



ИНСТРУКЦИЯ

по подготовке рабочего места для использования ЭП

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

1. Установка КриптоПро CSP	2
2. Установка КриптоПро ЭЦП Browser plug-in.....	5
3. Установка драйвера ключевого носителя Rutoken	5
4. Установка Личного сертификата.....	7
5. Установка Корневого сертификата ПАК «Минкомсвязь России».....	11
6. Настройка безопасности Internet Explorer	15
Заключение	17

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.

1. 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 «Скачать», нужно пройти предварительную регистрацию и авторизоваться по логину/пароллю.

The screenshot shows the website interface for Cryptopro.ru. At the top left is the logo with the text "КРИПТОПРО" and "Ключевое слово в защите информации". To the right is a search bar with a "Поиск" button. Below the header is a navigation menu with links: "О компании", "Продукты", "Услуги", "Партнёры", "Поддержка", "Купить", "Скачать", "Блог", "Форум". A main banner features "Защищённый доступ к корпоративным ресурсам через незащищённые сети" and "TLS-шлюз и VPN КриптоПро NGate". Below the banner is a section titled "Как загрузить дистрибутив?" with text explaining that distribution is only possible after registration and login. To the right is a "Купить" section listing products, technical services, and consulting. Below that is a "Вход" section with fields for "E-mail" and "Пароль / Password", and buttons for "Вход", "Регистрация", and "Забыли пароль?". At the bottom right is a "Услуги УЦ" section listing "Аккредитованный УЦ 63-ФЗ", "Неаккредитованный УЦ срса", and "ЦУС VPN".

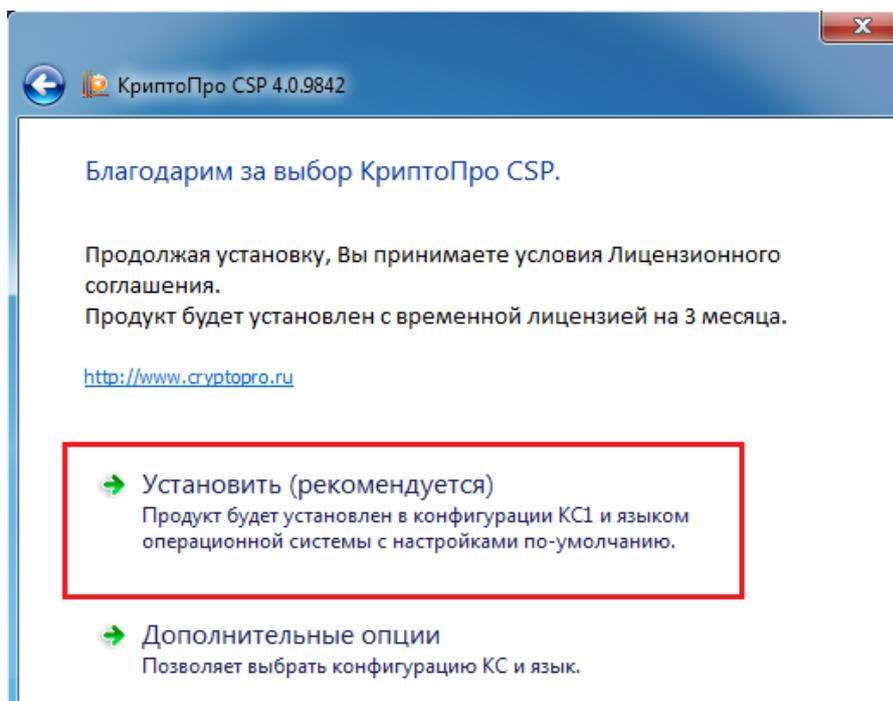
После регистрации появится страница с лицензионным соглашением. Ознакомившись с правилами и условиями нажимаем внизу экрана «Я согласен с Лицензионным соглашением. Перейти к загрузке» для перехода в раздел загрузки дистрибутивов. Далее необходимо скачать

и установить версию КриптоПРО CSP из раздела «Сертифицированные версии» согласно приобретенной лицензии (версия лицензии указана на бланке). Лицензии на право использования программного обеспечения оформляются на бумажном носителе формата А4.

