Руководство пользователя

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

Новосибирск

2021

Содержание

Введение 3

1. Установка КриптоПро CSP 4

2. Установка драйвера ключевого носителя 8

2.1 Установка драйвера Rutoken 9

2.2 Установка драйвера eToken 11

2.3 Установка драйвера ESMART 15

2.4 Установка драйвера Jacarta 19

3. Загрузка и установка корневых сертификатов УЦ 23

3.1 Автоматическая установка корневых сертификатов 24

3.2 Ручная установка корневых сертификатов 25

4. Установка Личного сертификата 31

Заключение 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!

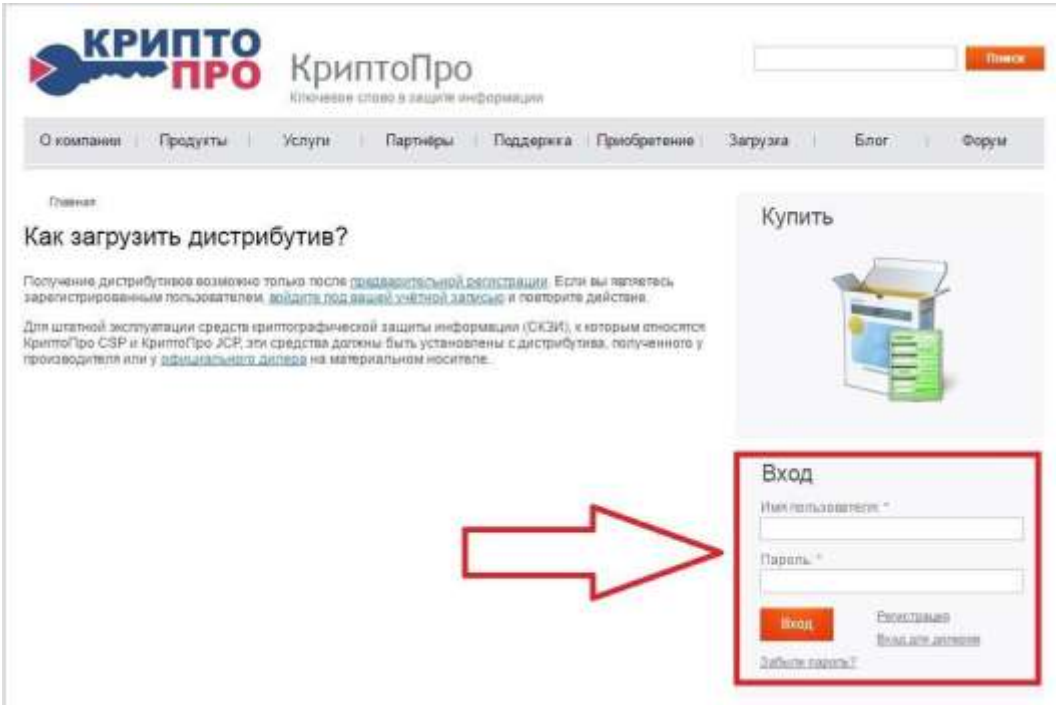
ДО НАЧАЛА РАБОТ ПО ПОДГОТОВКЕ ВАШЕГО КОМПЬЮТЕРА ДЛЯ ИСПОЛЬЗОВАНИЯ ЭЦП УБЕДИТЕСЬ В ОТСУТСТВИИ ВИРУСОВ НА НЁМ И ОБЕСПЕЧЬТЕ НАДЕЖНУЮ АНТИВИРУСНУЮ ЗАЩИТУ ВАШЕГО ПК, ИНАЧЕ КОРРЕКТНАЯ РАБОТА С ЭЦП НЕ ГАРАНТИРУЕТСЯ.

1. Установка КриптоПро CSP

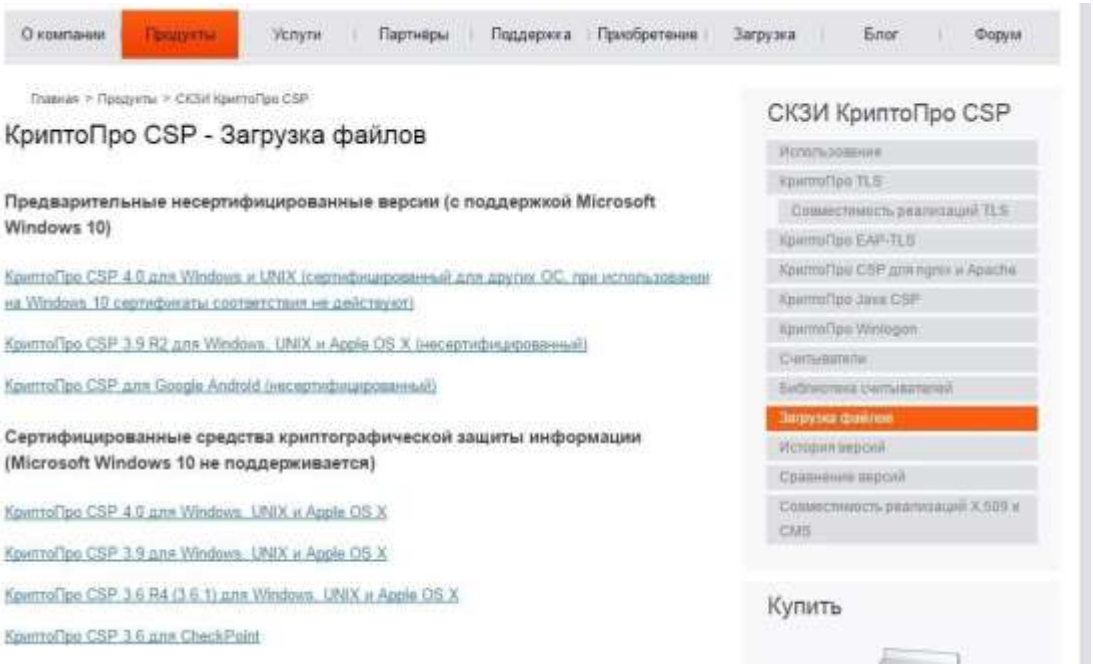
КриптоПро CSP — криптопровайдер (Cryptography Service Provider, CSP) — средство криптографической защиты информации (СКЗИ), представляющее собой независимый модуль, позволяющий осуществлять различные криптографические операции в ОС Windows и выполняющий взаимодействие с различными приложениями, работающими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

Криптопровайдер КриптоПро CSP разработан компанией «Крипто-Про» (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.

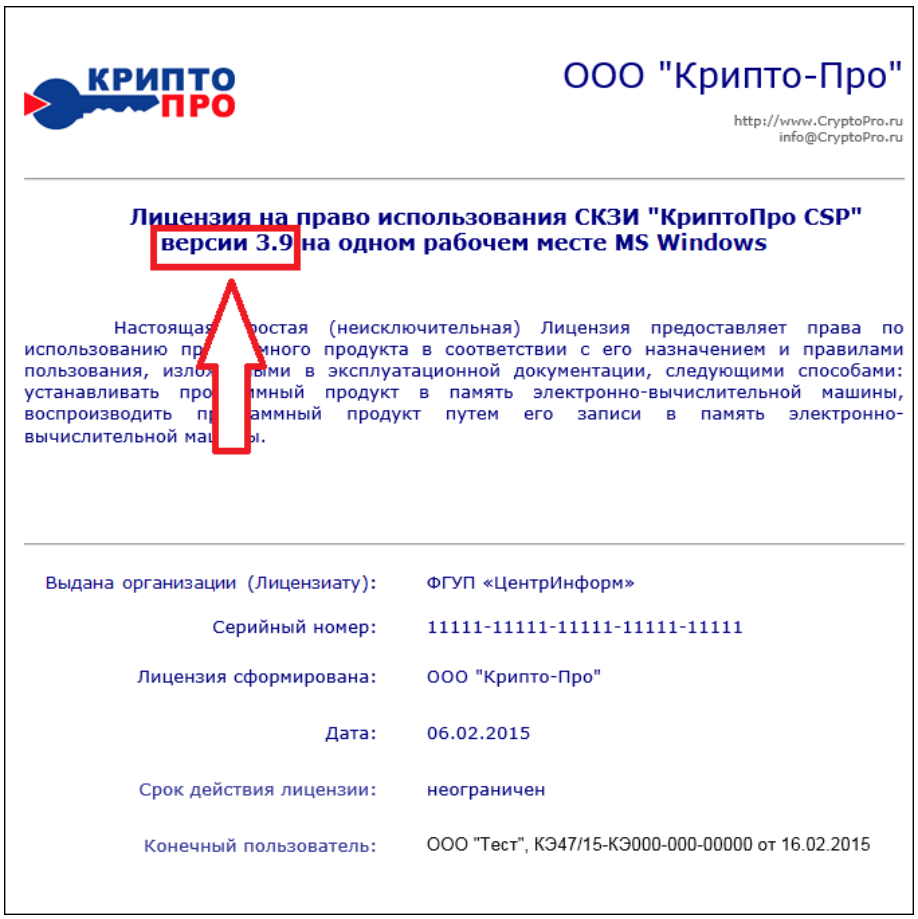
Дистрибутив КриптоПро CSP необходимо скачать с официального сайта «КриптоПро» https://www.cryptopro.ru/products/csp/downloads.



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



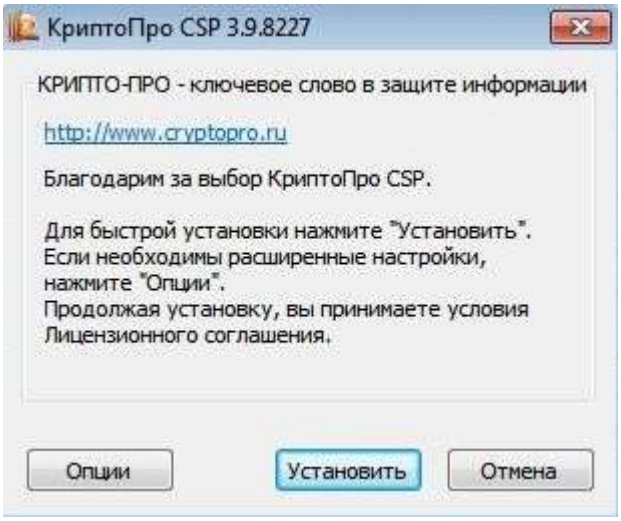
Скачать и установить нужно ту версию КриптоПРО CSP на которую была куплена лицензия. Версия лицензии указана в шапке бланка.



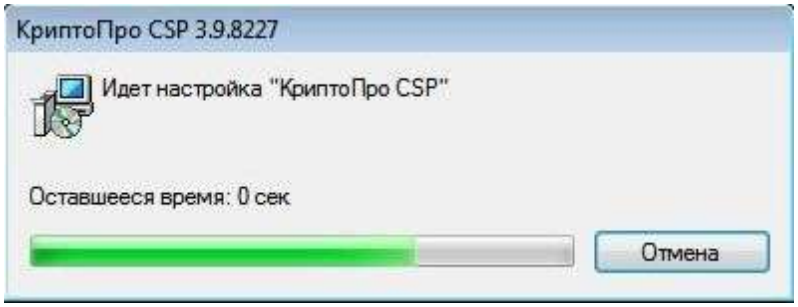
Ниже приведена последовательность установки КриптоПро CSP.

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.

