# 

# ИНСТРУКЦИЯ по подготовке рабочего места для использования ЭП

Для подготовки Вашего ПК к использованию электронной цифровой подписи (ЭП), выпущенной Удостоверяющим центром ООО «РУЦ», необходимо выполнить следующие установки и настройки:

1. [Установить КриптоПро CSP](#_Установка_КриптоПро_CSP)
2. [Установить КриптоПро ЭЦП Browser plug-in](#_Установка_КриптоПро_ЭЦП_1)
3. [Установить драйвер ключевого носителя Rutoken](#_Установка_драйвера_Rutoken)
4. [Установить корневые сертификаты Удостоверяющего центра](#_Установка_корневых_сертификатов)
5. [Установить Личный сертификат](#_Установка_личного_сертификата)
6. [Настроить браузер Internet Explorer](#Настройка_безопасности_IE)

**ВНИМАНИЕ! ПЕРЕД УСТАНОВКОЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НЕОБХОДИМО УБЕДИТЬСЯ В ОТСУТСТВИИ ВИРУСОВ НА КОМПЬЮТЕРЕ, А ТАКЖЕ ОБЕСПЕЧИТЬ АНТИВИРУСНУЮ ЗАЩИТУ ВАШЕГО ПК, ИНАЧЕ РАБОТА С ЭП НЕ ГАРАНТИРУЕТСЯ.**