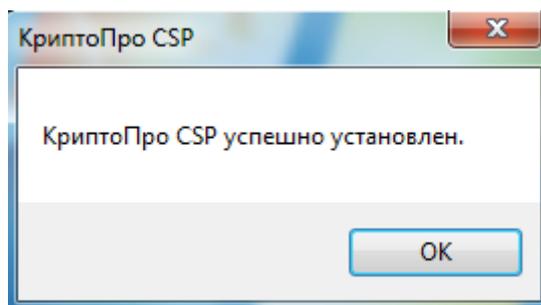
The screenshot shows the website for CryptoPro CSP. The header includes the CryptoPro logo and the tagline "Ключевое слово в защите информации". A search bar is located in the top right. The main navigation menu includes "О компании", "Продукты", "Услуги", "Партнёры", "Поддержка", "Купить", "Скачать", "Блог", and "Форум". Two main banners are present: "Корпоративные решения в области инфраструктуры «облачной» электронной подписи" and "Электронная подпись на базе КриптоПро DSS". The breadcrumb trail is "Главная > Продукты > КриптоПро CSP". The main heading is "КриптоПро CSP - Загрузка файлов". Under "Предварительные несертифицированные версии", there is a link for "КриптоПро CSP 4.0 R5 для Windows, macOS и UNIX (несертифицированный)". The "Сертифицированные версии" section is highlighted with a red box and contains links for "КриптоПро CSP 5.0 для Windows, macOS, UNIX и Android", "КриптоПро CSP 4.0 R4 для Windows, macOS и UNIX", and "КриптоПро CSP 4.0 R3 для Windows, macOS и UNIX". The "Архивные версии" section has a link for "Устаревшие СКЗИ". A right-hand sidebar menu lists various options, with "Загрузка файлов" highlighted in blue.

Последовательность установки КриптоПро CSP:

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

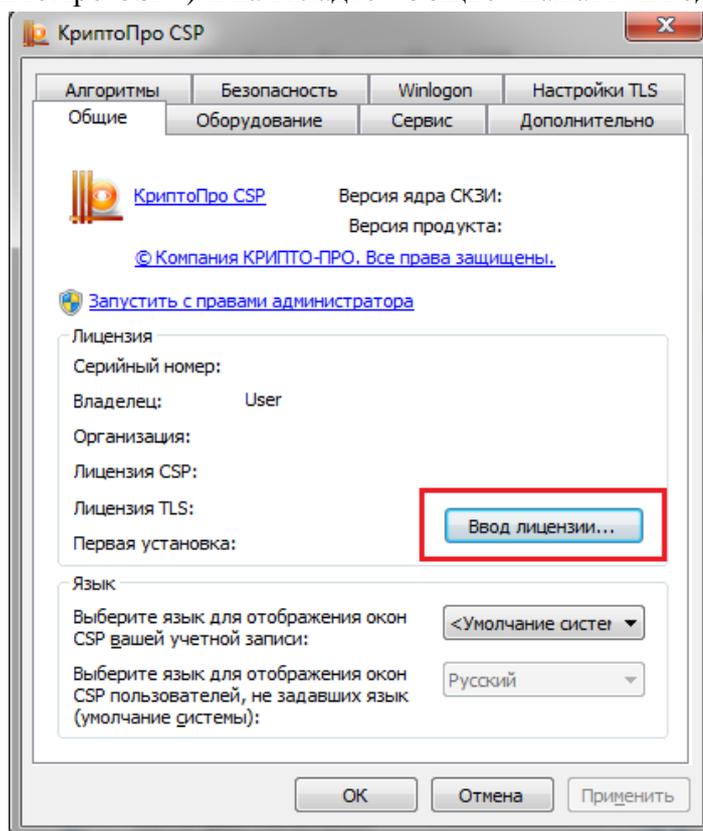


- Установка программы проходит автоматически в течение нескольких минут и не требует участия пользователя.
- По окончании процесса установки на экране появляется сообщение «КриптоПро CSP успешно установлен». Нажимаем «ОК».