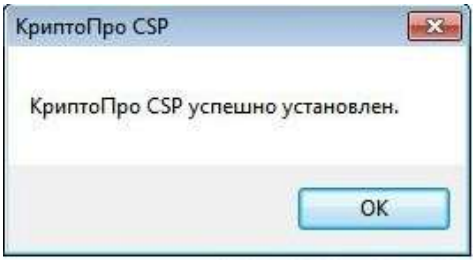
1.1) Запустите установочный пакет КриптоПро CSP. В открывшемся окне нажимаете кнопку «**Установить**»



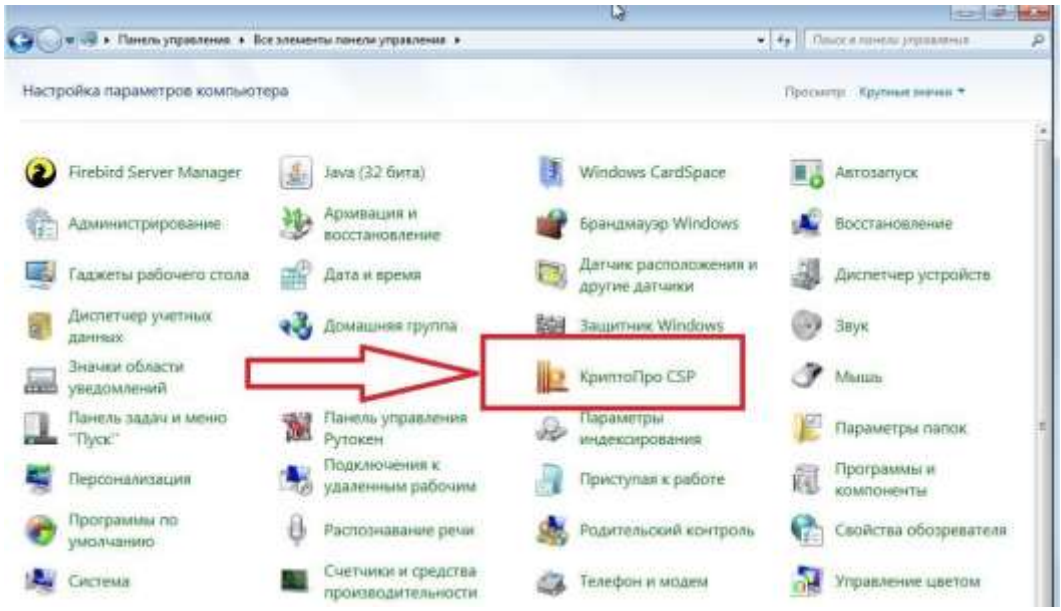
1.2) Дождитесь окончания процесса установки



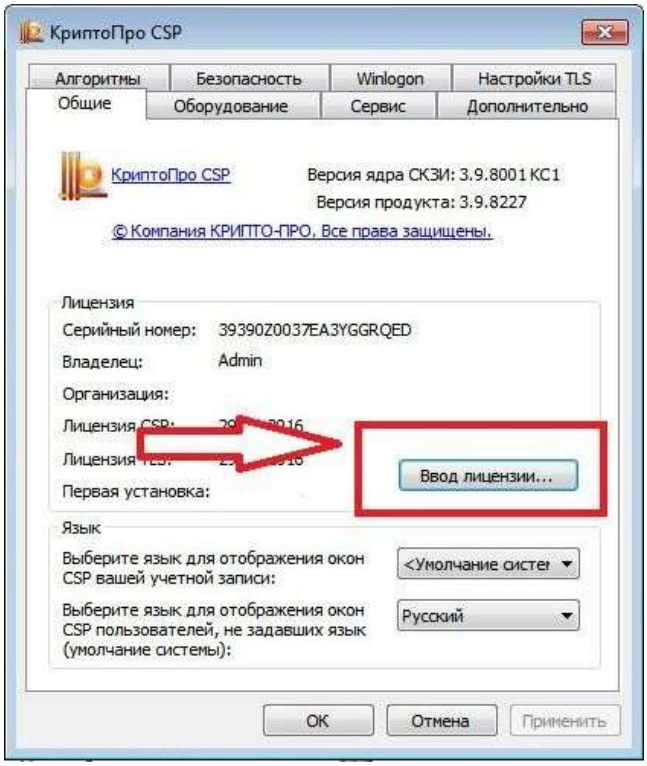
1.3) По окончанию установки выйдет окно «КриптоПро CSP успешно установлен». Нажимаете «**Ок**»



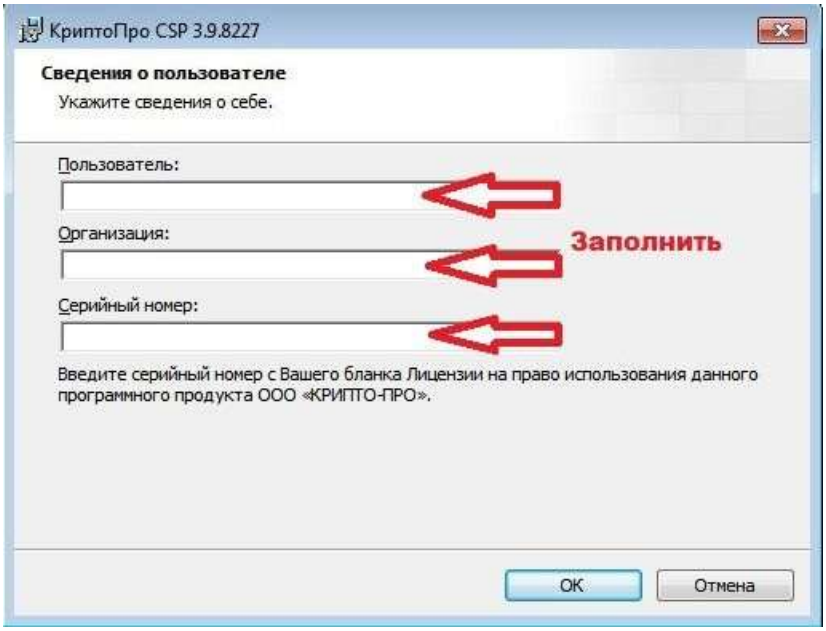
1.4) Зайдите в «**Панель управления**» Windows, откройте **КриптоПро CSP**



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

---

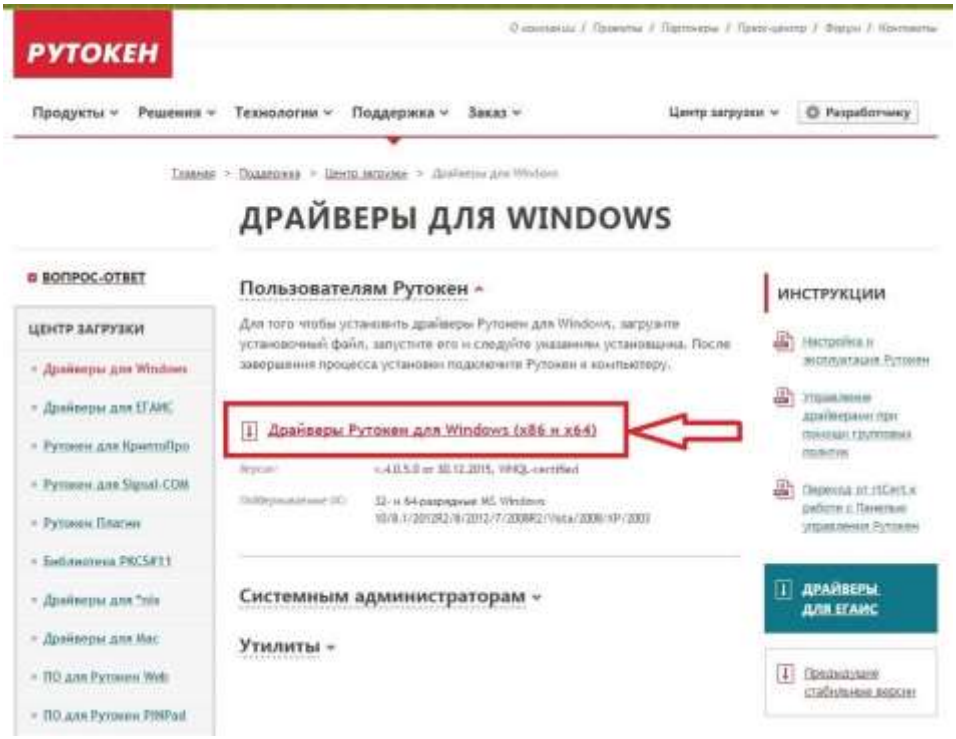
ВНИМАНИЕ! Установка драйвера ключевого носителя должна выполняться только с учетной записи пользователя имеющего права Администратора системы. До завершения установки не подключайте носитель электронных криптографических ключей с вашей ЭП к USB-порту компьютера.

Процесс установки для каждого из носителей представлен ниже.

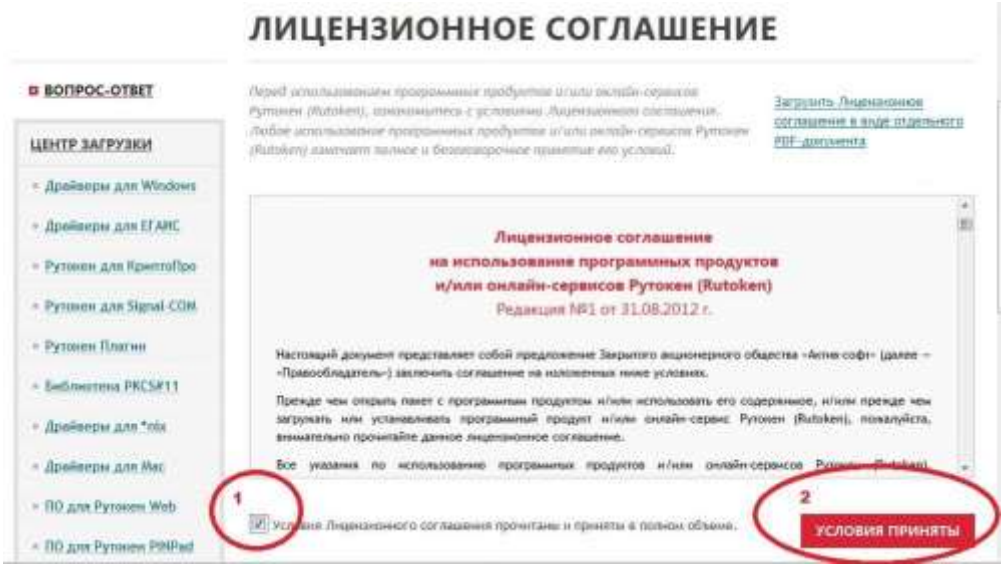
2.1 Установка драйвера Rutoken

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

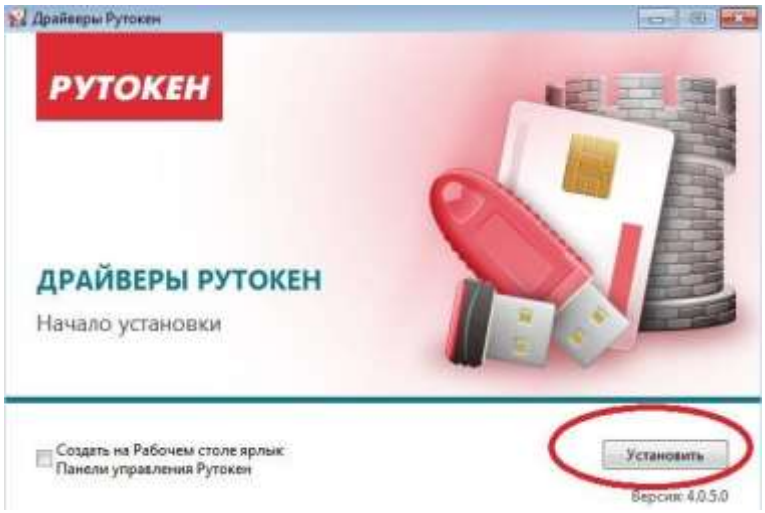
2.1.1) На странице http://www.rutoken.ru/support/download/drivers-for-windows/ нажмите на ссылку «Драйверы Рутокен для Windows (x86 и x64)»



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



2.1.3) Запустите установочный файл. Нажмите кнопку «Установить»



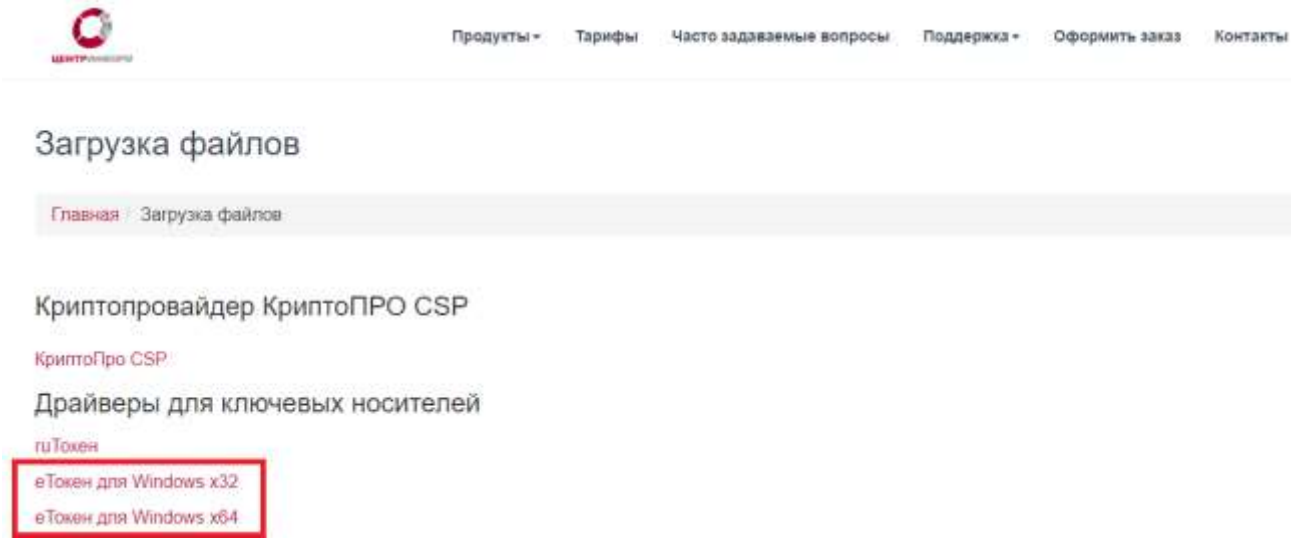
2.1.4) Дождитесь окончания установки и нажмите на кнопку «Закрыть»

