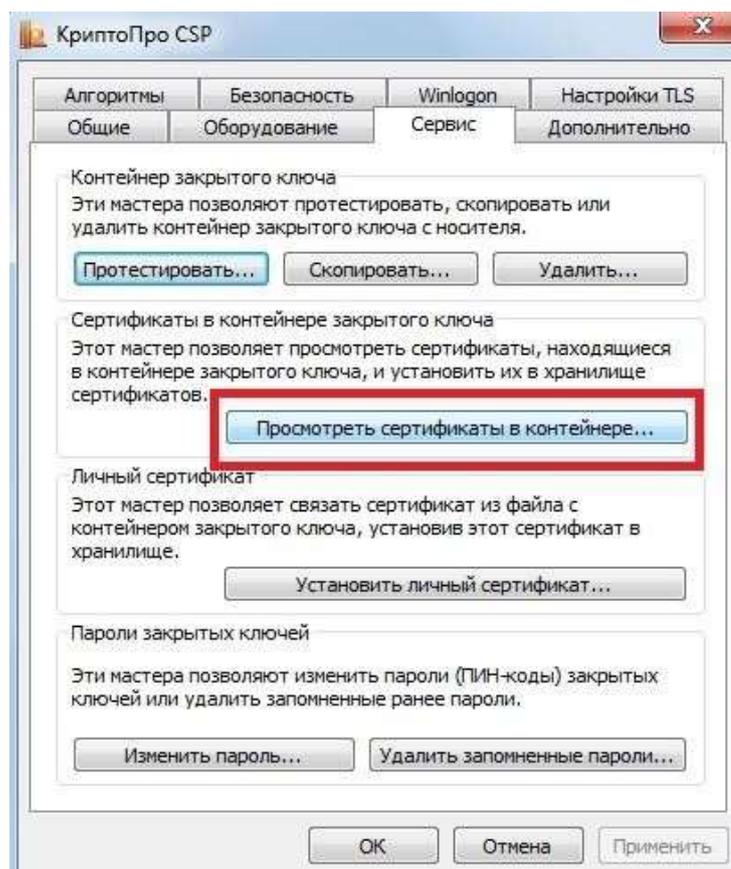
#### 4. Установка Личного сертификата

Под установкой личного сертификата понимается установка сертификата субъекта (вашего сертификата) в хранилище **«Личные»** с формированием ссылки на закрытый ключ, соответствующий данному сертификату.

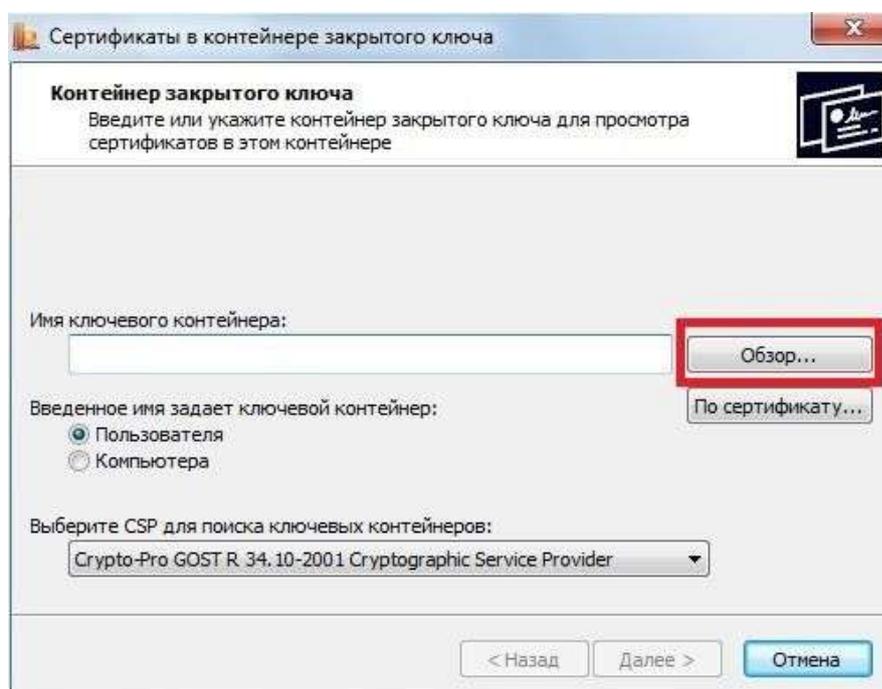
Установку Личного сертификата рекомендуем выполнять в приведенной ниже последовательности.

4.1) Подключите ключевой носитель (Rutoken или eToken) с вашей ЭП к USB-порту компьютера.