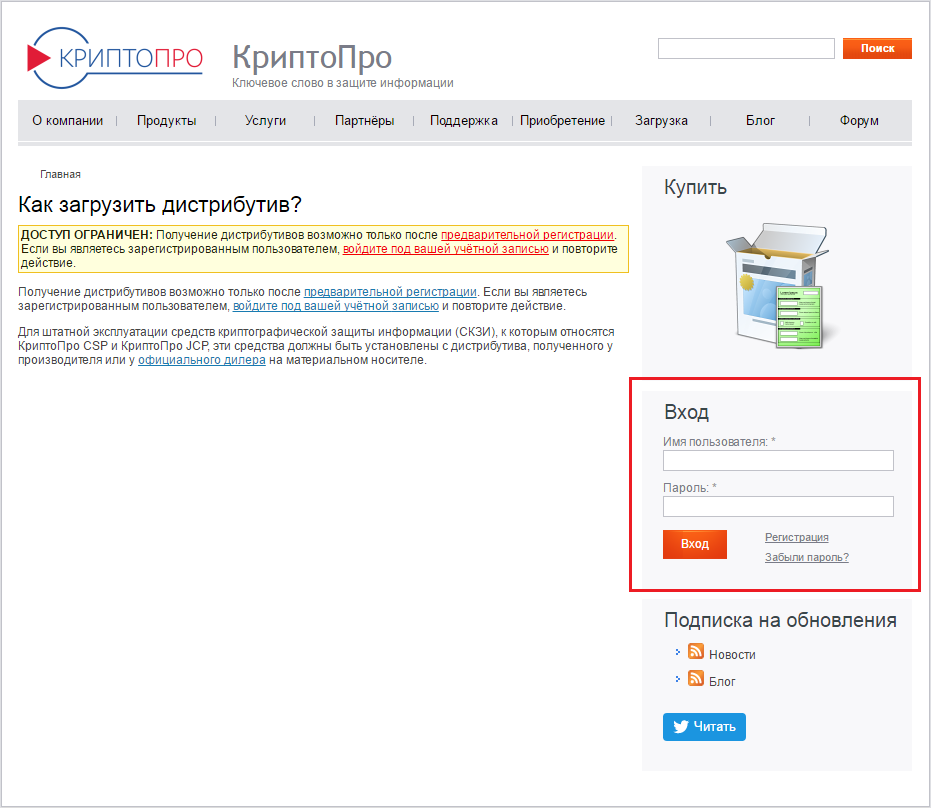
## Установка КриптоПро CSP

**КриптоПро CSP** — криптопровайдер — средство криптографической защиты информации (СКЗИ).

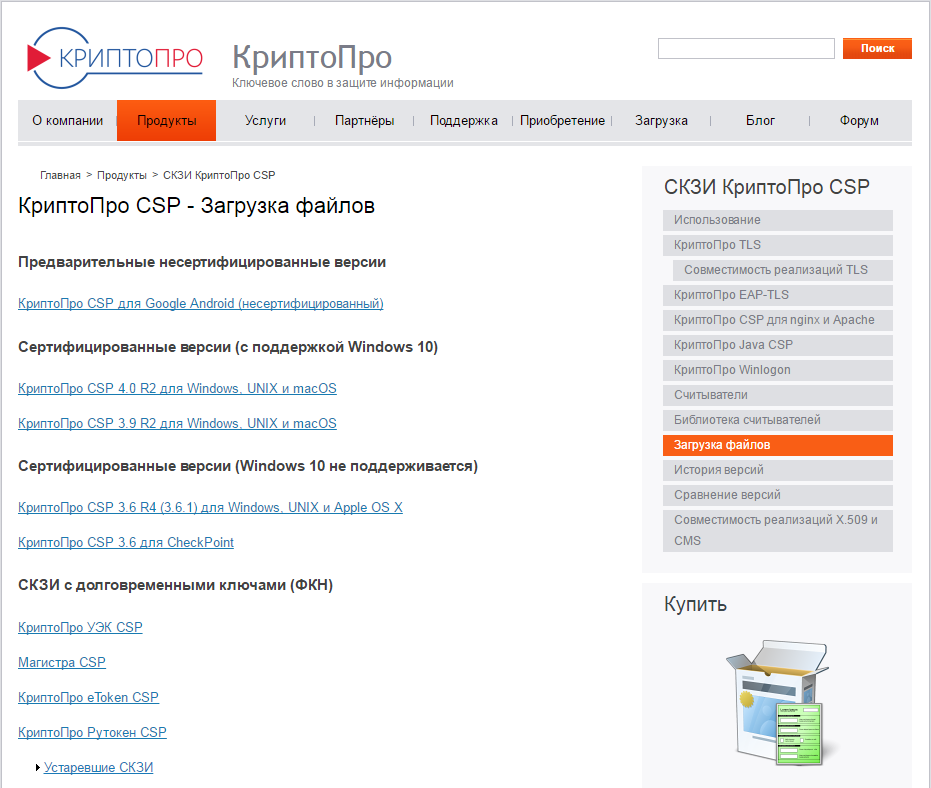
Утилита КриптоПро CSP разработана по согласованному с ФАПСИ техническому заданию в соответствии с криптографическим интерфейсом фирмы Microsoft (Cryptographic Service Provider — CSP) и используется для формирования ключей шифрования и ключей ЭП, шифрования и имитозащиты данных, обеспечения целостности и подлинности информации, не содержащей сведений, составляющих государственную тайну. КриптоПро CSP имеет сертификаты соответствия ФАПСИ.

Дистрибутив КриптоПро CSP необходимо загрузить с официального сайта КриптоПро: <http://cryptopro.ru/downloads/howto?destination=node%2F148>. Установка дистрибутива СКЗИ КриптоПро CSP должна производиться пользователем, имеющим права администратора.

Чтобы дистрибутивы стали доступны для скачивания в разделе «Загрузки», нужно пройти предварительную регистрацию и авторизоваться по логину/паролю.

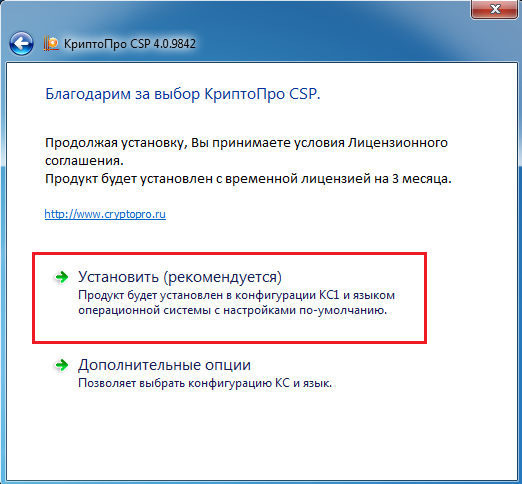


После регистрации появится страница с лицензионным соглашением. Ознакомившись с правилами и условиями нажимаем внизу экрана «Я согласен» для перехода в раздел загрузки дистрибутивов. Далее необходимо скачать и установить версию КриптоПРО CSP согласно приобретенной лицензии (версия лицензии указана на бланке). Лицензии на право использования программного обеспечения оформляются на бумажном носителе формата А4.

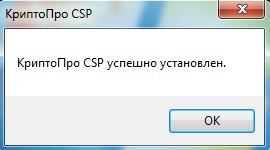


Последовательность установки КриптоПро CSP:

* Запускаем установочный файл **cspsetup.exe** и в появившемся окне программы установки нажимаем «Установить».

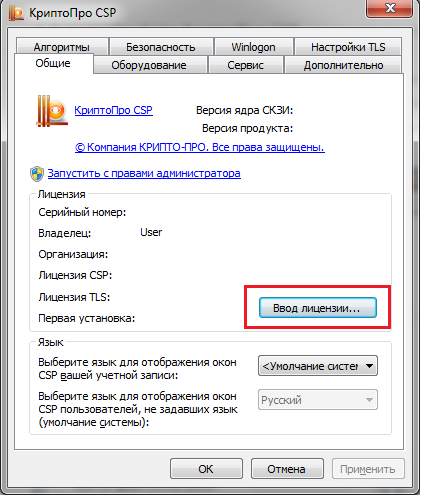


* Инсталляция программы проходит автоматически в течение нескольких минут и не требует участия пользователя.
* По окончанию процесса установки на экране появляется сообщение «КриптоПро CSP успешно установлен». Нажимаем «ОК».

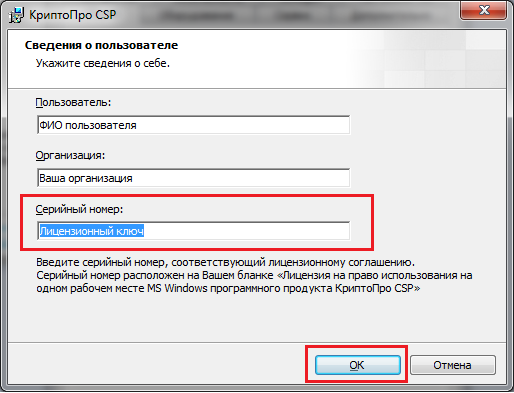


По условиям лицензионного соглашения срок использования демонстрационной версии КриптоПро CSP ограничен 90 днями с момента установки программы. Примечание: демонстрационный период предоставляется лишь при первой установке программы на компьютере.