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

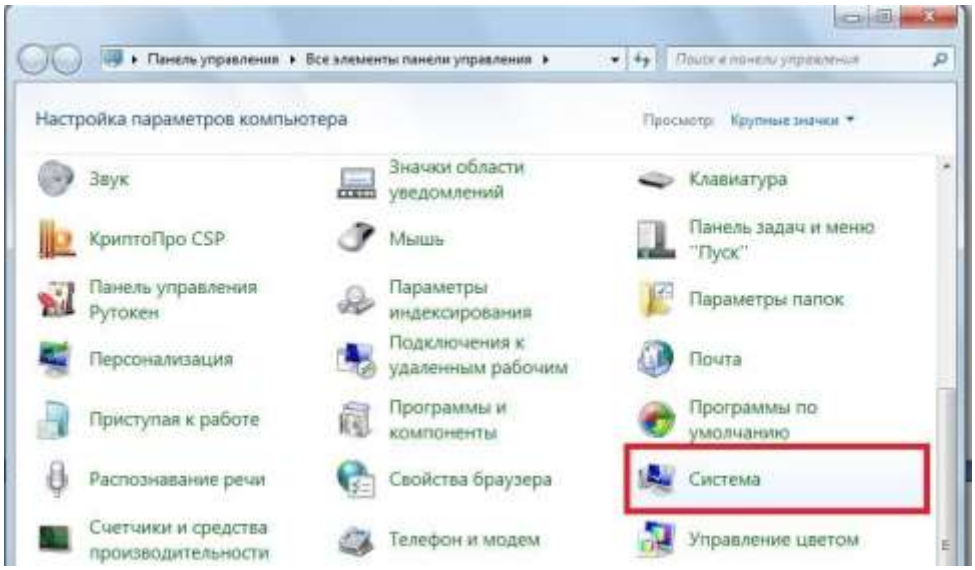


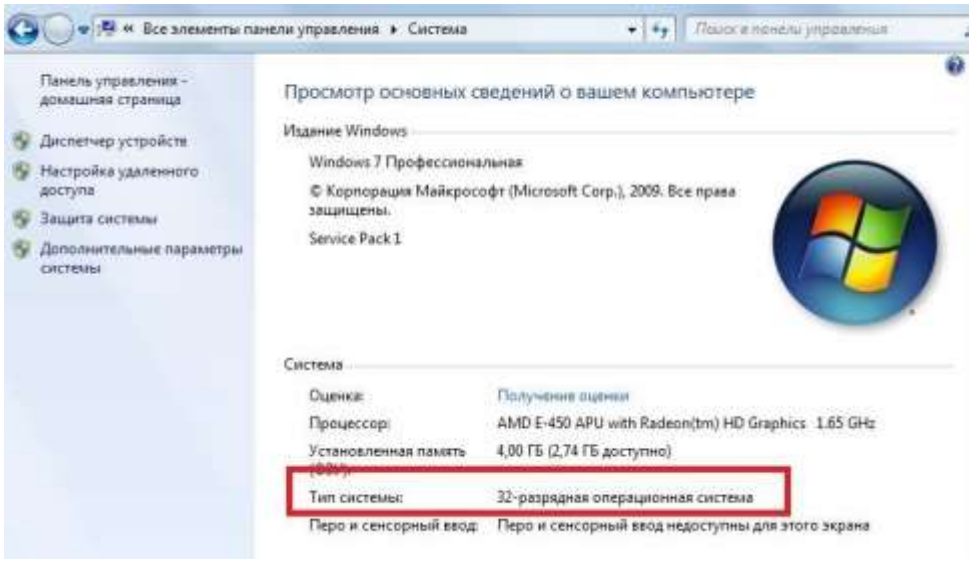
2.2.2) Запустите

- *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»

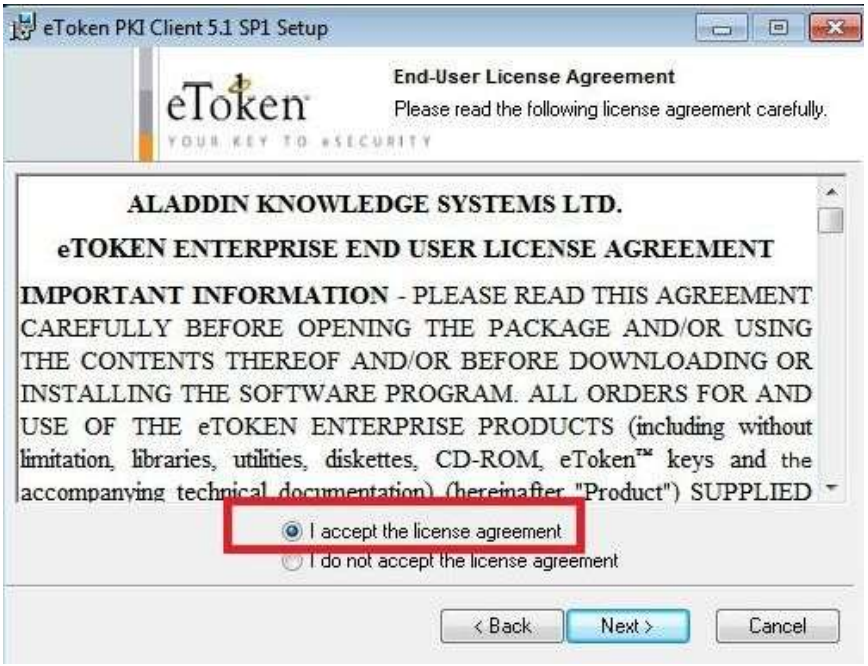




2.2.1) В открывшемся окне приветствия мастера установки нажмите кнопку «**Next**»:

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

2.2.3) Согласитесь с условиями лицензионного соглашение, 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 окончанию выйдет окно «eToken PKI Client 5.1 SP1 has been successfully installed», Нажимаете кнопку «**Finish**»

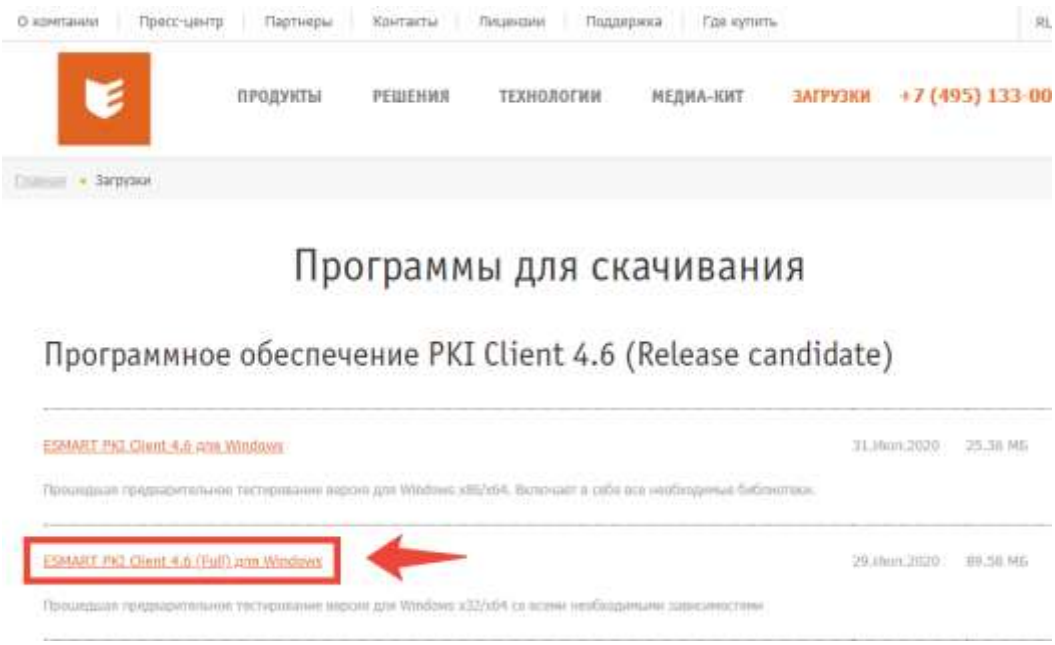
2.2.6) Выйдет окно с предложением перезагрузить компьютер

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

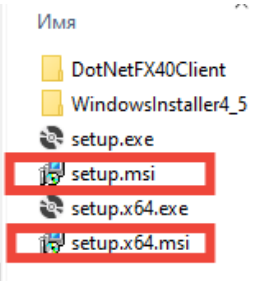
9) Вставьте в USB порт eToken.Windows должен определить его как новое устройство.

2.3 Установка драйвера ESMART

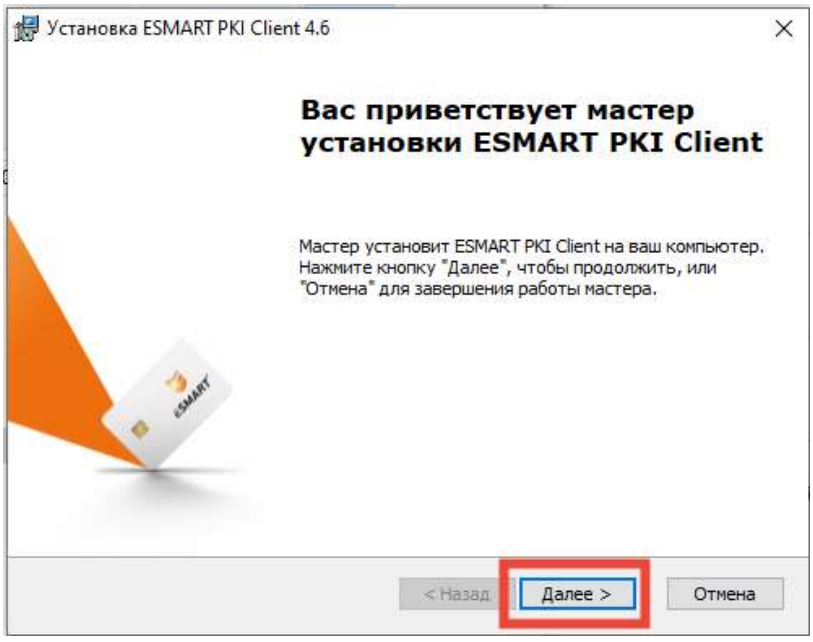
Откройте страницу https://esmart.ru/download/ и загрузите файл «*ESMART PKI Client 4.6 (Full) для Windows*».