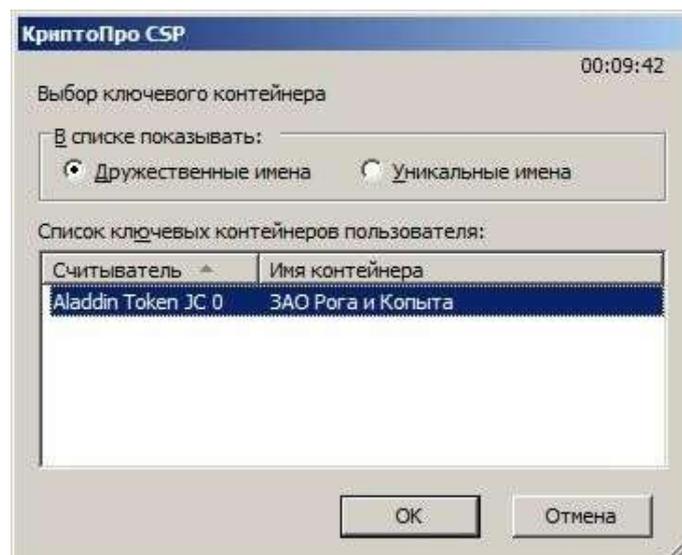
4.2) Запустите КриптоПро CSP (Панель управления -> **КриптоПро CSP**). В открывшемся окне управления свойствами КриптоПро CSP на вкладке **«Сервис»** нажмите кнопку **«Посмотреть сертификаты в контейнере»**:



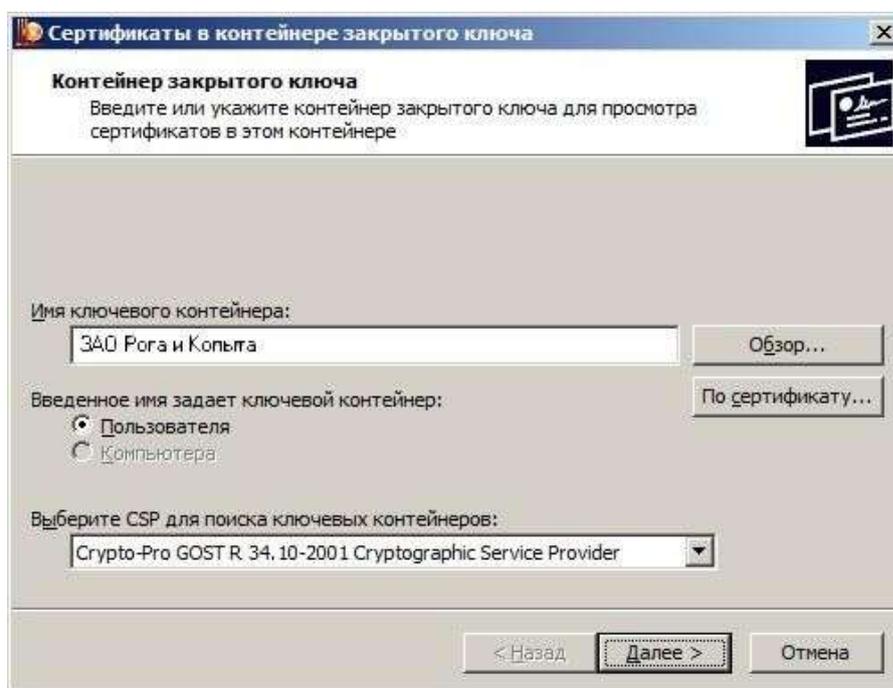
4.3) Откроется окно указания контейнера закрытого ключа:



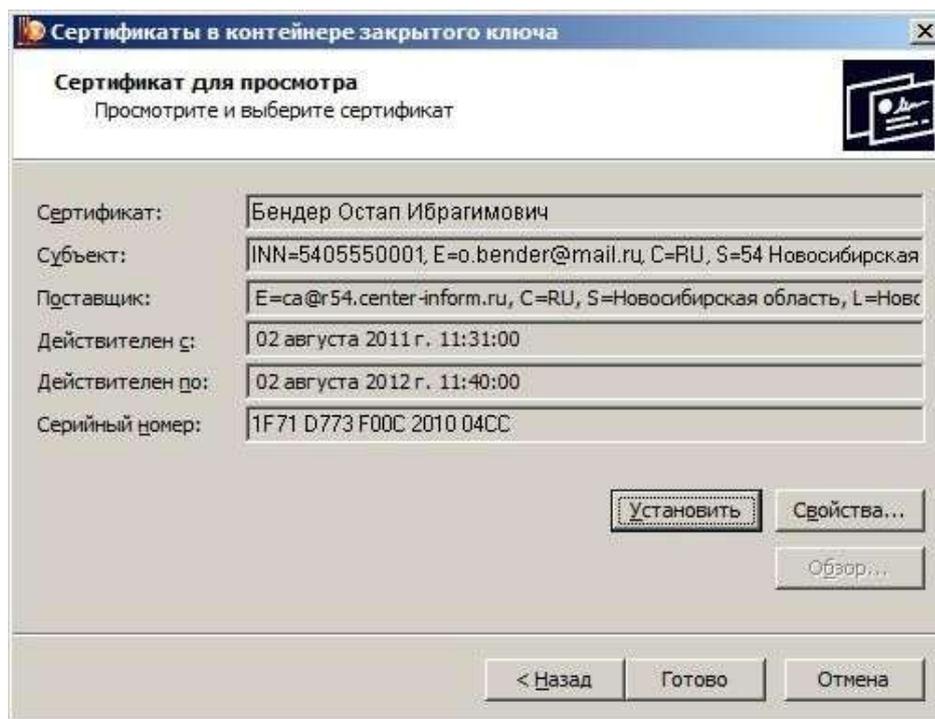
4.4) Нажатием кнопки «Обзор» откройте окно выбора ключевого контейнера. В списке обнаруженных ключевых контейнеров укажите контейнер вашей ЭП и нажмите кнопку «ОК».