Для активации лицензии на право использования программного продукта КриптоПро CSP необходимо запустить программу КриптоПро CSP («Пуск» -> «Панель управления» -> «КриптоПро CSP») и в окне «Общие» нажать «Ввод лицензии».



В открывшемся окне заполняем поля, в соответствии с приобретенной лицензией и нажимаем «ОК».



## Установка КриптоПро ЭЦП Browser plug-in

Плагин загружается с официального сайта КриптоПро: <http://www.cryptopro.ru/products/cades/plugin/get_2_0> и устанавливается путем двойного клика по скаченному файлу. Во время установки все время нажимаем «Далее».

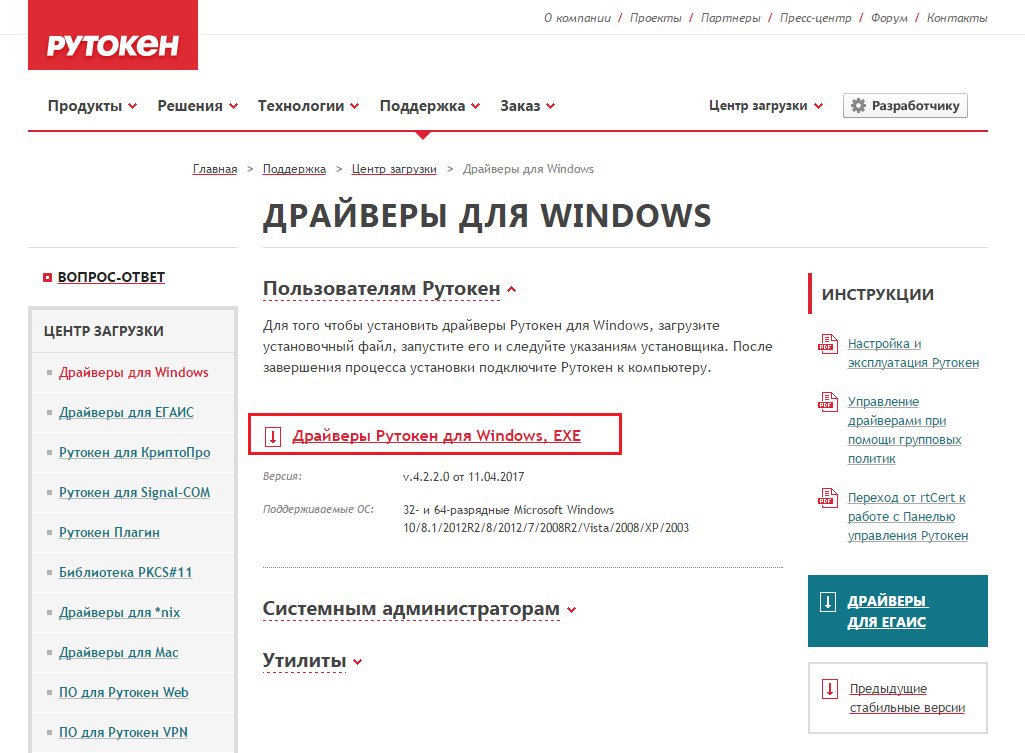
## Установка драйвера ключевого носителя Rutoken

Ключевой носитель Rutoken обеспечивает безопасную двухфакторную аутентификацию пользователей, защищенное хранение ключей шифрования и ключей электронной подписи, а также цифровых сертификатов и иной информации.

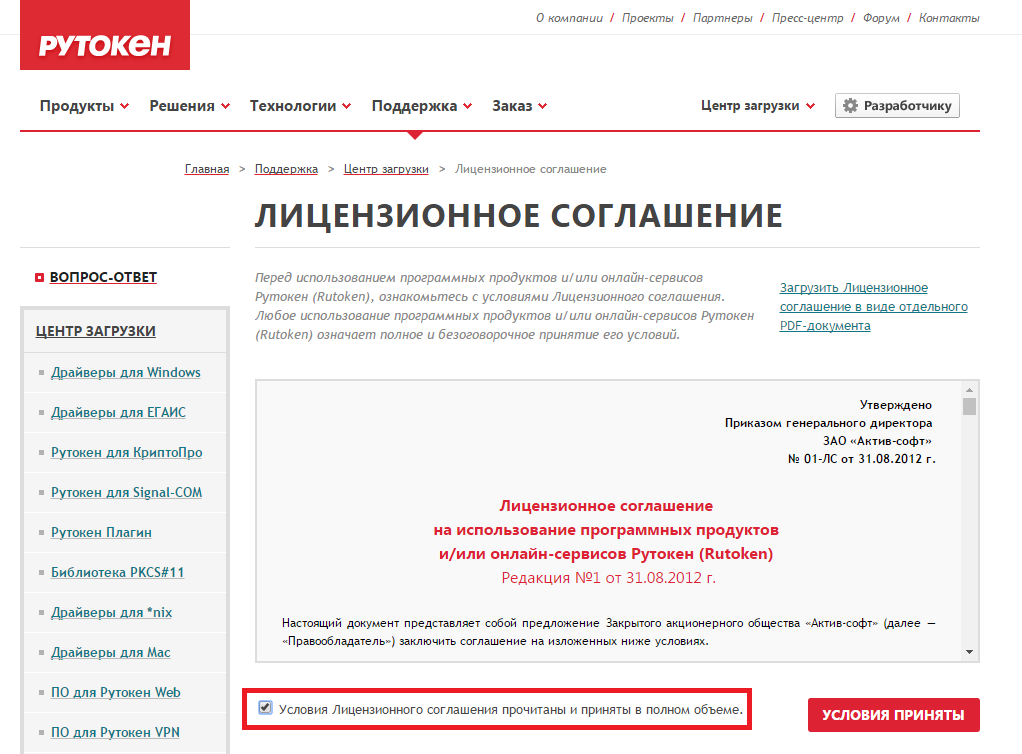
Вставляем ключевой носитель Rutoken в разъем USB и устанавливаем драйвер Rutoken, который необходимо загрузить с официального сайта: <http://www.rutoken.ru/support/download/drivers-for-windows/>