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

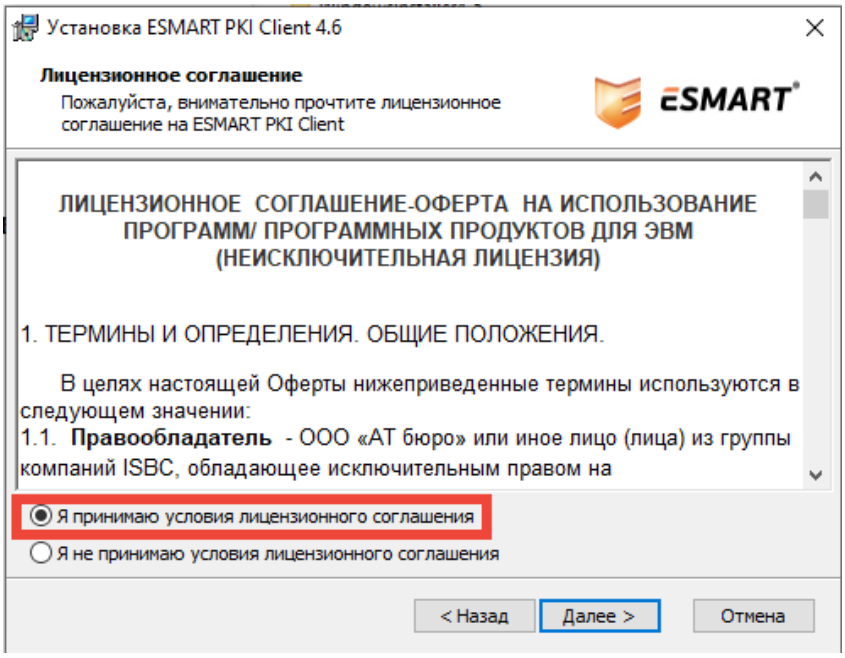


В открывшемся окне нажмите *Далее*

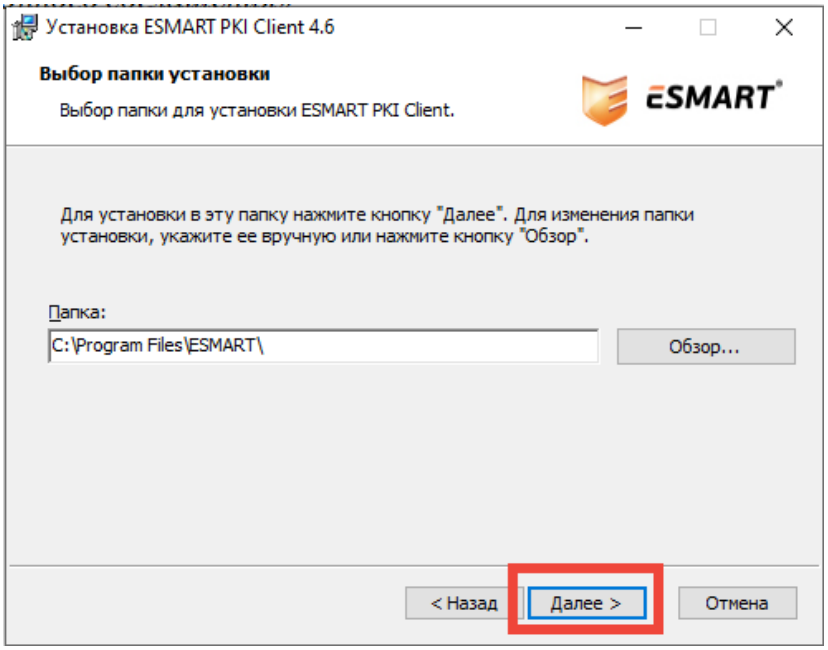


Поставьте перелючатель в положение *«Я принимаю условия*

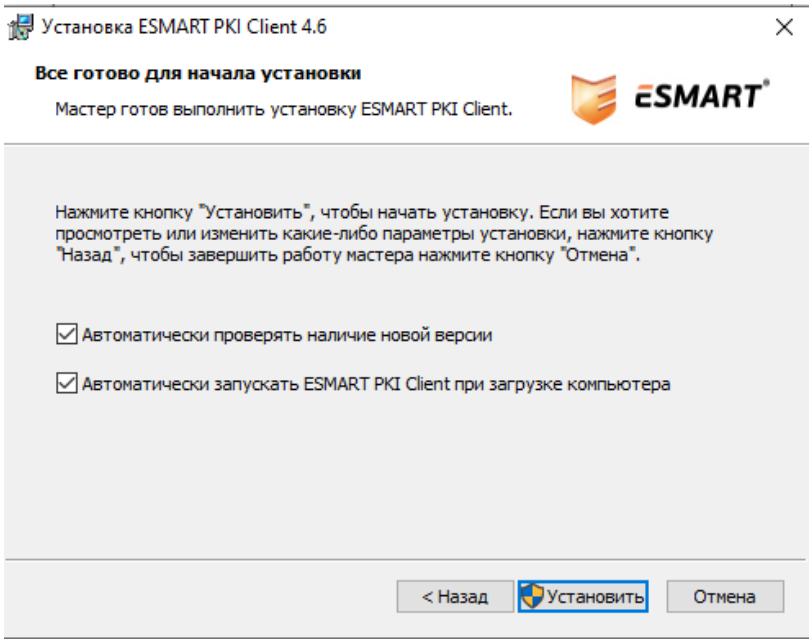
лицензионного соглашения»



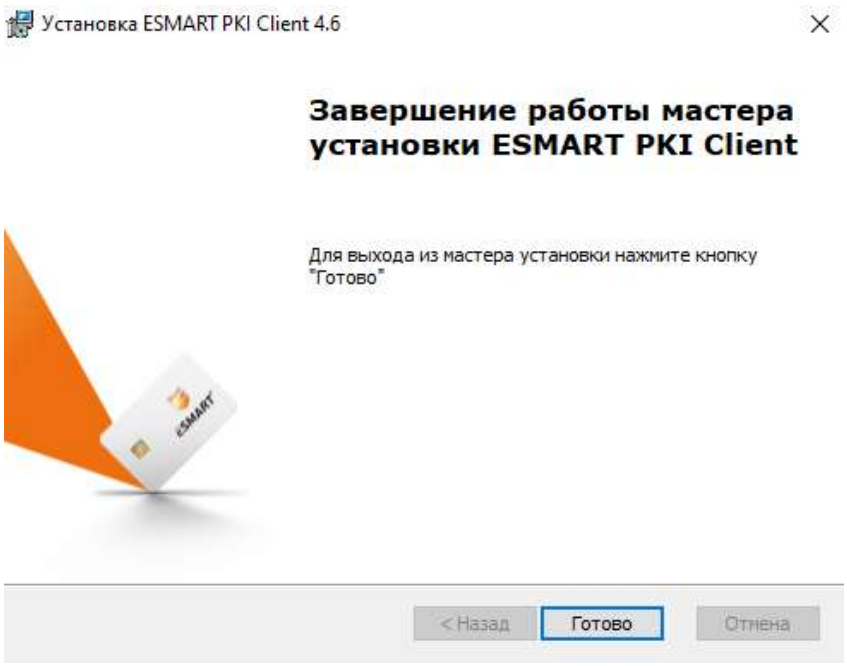
Папку установки оставьте по умолчанию



На следующем шаге поставьте все флаги и нажмите *Установить*



Дождитесь окончания установки и нажмите *Готово*



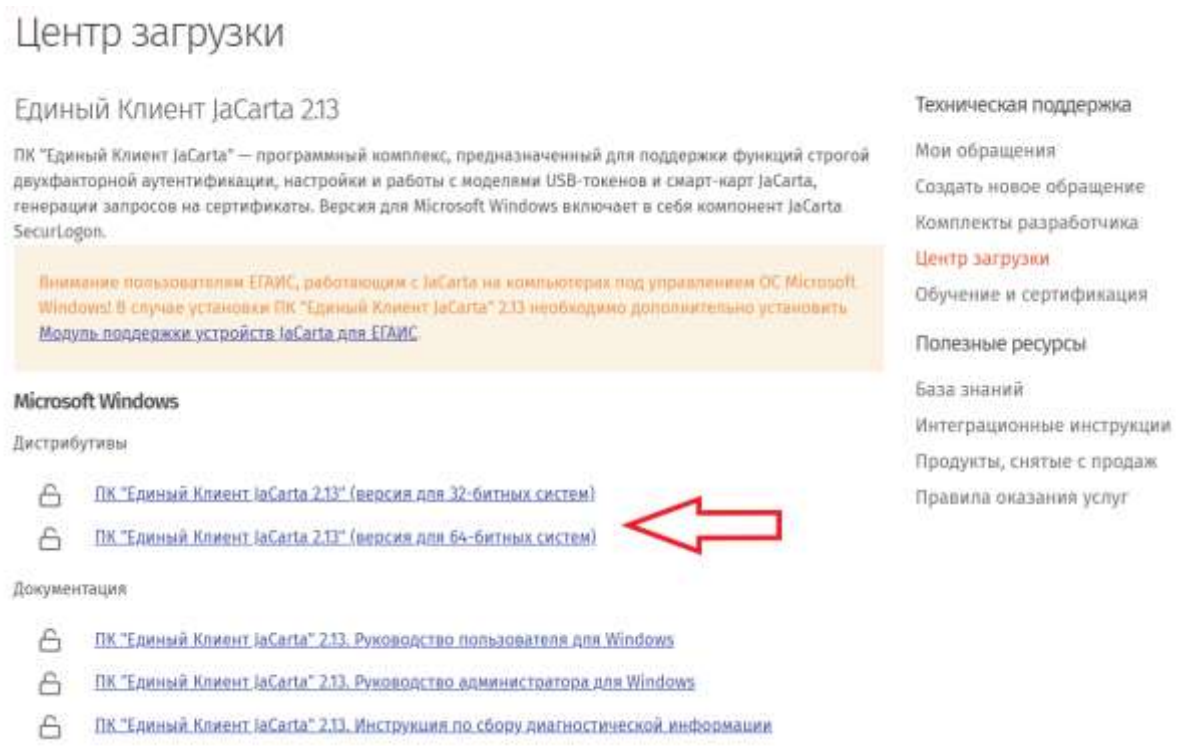
2.4 Установка драйвера Jacarta

Откройте страницу https://www.aladdin-rd.ru/support/downloads/jacarta_client и загрузите файл

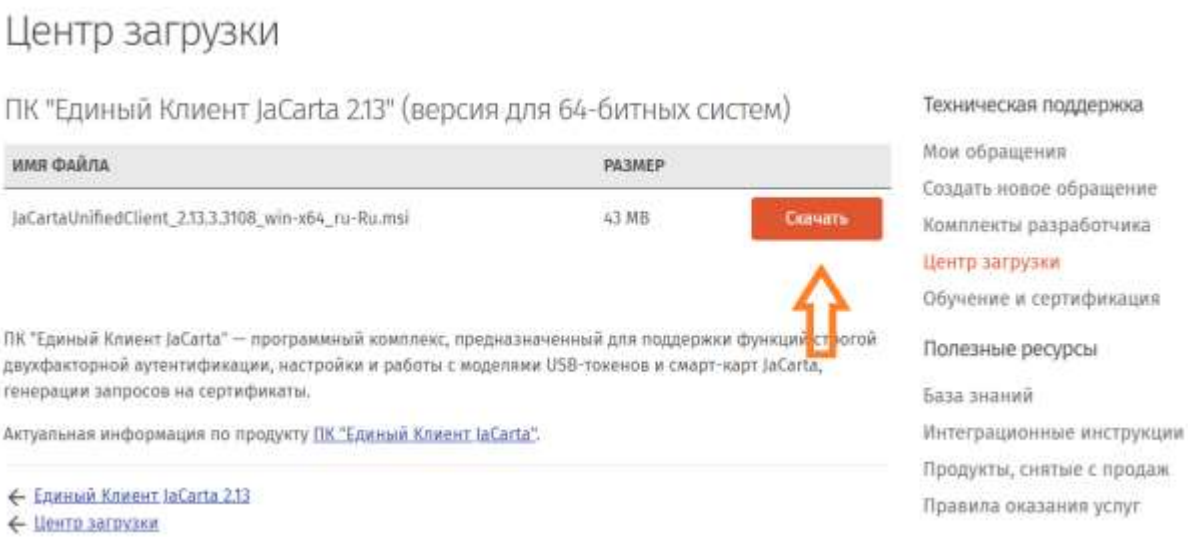
«*ПК "Единый Клиент JaCarta 2.13" (версия для 32-битных систем)*»

или

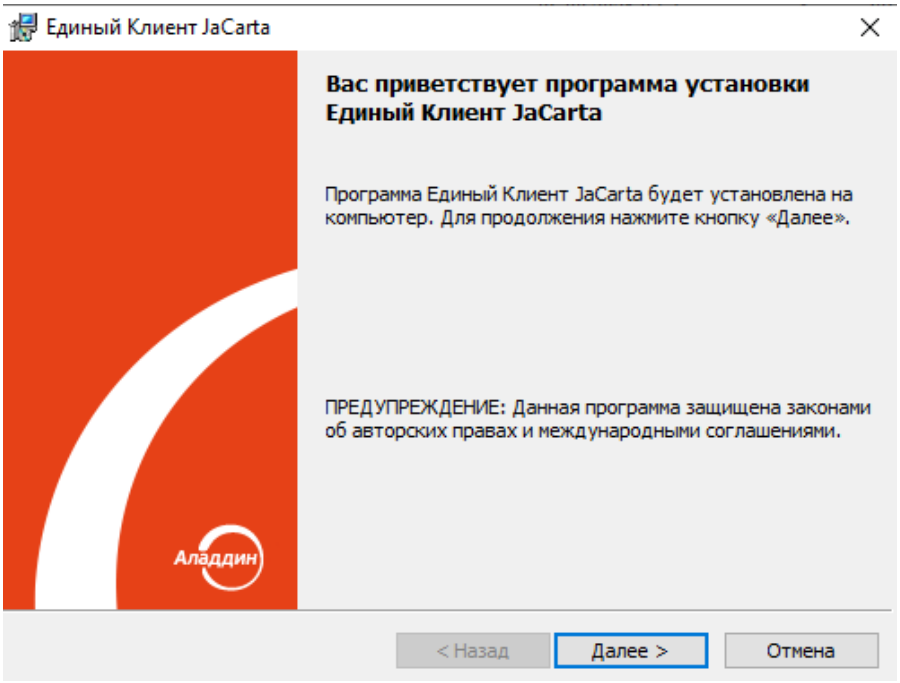
«*ПК "Единый Клиент JaCarta 2.13" (версия для 64-битных систем)*»



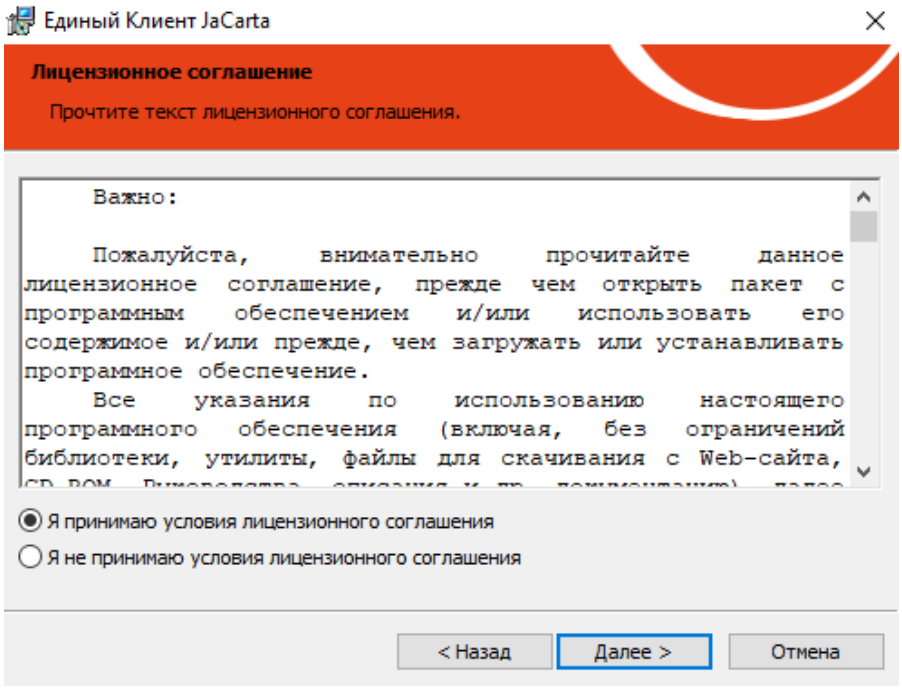
На следующей странице нажимаете кнопку «*Скачать*»