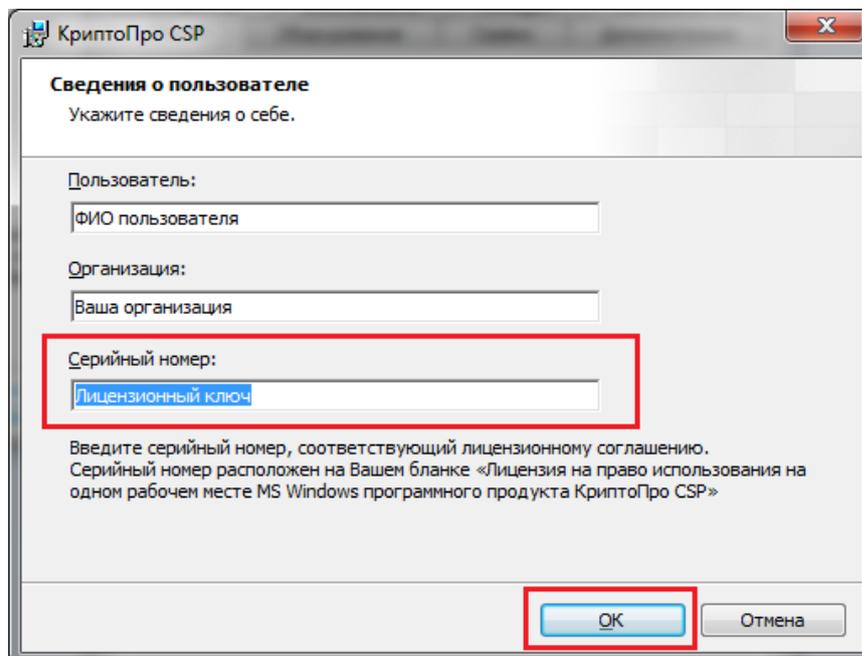


По условиям лицензионного соглашения срок использования демонстрационной версии КриптоПро CSP ограничен 90 днями с момента установки программы. Примечание: демонстрационный период предоставляется лишь при первой установке программы на компьютере.

Для активации лицензии на право использования программного продукта КриптоПро CSP необходимо запустить программу КриптоПро CSP («Пуск» -> «Все программы» -> «КРИПТО-ПРО» -> «КриптоПро CSP») и на вкладке «Общие» нажать «Ввод лицензии».



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



2. 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».

3. 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: <https://www.rutoken.ru/support/download/windows/>

Последовательность установки драйвера:

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

ДРАЙВЕРЫ ДЛЯ WINDOWS

ВОПРОС-ОТВЕТ

ЦЕНТР ЗАГРУЗКИ

- [Драйверы для Windows](#)
- [Драйверы для ЕГАИС](#)
- [Рутокен для КристоПро](#)
- [Рутокен для Signal-COM](#)
- [Рутокен Плагин](#)
- [Библиотека PKCS#11](#)
- [Драйверы для *nix](#)
- [Драйверы для Mac](#)
- [ПО для Рутокен Web](#)
- [ПО для Рутокен VPN](#)

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, EXE

Версия: v.4.2.2.0 от 11.04.2017
 Поддерживаемые ОС: 32- и 64-разрядные Microsoft Windows 10/8.1/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003

Системным администраторам ▾

Утилиты ▾

ИНСТРУКЦИИ

-  [Настройка и эксплуатация Рутокен](#)
-  [Управление драйверами при помощи групповых политик](#)
-  [Переход от rtCert к работе с Панелью управления Рутокен](#)

ДРАЙВЕРЫ ДЛЯ ЕГАИС

Предыдущие стабильные версии

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

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

ВОПРОС-ОТВЕТ

ЦЕНТР ЗАГРУЗКИ

- [Драйверы для Windows](#)
- [Драйверы для ЕГАИС](#)
- [Рутокен для КристоПро](#)
- [Рутокен для Signal-COM](#)
- [Рутокен Плагин](#)
- [Библиотека PKCS#11](#)
- [Драйверы для *nix](#)
- [Драйверы для Mac](#)
- [ПО для Рутокен Web](#)
- [ПО для Рутокен VPN](#)

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

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

Утверждено
Приказом генерального директора
ЗАО «Актив-софт»
№ 01-ЛС от 31.08.2012 г.