Последовательность установки драйвера:

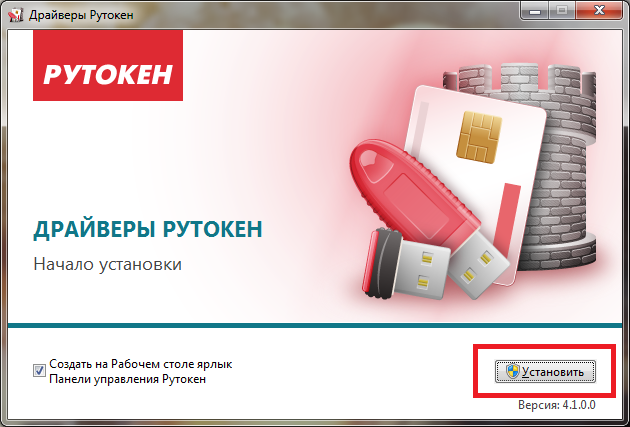
* На странице <http://www.rutoken.ru/support/download/drivers-for-windows/> нажимаем на ссылку «Драйверы Рутокен для Windows».



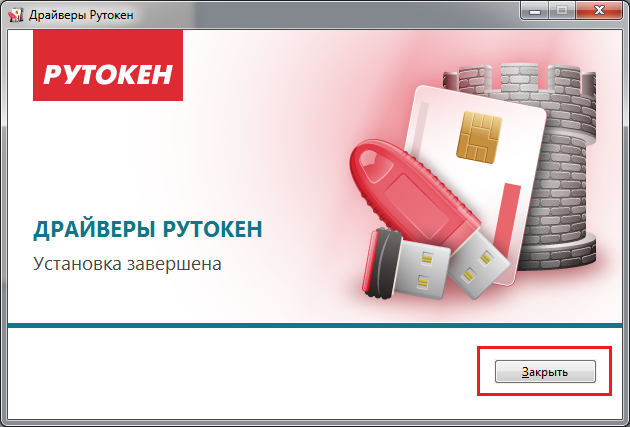
* Далее устанавливаем флаг, что принимаем условия лицензионного соглашения в полном объеме и нажимаем кнопку «Условия приняты». После этого происходит загрузка установочного файла.



* Запускаем установочный файл **rtDrivers.exe** и в появившемся окне программы установки нажимаем «Установить». Во время установки все время нажимаем «Далее».



* Дождитесь окончания установки и нажмите на кнопку «Закрыть».