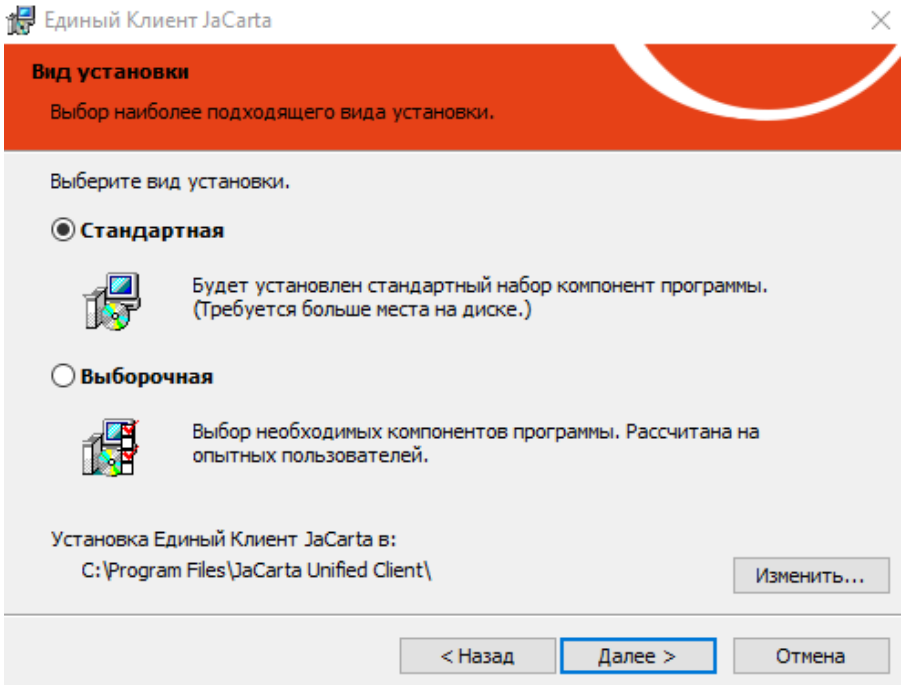
Запускаете загруженный файл и нажимаете «*Далее*»



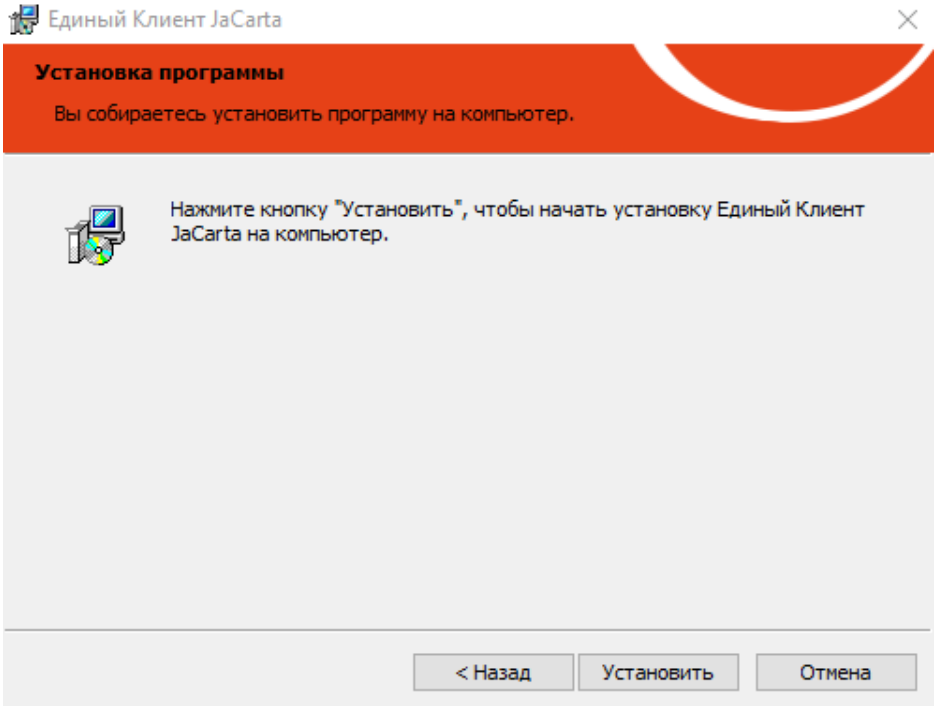
Принимаете условия лицензионного соглашения, нажимаете «*Далее*»



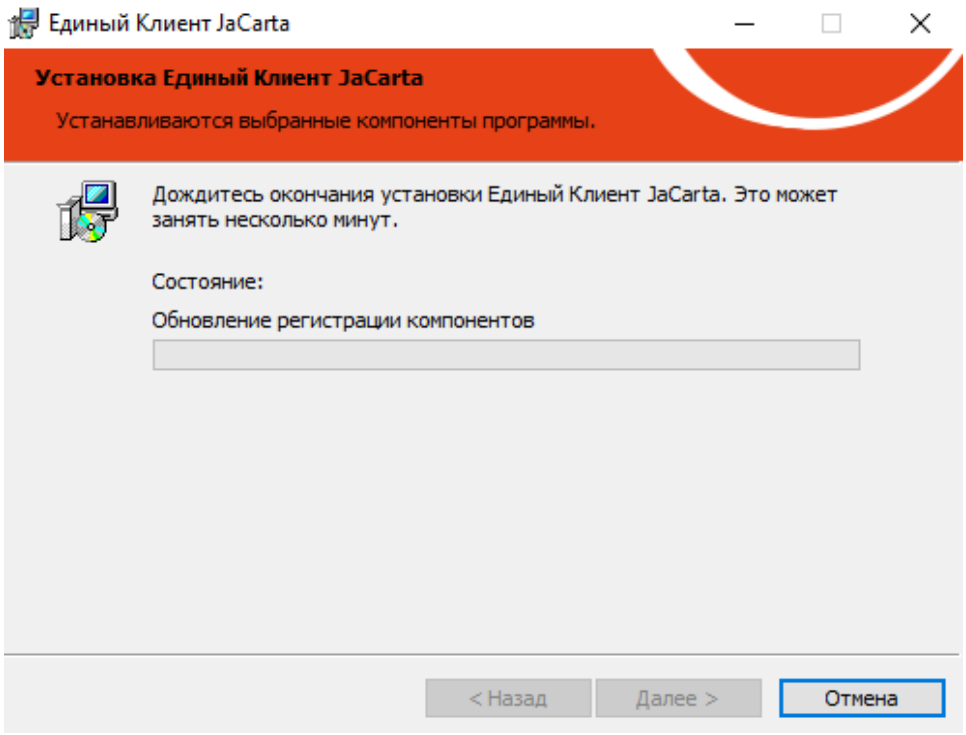
Выбираете стандартную установку, нажимаете «*Далее*»



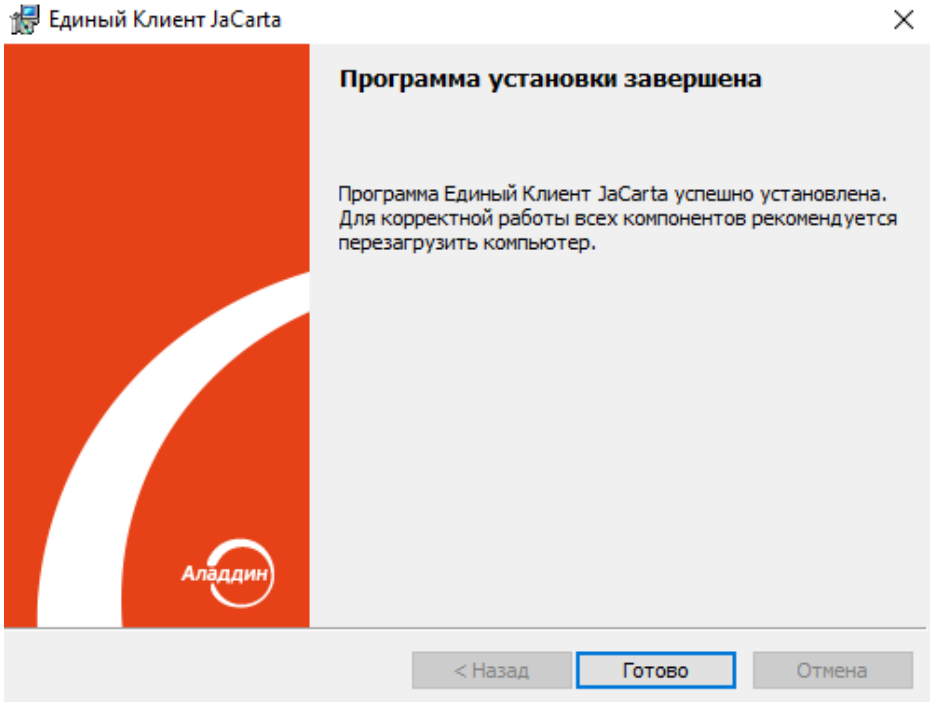
Нажимаете «*Установить*»



Дожидаетесь окончания установки



Нажимаете «*Готово*»



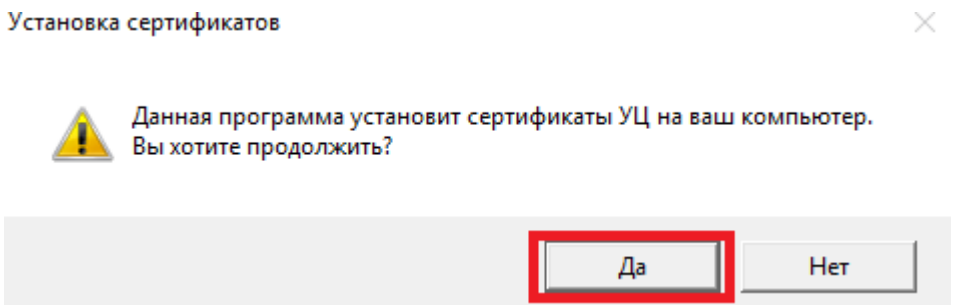
3. Загрузка и установка корневых сертификатов УЦ

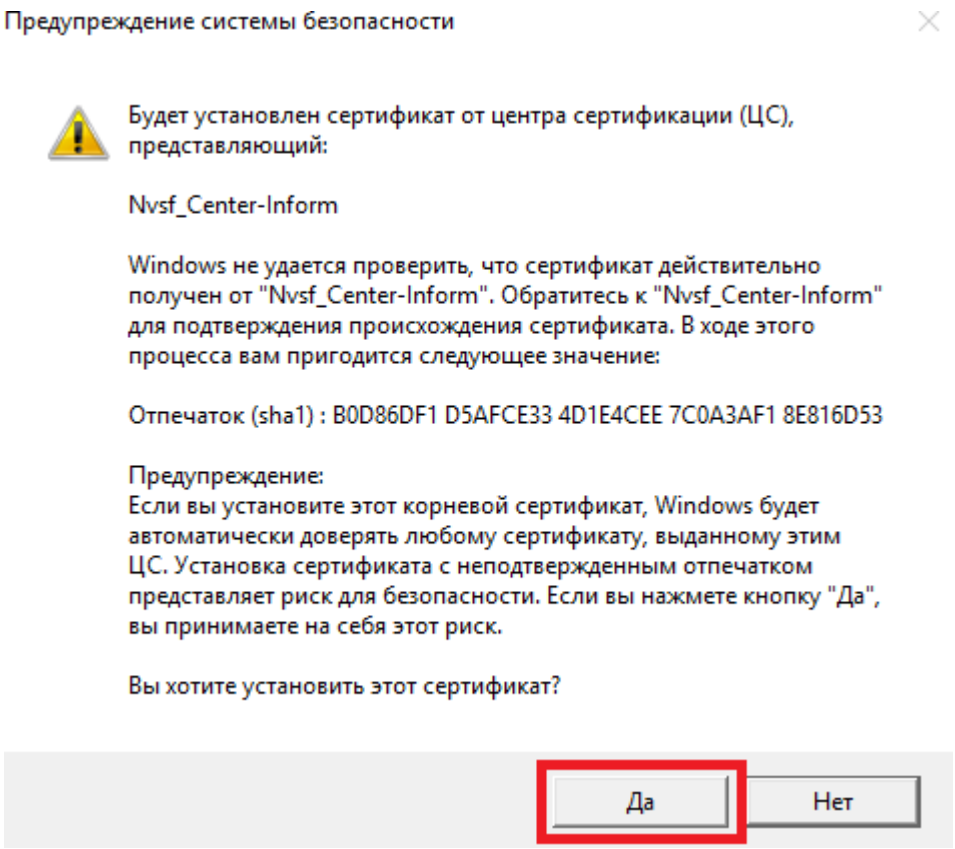
Важным элементом любых криптографических ключей является сертификат или набор сертификатов поставщика (УЦ), выпустивших эти ключи и содержащих сведения для идентификации поставщика и цифровую

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. Запустите и разрешите установку всех предложенных сертификатов.