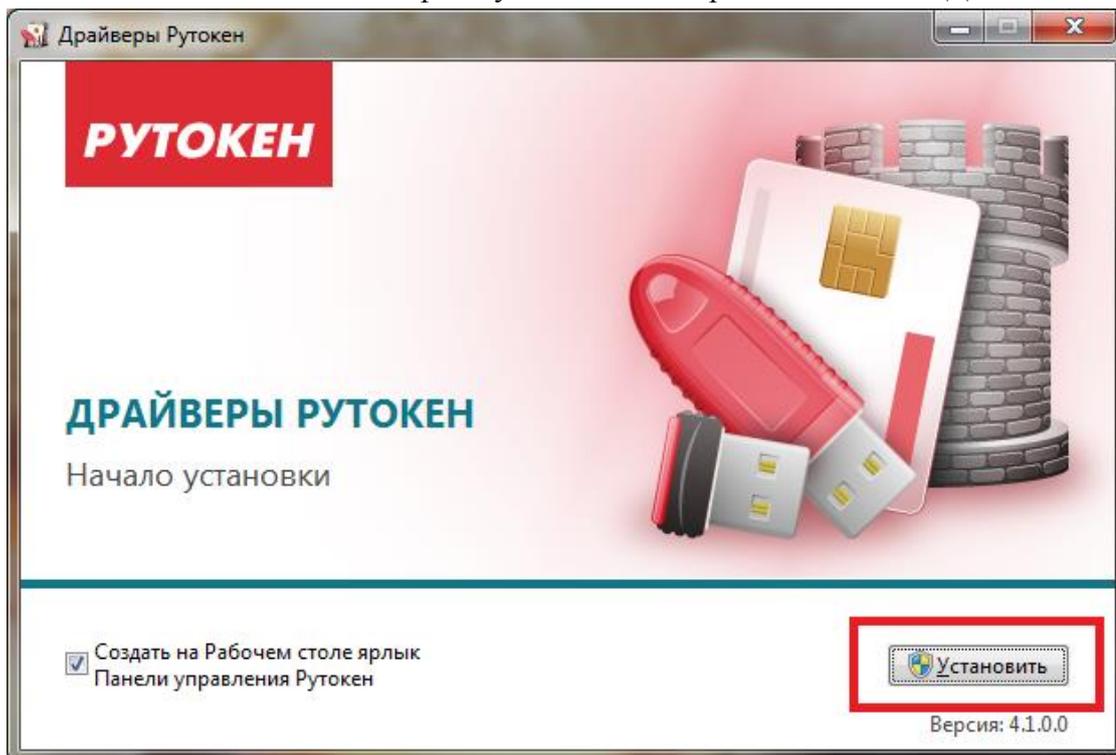
**Лицензионное соглашение
на использование программных продуктов
и/или онлайн-сервисов Рутокен (Rutoken)**
Редакция №01 от 31.08.2012 г.

Настоящий документ представляет собой предложение Закрытого акционерного общества «Актив-софт» (далее — «Правообладатель») заключить соглашение на изложенных ниже условиях.