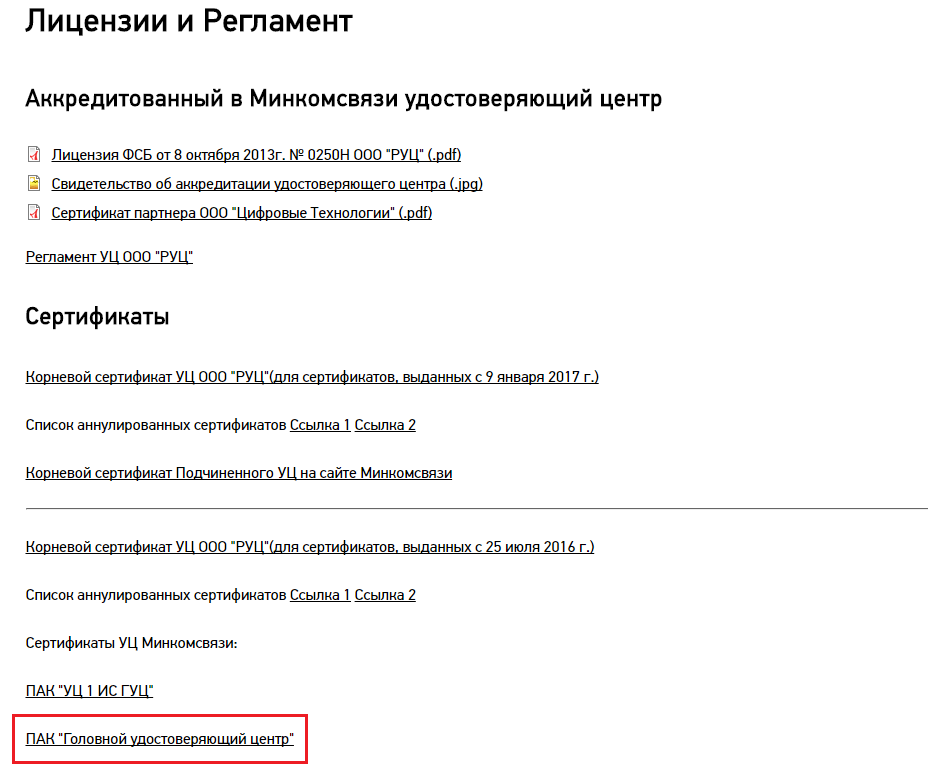


## Установка корневых сертификатов УЦ

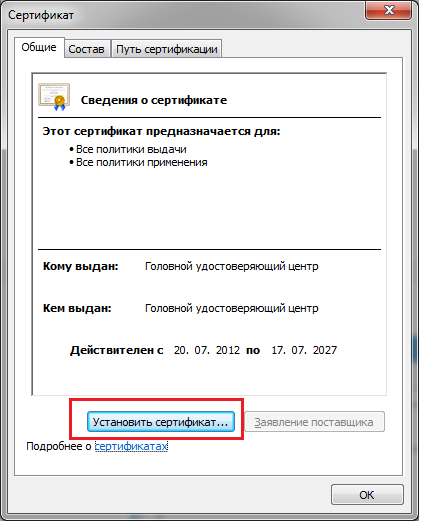
Для подтверждения подлинности личного сертификата, необходимо установить сертификаты Удостоверяющего центра.

**Загрузка и установка корневого сертификата «Головной удостоверяющий центр»:**

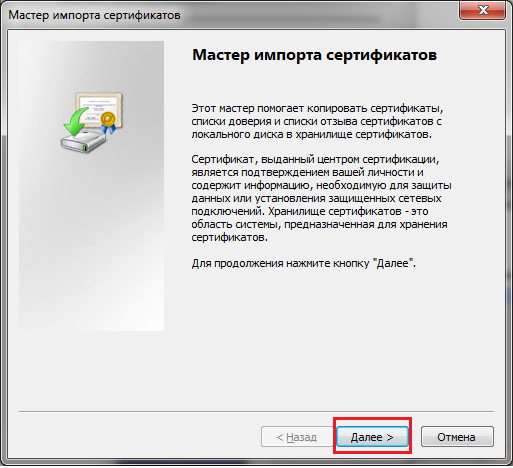
* Загрузить файл «Головной удостоверяющий центр.cer» можно с сайта УЦ: <http://www.rcarus.ru/licenzii-i-reglament>

****

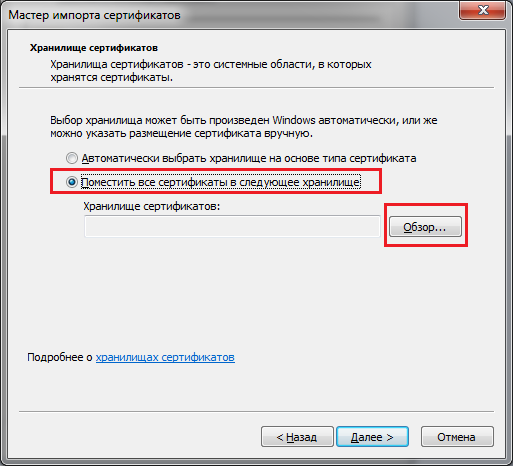
* Или по прямой ссылке: <https://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=8CAE88BBFD404A7A53630864F9033606E1DC45E2>
* В открывшемся окне сертификата нажимаем кнопку «Установить сертификат».



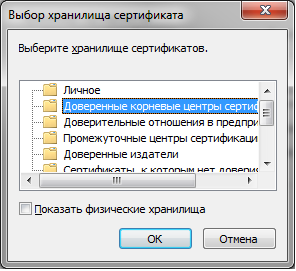
* Откроется окно «Мастер импорта сертификатов». Нажимаем кнопку «Далее».



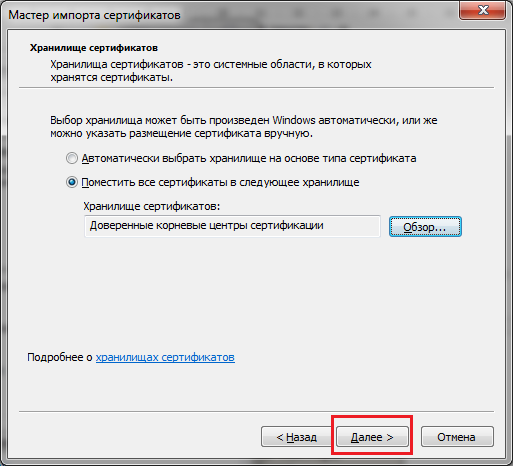
* Выбираем пункт «Поместить все сертификаты в следующее хранилище» и нажимаем кнопку «Обзор».



* В окне «Выбор хранилища сертификата» выбираем папку «Доверенные корневые центры сертификации» и нажимаем кнопку «ОК».