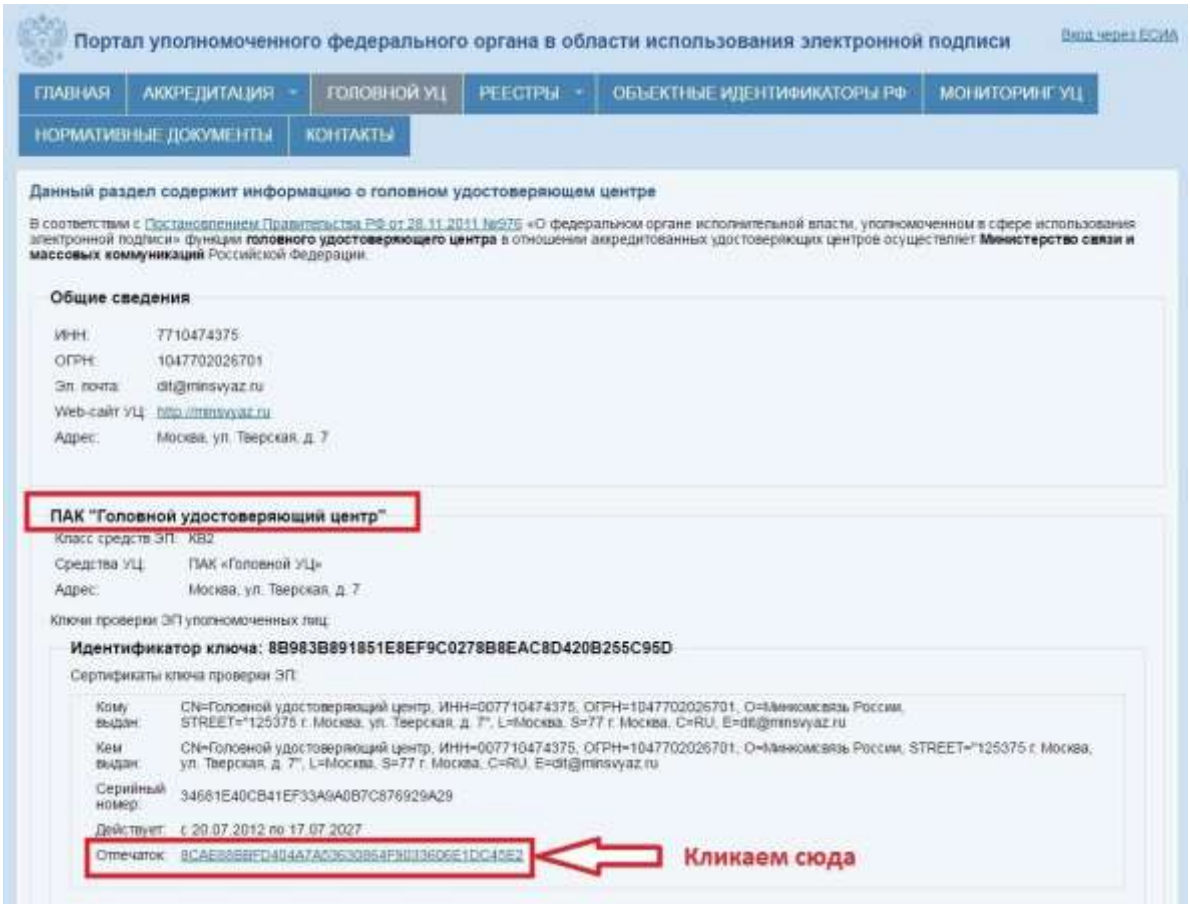
3.2 Ручная установка корневых сертификатов

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

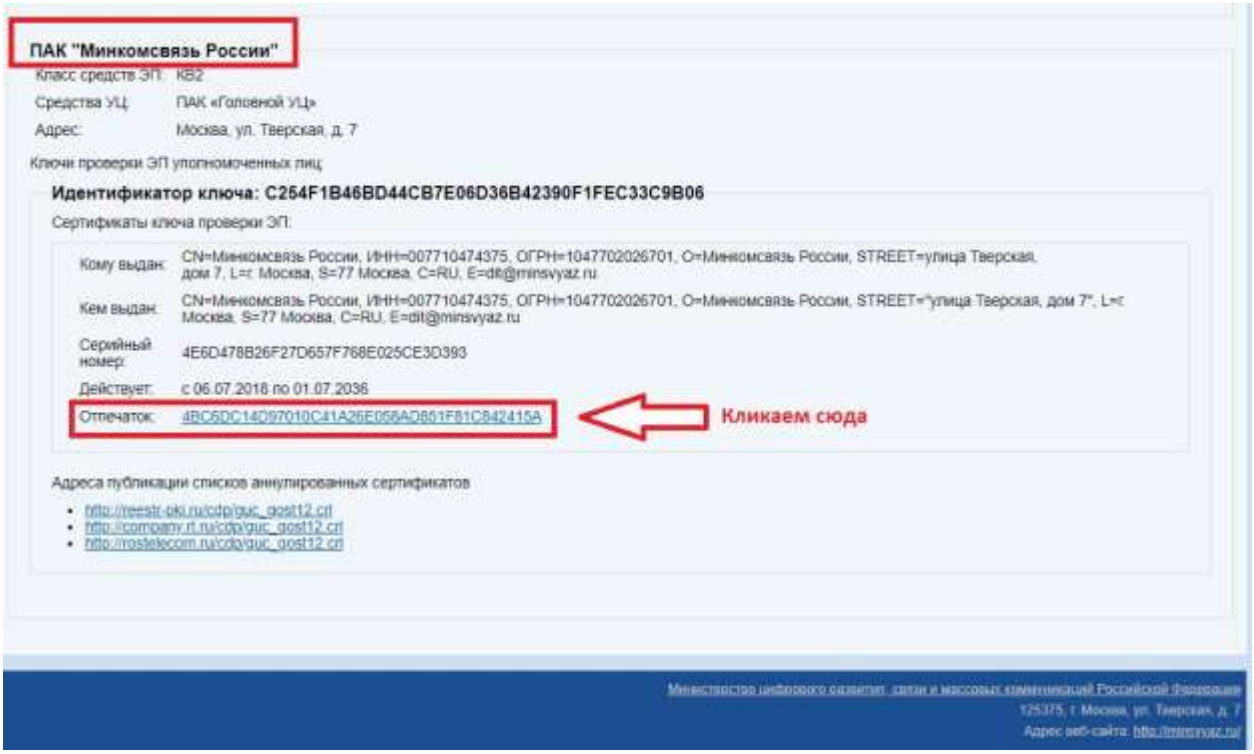
3.2.1 Установка в доверенные корневые центры сертификации

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

ПАК "Головной удостоверяющий центр" (действует с 20.07.2012 по 17.07.2027)

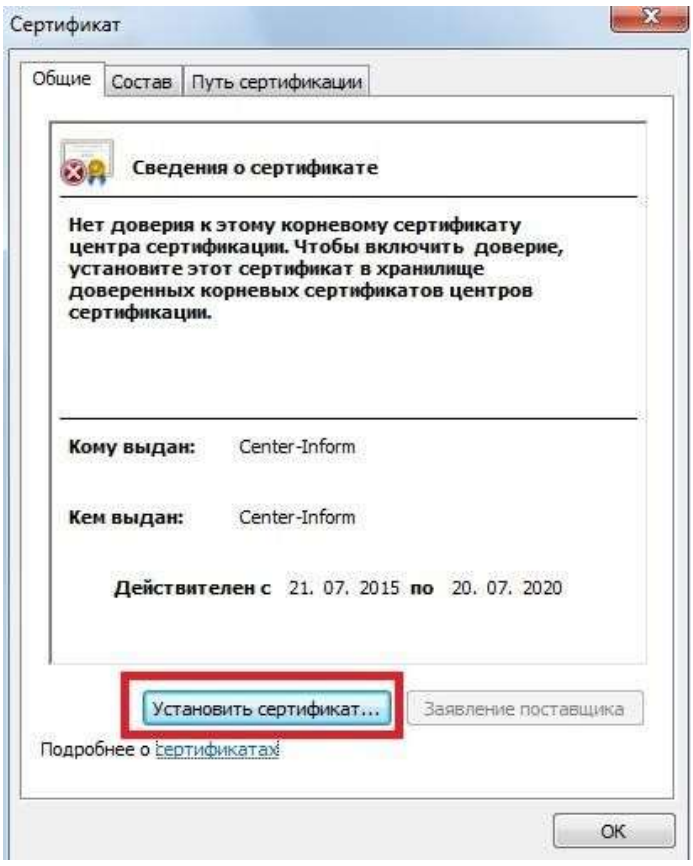


ПАК "Минкомсвязь России" (действует с 06.07.2018 по 01.07.2036)

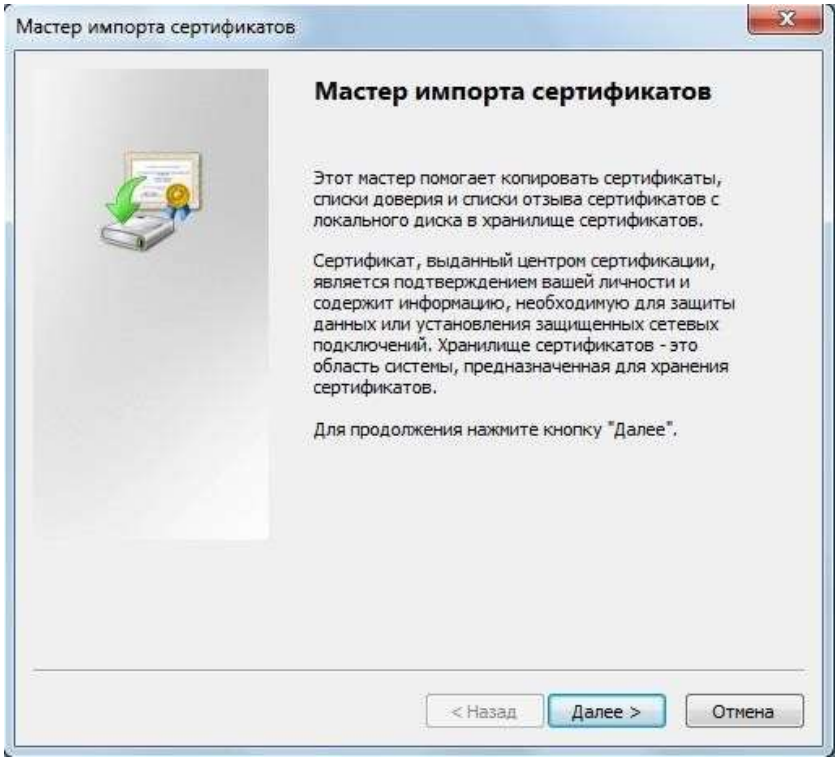


Поочередно установите сертификаты в доверенные корневые центры сертификации:

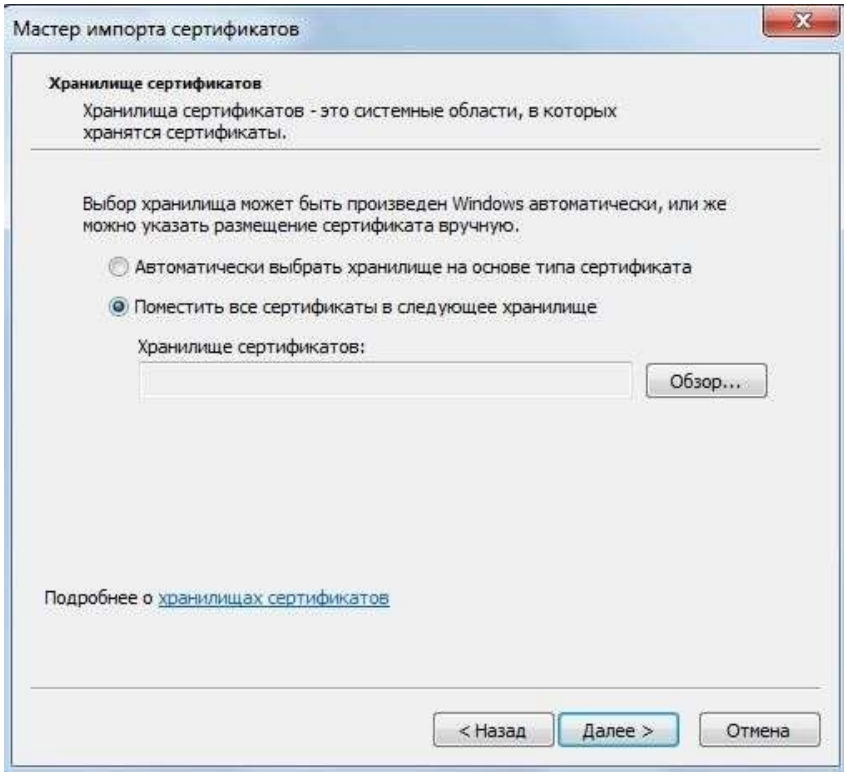
двойным щелчком мыши откройте скачанный файл и в открывшемся окне сертификата нажмите кнопку «**Установить сертификат**»:



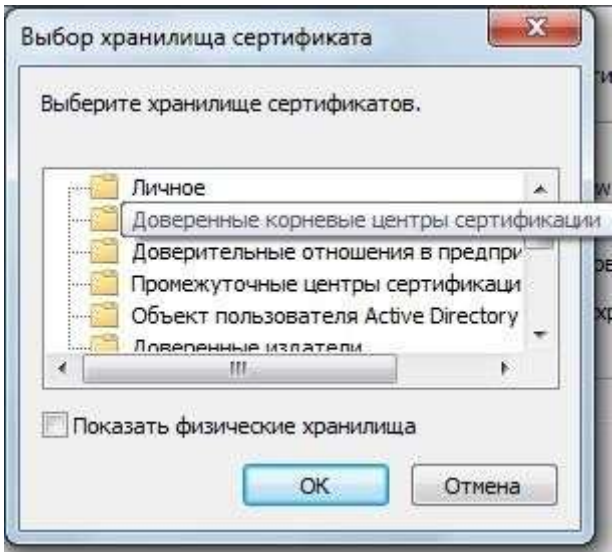
Откроется Мастер импорта сертификатов. Нажмите кнопку «**Далее**»:



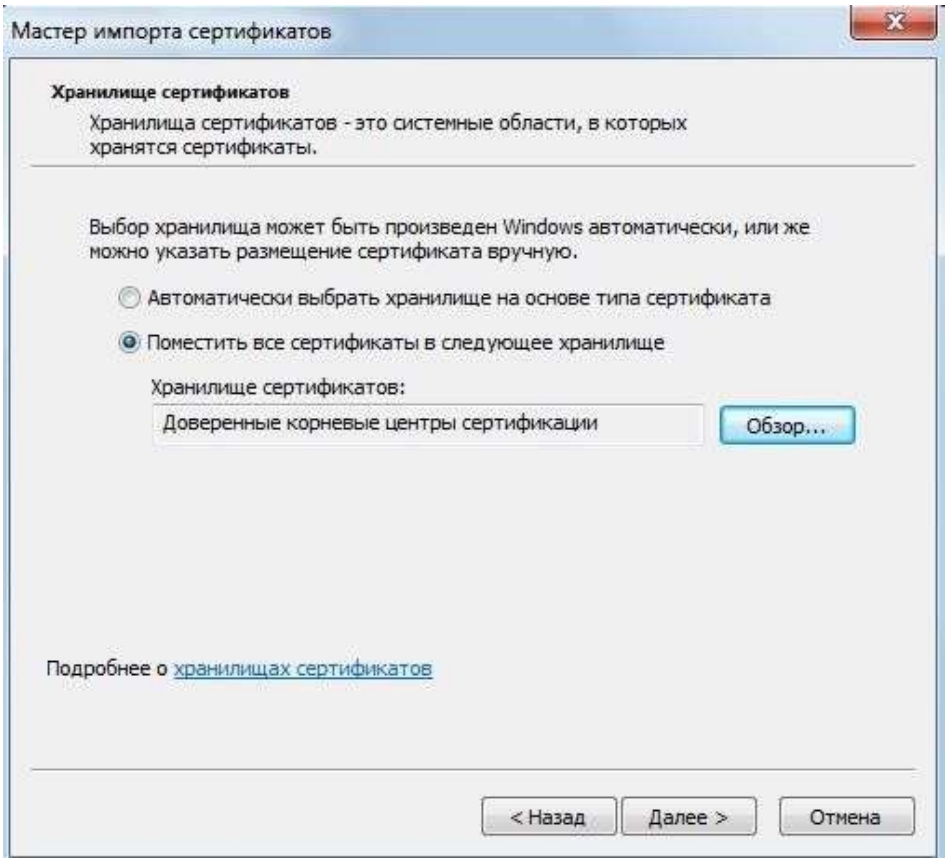
Выберите пункт «Поместить все сертификаты в следующее хранилище» и нажмите кнопку «**Обзор**».



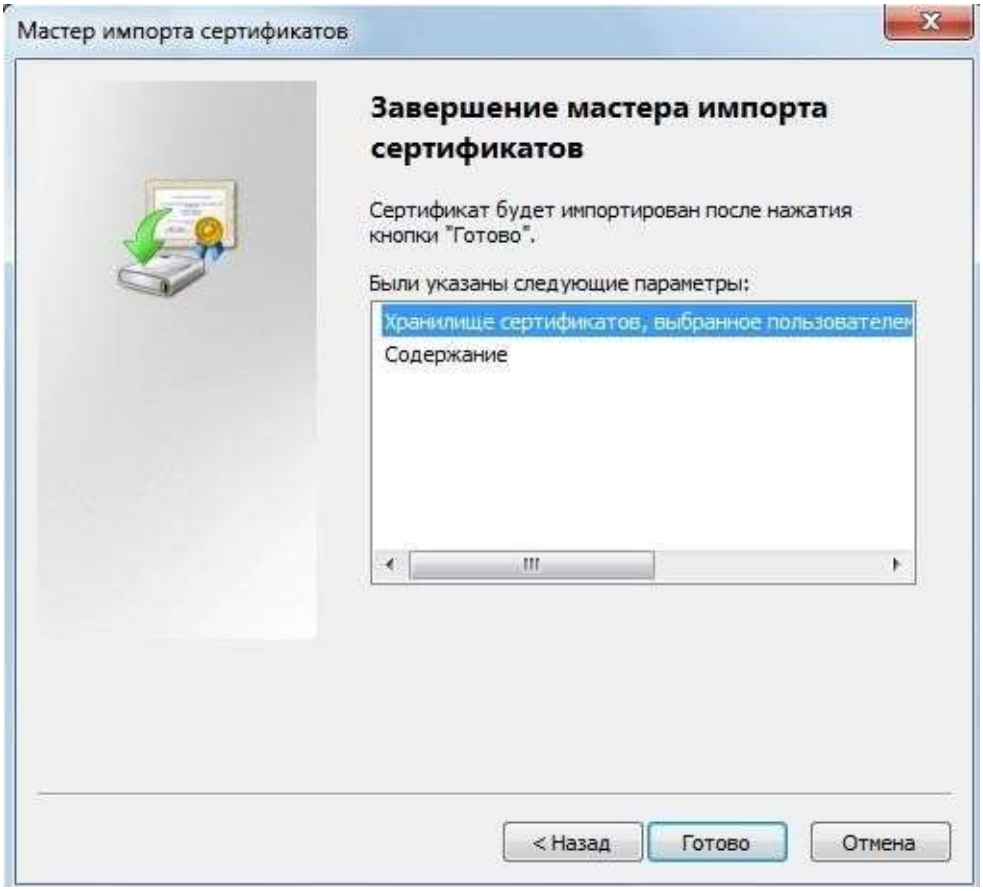
В окне «Выбор хранилища сертификата» выберите папку «**Доверенные корневые центры сертификации**» и нажмите кнопку «**ОК**»:



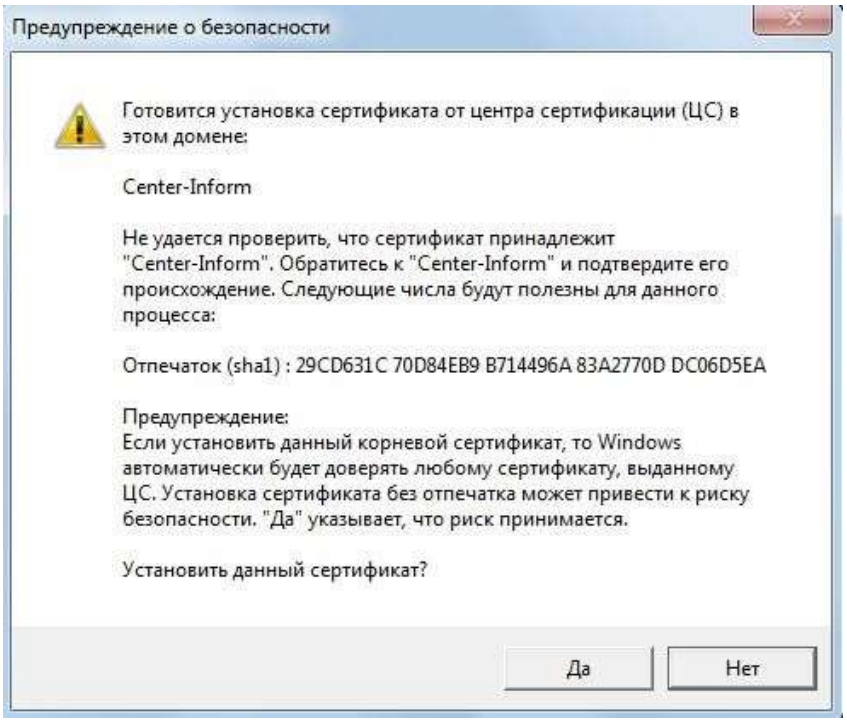
Указав хранилище сертификата, нажмите кнопку «**Далее**»:



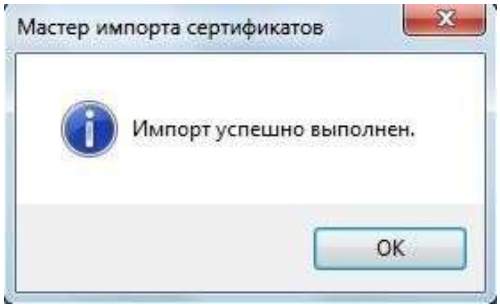
Для завершения установки сертификата нажмите кнопку «**Готово**»:



Появится «Предупреждение системы безопасности»:



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



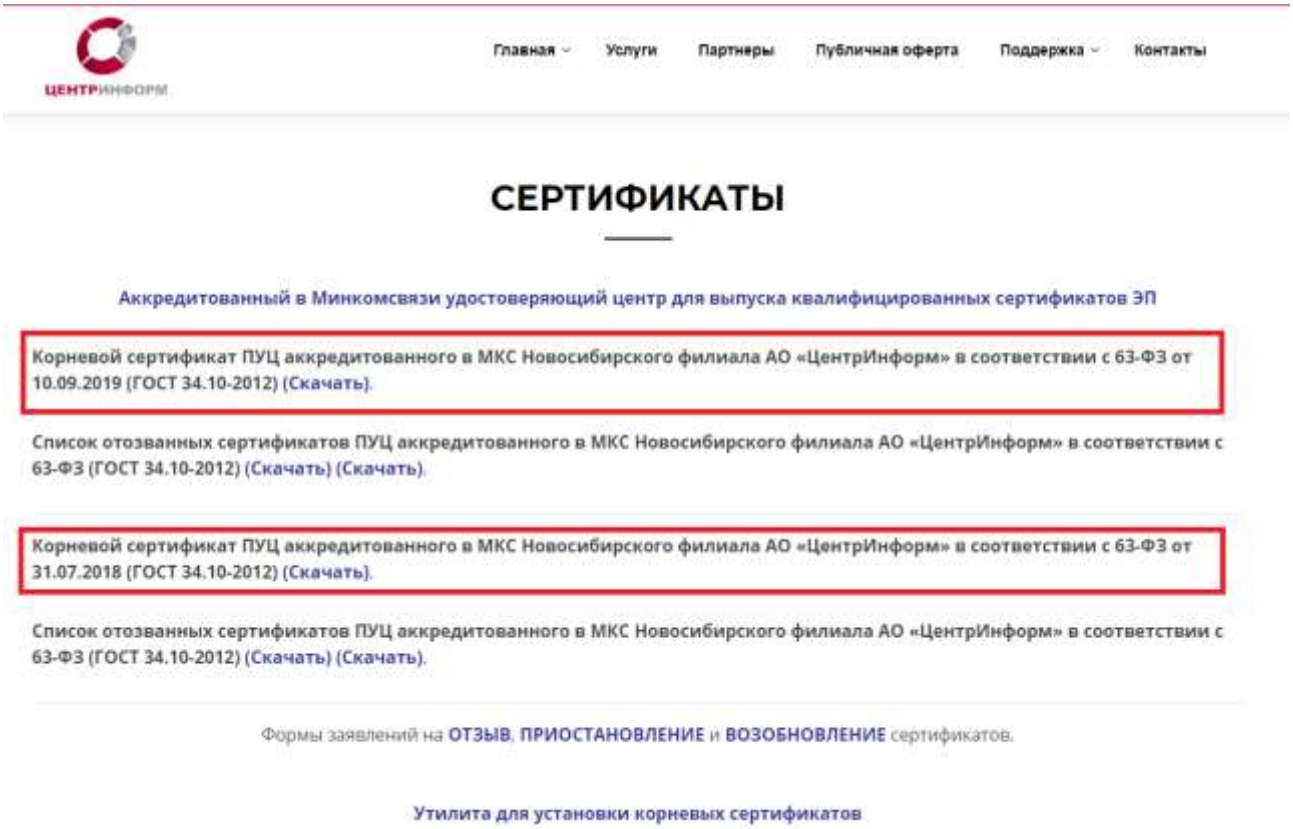
Нажатием кнопок «**ОК**» закройте окна сообщения и сертификата.