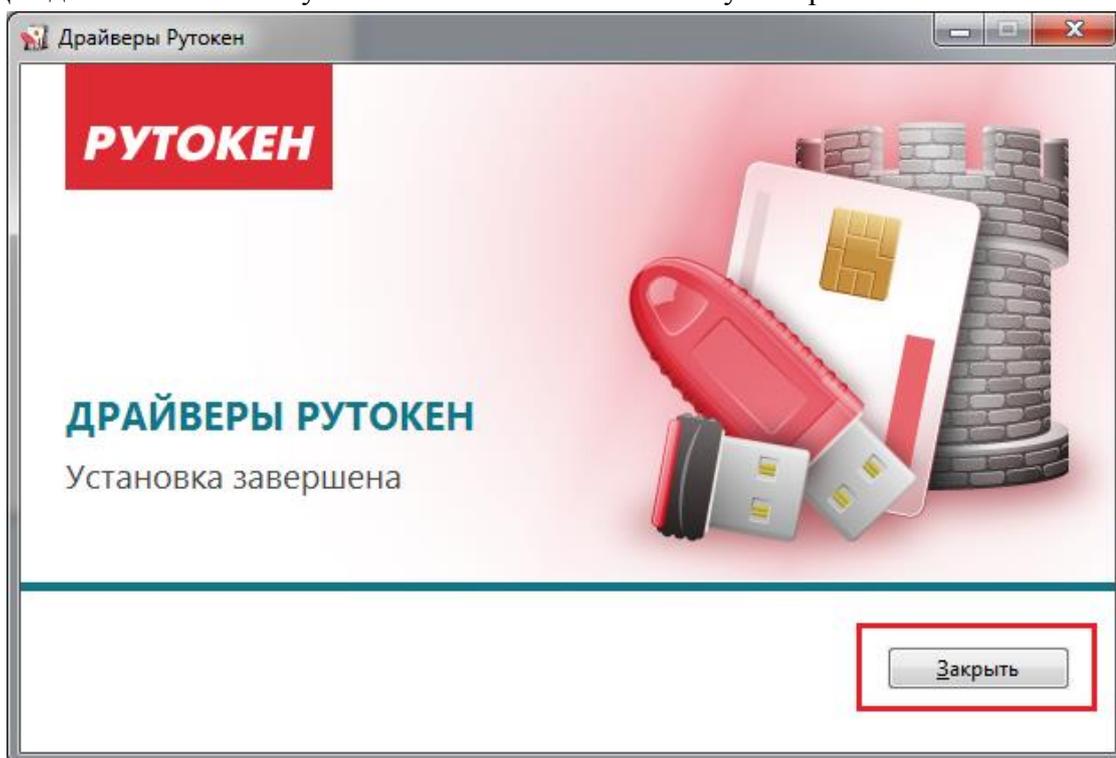
Условия Лицензионного соглашения прочитаны и приняты в полном объеме.

УСЛОВИЯ ПРИНЯТЫ

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



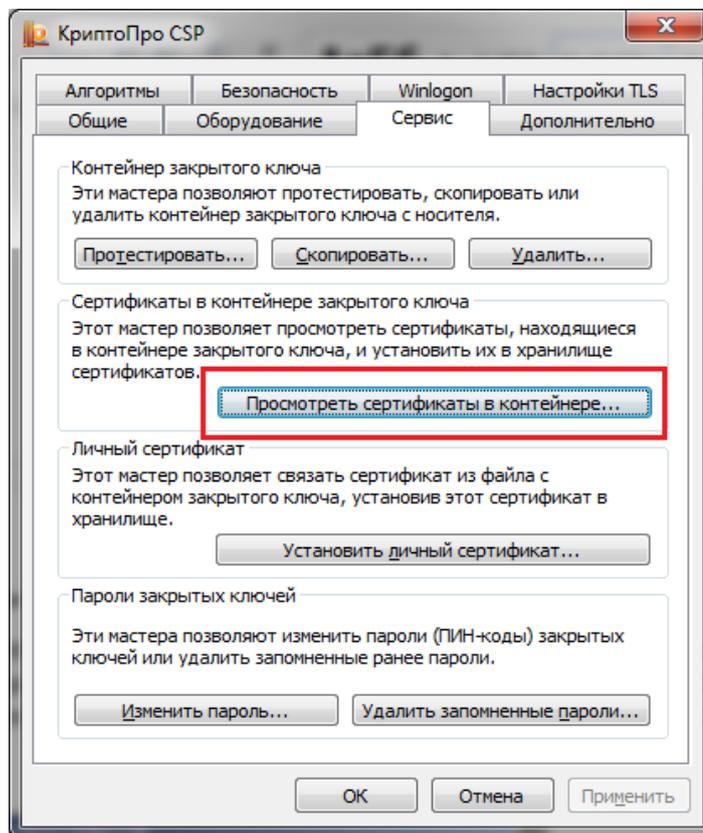
- Дождитесь окончания установки и нажмите на кнопку «Закреть».