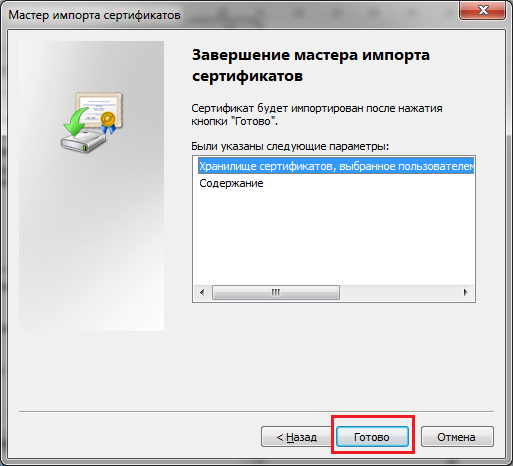


* Выбрав хранилище, нажимаем кнопку «Далее».



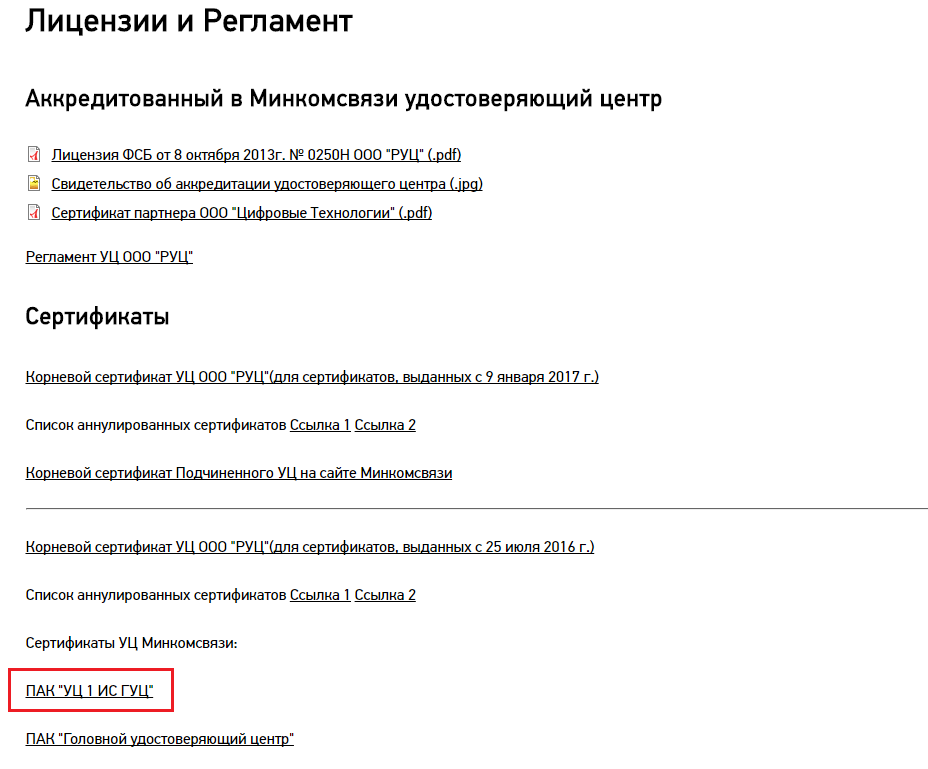
* Для завершения установки сертификата нажимаем кнопку «Готово».
* Соглашаясь с предупреждением системы безопасности Windows, нажимаем «Да». После Мастером будет выдано сообщение об успешном импорте сертификата.

Во многих случаях установки корневого сертификата «Головной удостоверяющий центр» достаточно для построения цепочки доверия сертификатов.

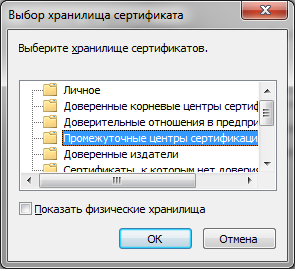


**Загрузка и установка промежуточного сертификата «УЦ 1 ИС ГУЦ»:**

* Загрузить файл «УЦ 1 ИС ГУЦ.cer» можно с сайта УЦ: <http://www.rcarus.ru/licenzii-i-reglament>