3.2.2 Установка в промежуточные центры сертификации

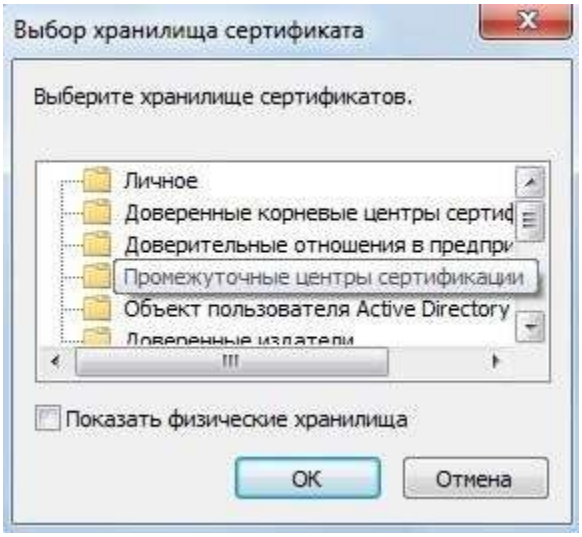
Скачайте со страницы http://www.ci54.ru/index.php?id=73 следующие сертификаты

- 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



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**»:



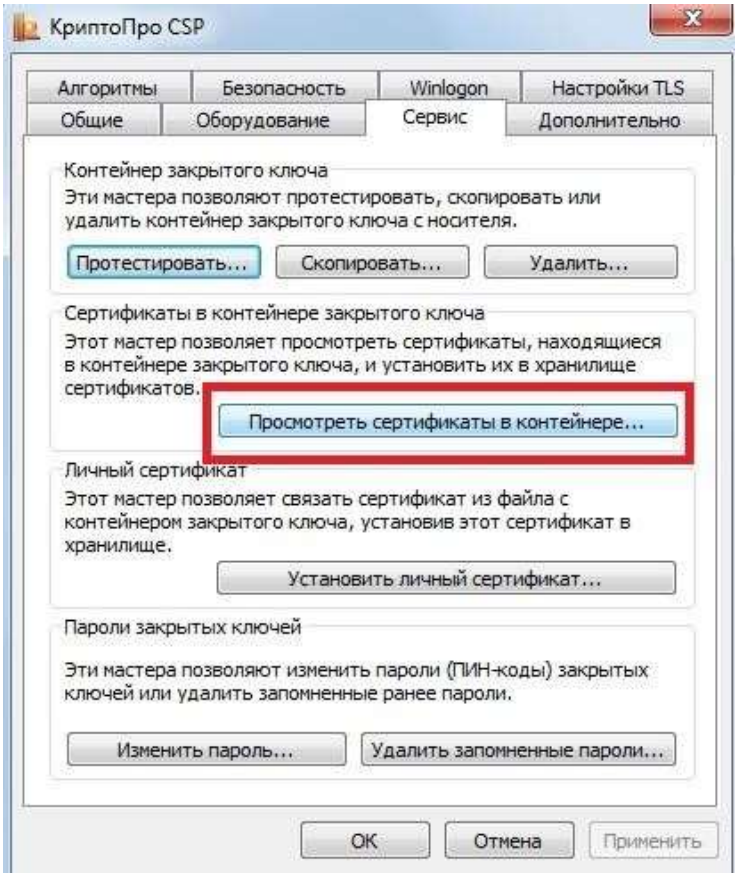
4. Установка Личного сертификата

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

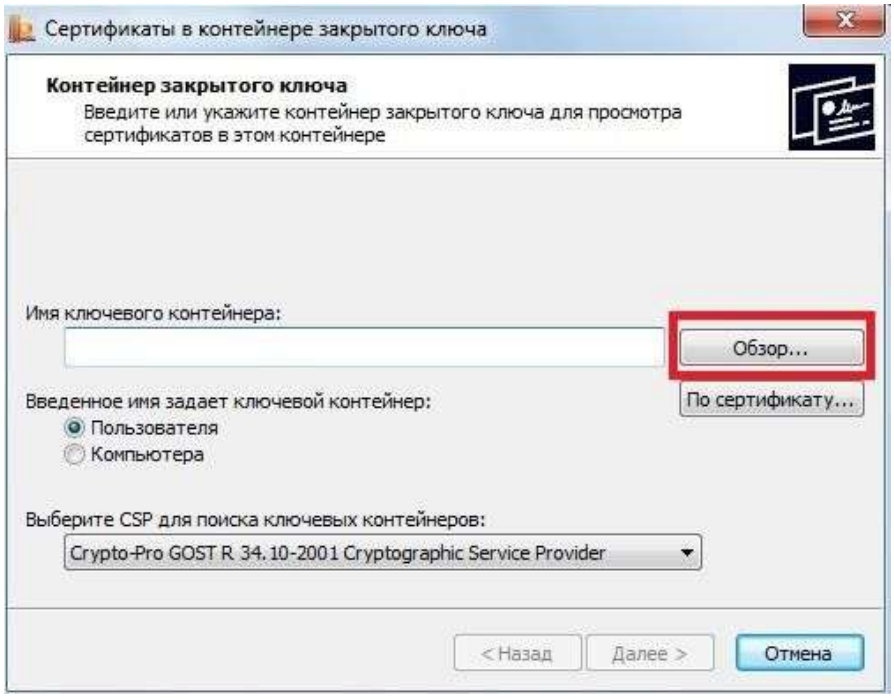
Установку Личного сертификата рекомендуем выполнять в приведенной ниже последовательности.

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

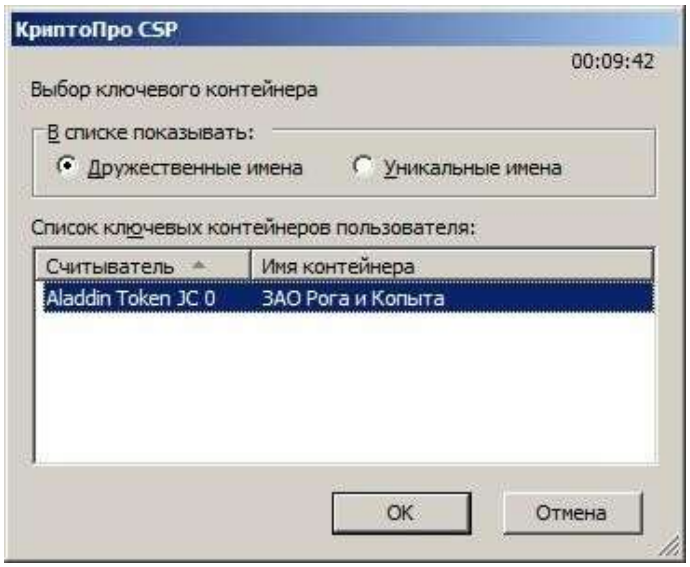
4.2) Запустите КриптоПро CSP (Панель управления -> **КриптоПро CSP**). В открывшемся окне управления свойствами КриптоПро CSP на вкладке «**Сервис**» нажмите кнопку «**Посмотреть сертификаты в контейнере**»:



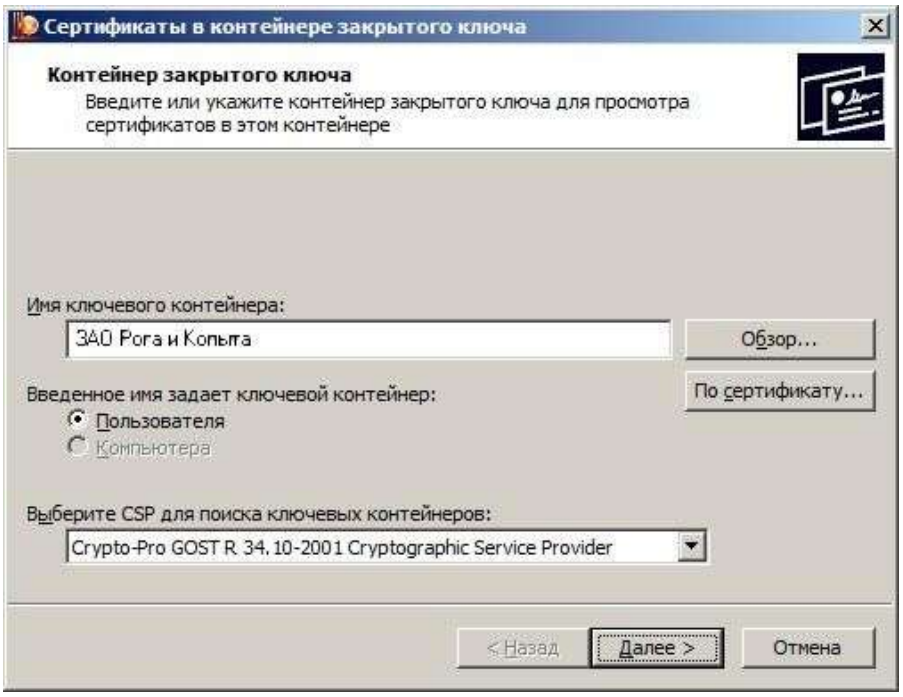
4.3) Откроется окно указания контейнера закрытого ключа:



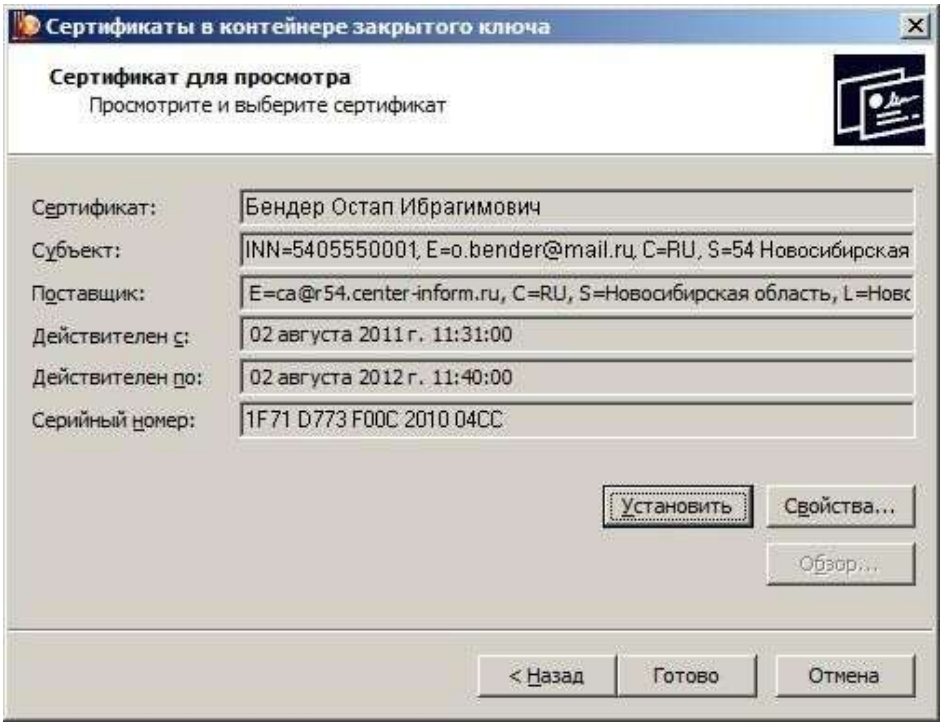
4.4) Нажатием кнопки «**Обзор**» отройте окно выбора ключевого контейнера. В списке обнаруженных ключевых контейнеров укажите контейнер вашей ЭП и нажмите кнопку «**ОК**».



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

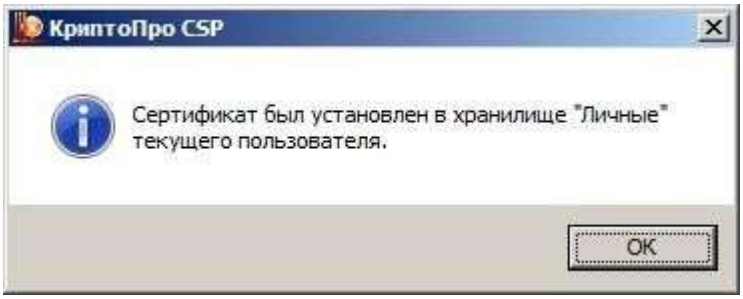


4.6) Откроется окно просмотра и установки сертификата:

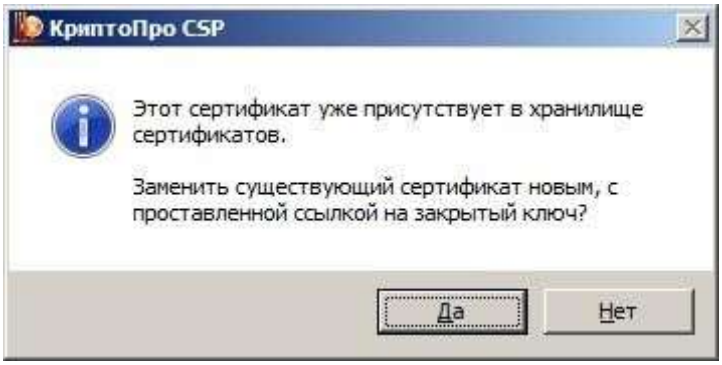


Примечание: Полную информацию о сертификате можно получить нажатием кнопки «**Свойства**».

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!