4.5) Имя выбранного ключевого контейнера будет подставлено в соответствующее поле. Нажмите кнопку «Далее»:



4.6) Откроется окно просмотра и установки сертификата:

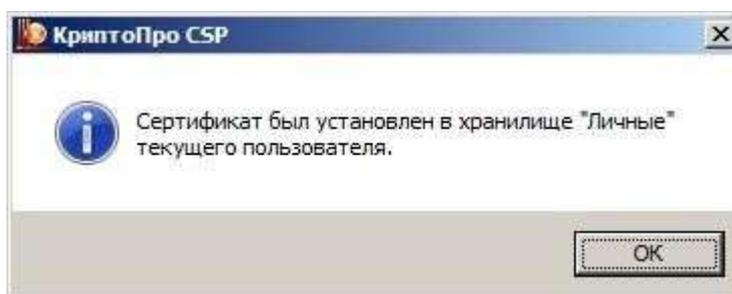


---

**Примечание:** Полную информацию о сертификате можно получить нажатием кнопки «Свойства».

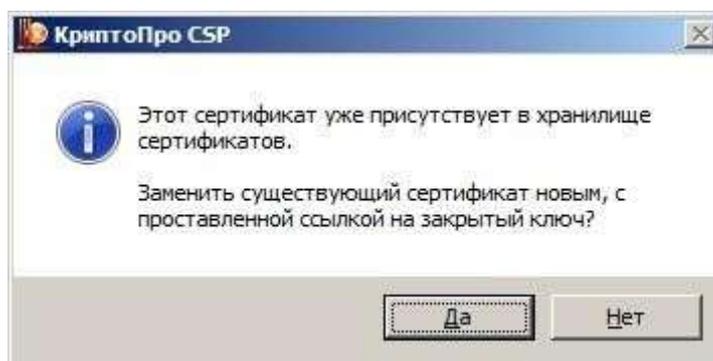
---

4.7) Нажатием кнопки «Установить» будет выполнена установка сертификата выбранного ключевого контейнера в хранилище Личных сертификатов:



---

**Примечание:** Если в настройках ключевых носителей установлены параметры автоматической установки сертификатов с данного типа носителей, то при первом подключении вашего ключевого носителя размещенный на нем сертификат был автоматически установлен в хранилище личных сертификатов, о чем системой будет выдано соответствующее сообщение:



Нажатием кнопки «**Да**» будет выполнена замена ранее установленного Личного сертификата выбранным, нажатием кнопки «**Нет**» установка выбранного сертификата будет отменена. Вы можете выбрать любой вариант — на результат установки Личного сертификата это никак не повлияет.

---

Завершив установку Личного сертификата, закройте окна Сертификата и КриптоПро CSP.

## **Заключение**

Если у вас возникли вопросы или проблемы, связанные с выполнением каких-либо из вышеперечисленных установок и/или настроек, вы можете в рабочие дни с 9:00 до 18:00 (в пятницу до 17:00) обратиться в службу технической поддержки пользователей Новосибирского филиала АО «ЦентрИнформ» по телефону (383) 383-30-03.

**Вы также можете воспользоваться платными услугами поддержки пользователей в режиме удаленного доступа («Однократная удаленная установка и настройка ПК» и/или «Годовая удаленная поддержка рабочего места»).**

При обращении в техническую поддержку желательно предварительно скачать и запустить программу удаленного доступа. Скачать их можно по ссылкам [TeamViewer](#), [Ammyy Admin](#), [СБИС\(удаленный помощник\)](#)

**Желаем успехов!**