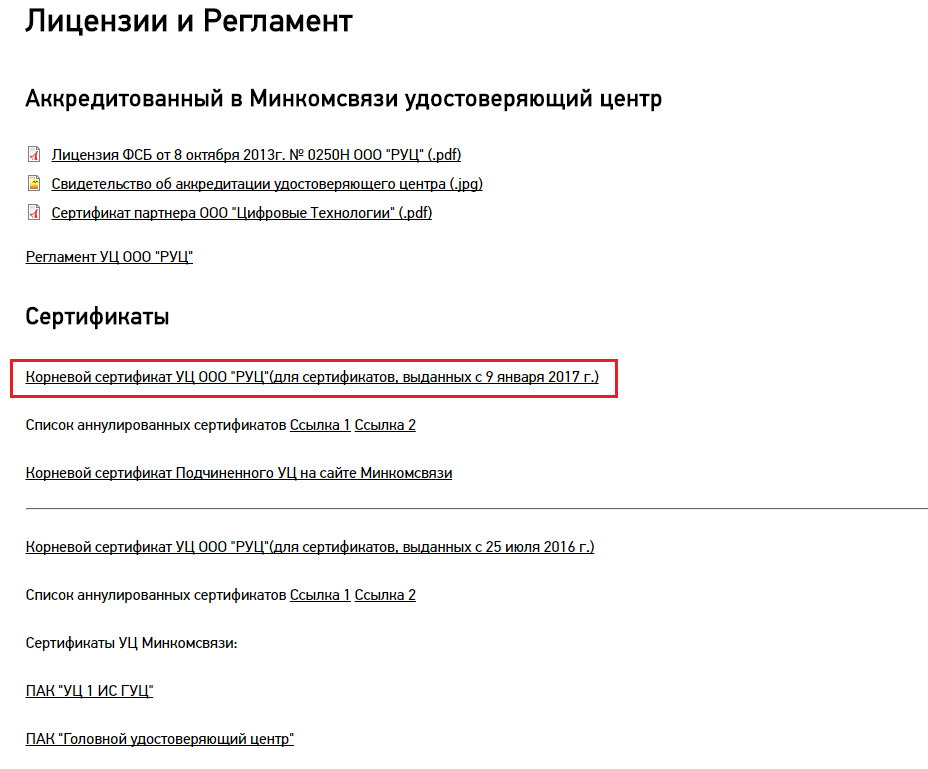


* Загрузить данный файл можно и по ссылке: <https://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=0408435EB90E5C8796A160E69E4BFAC453435D1D>.
* В открывшемся окне сертификата нажимаем кнопку «Установить сертификат». Процесс установки промежуточного сертификата аналогичен установке корневого сертификата «Головной удостоверяющий центр», но в окне «Выбор хранилища сертификата» выбираем папку «Промежуточные центры сертификации» и нажимаем кнопку «ОК».



**Загрузка и установка промежуточного корневого сертификата «ООО РУЦ»:**

* Загрузить файл «ООО РУЦ.cer» можно с сайта УЦ: <http://www.rcarus.ru/licenzii-i-reglament>.

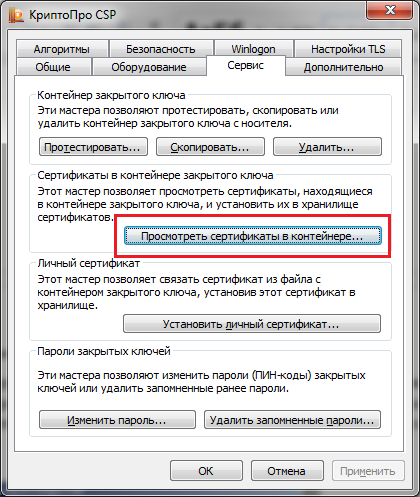


* Процесс установки промежуточного сертификата аналогичен установке корневого сертификата «УЦ 1 ИС ГУЦ».

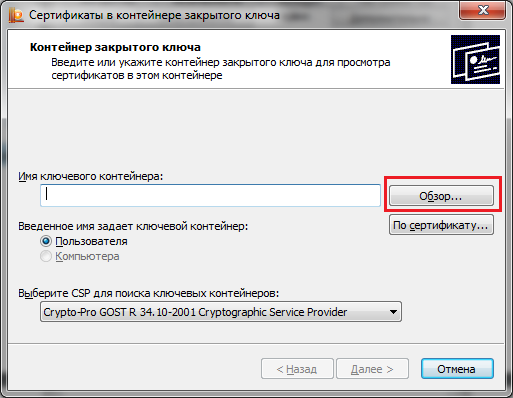
## Установка Личного сертификата

Установка личного сертификата выполняется в приведенной ниже последовательности:

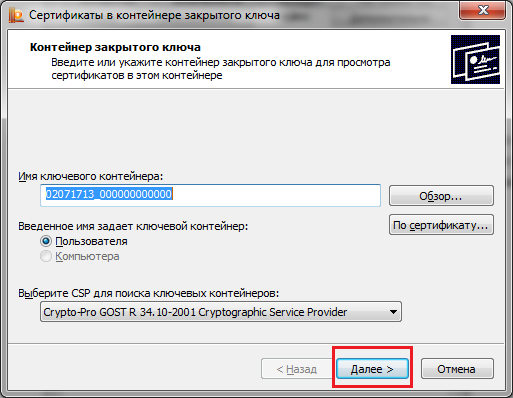
* Запускаем КриптоПро CSP («Пуск» -> «Панель управления» -> «КриптоПро CSP»). В открывшемся окне управления свойствами КриптоПро CSP на вкладке «Сервис» нажимаем кнопку «Посмотреть сертификаты в контейнере».



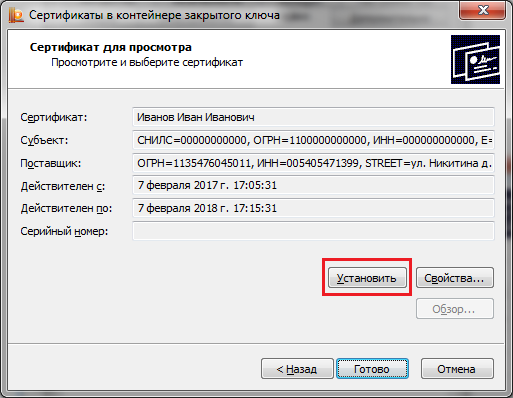
* В окне «Сертификаты в контейнере закрытого ключа» следует указать контейнер закрытого ключа, соответствующего выбранному сертификату. Для этого нажимаем кнопку «Обзор» и в открывшемся окне выбора в списке обнаруженных контейнеров указываем контейнер, соответствующий сертификату Вашей организации и нажимаем кнопку «ОК».



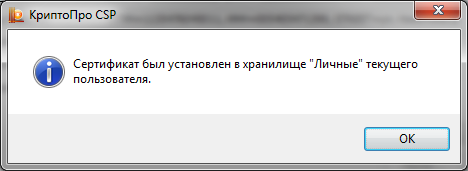
* Выбрав контейнер закрытого ключа, нажимаем кнопку «Далее».



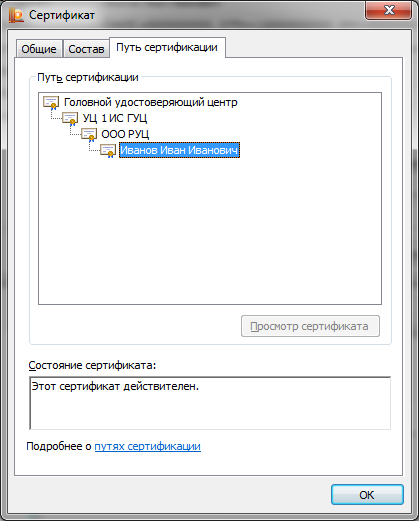
* В окне просмотра и установки сертификата нажимаем «Установить».



* Нажатием кнопки «Установить» будет выполнена установка сертификата выбранного ключевого контейнера в хранилище Личных сертификатов.



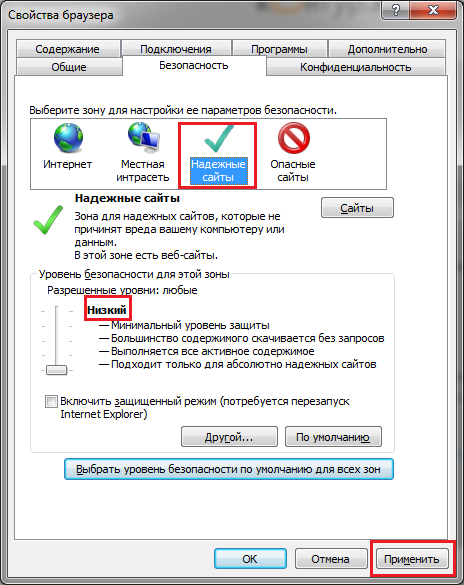
После установки всех сертификатов, цепочка доверия должна выглядеть следующим образом:



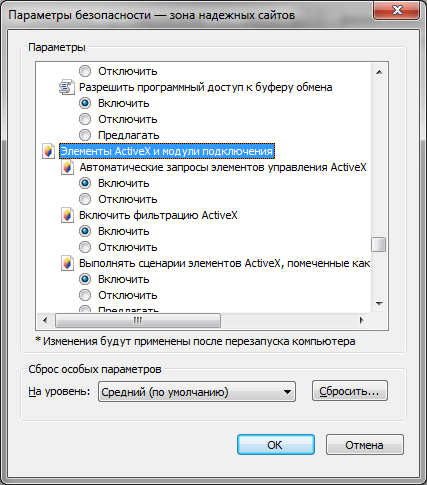
## Настройка безопасности Internet Explorer

Все необходимые настройки Internet Explorer Вы можете сделать, придерживаясь приведенной ниже последовательности:

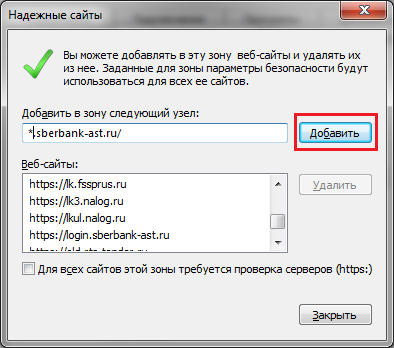
* Открываем «Свойства обозревателя» и, переключившись на вкладку «Безопасность», выбираем зону «Надежные сайты». Уровень безопасности установить «Низкий». Далее нажимаем «Применить».



* В блоке «Уровень безопасности для этой зоны» нажимаем кнопку «Другой» — будет открыто окно «Параметры безопасности». В разделе «Элементы ActiveX и модули подключения» необходимо включить все элементы, содержащие слово «ActiveX». Нажимаем «ОК»



* Нажимаем кнопку «Сайты». В открывшемся списке надежных сайтов снимаем флаг «Для всех узлов этой зоны требуется проверка серверов (https)», а в строке «Добавить в зону следующий узел» указываем адрес сайта, на котором вы собираетесь работать и нажимаем «Добавить».



Добавлять в список надежных узлов адреса сайтов рекомендуем в формате «\*.сайт.рф» — где: «\*» заменяет любые символы до точки, а строка «сайт.рф» является адресом основного узла. Такой формат позволит вам без проблем работать по всем протоколам (http:/ и https:/) и на всех уровнях узла.