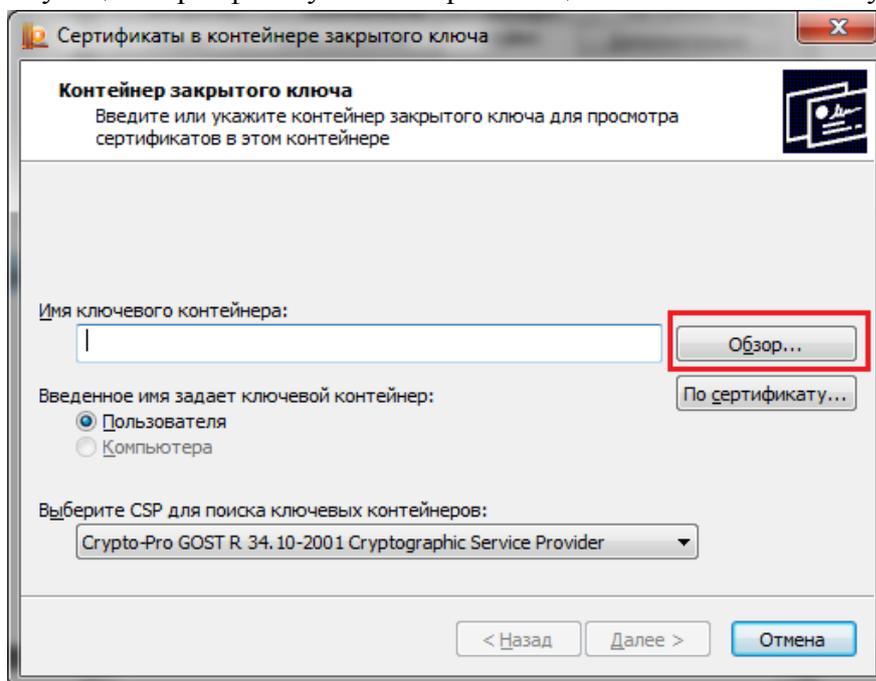
4. Установка Личного сертификата

Установка личного сертификата выполняется в приведенной ниже последовательности:

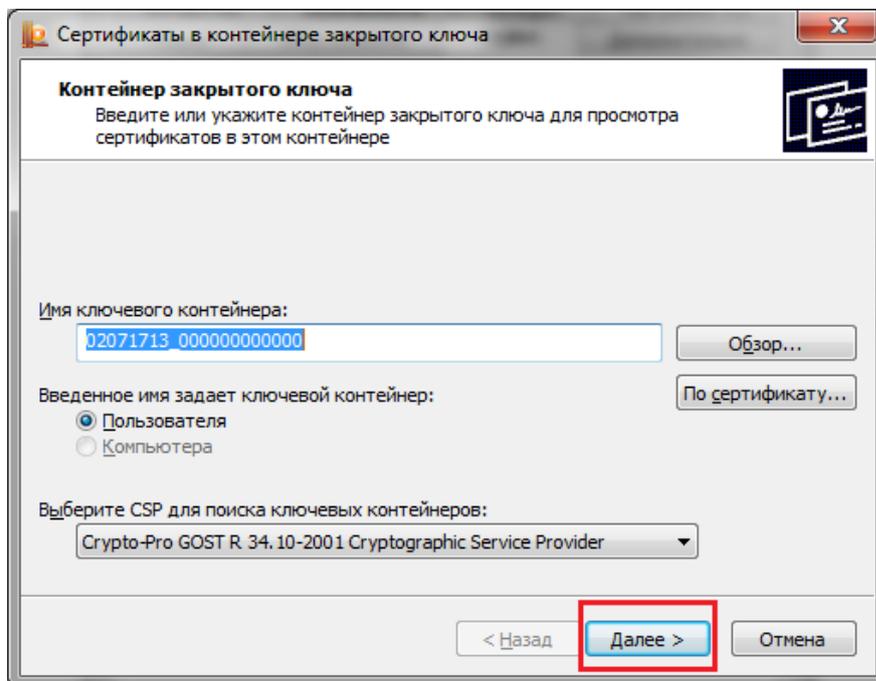
- Запускаем КриптоПро CSP («Пуск» -> «Все программы» -> «КРИПТО-ПРО» -> «КриптоПро CSP»). В открывшемся окне управления свойствами КриптоПро CSP на вкладке «Сервис» нажимаем кнопку «Посмотреть сертификаты в контейнере».



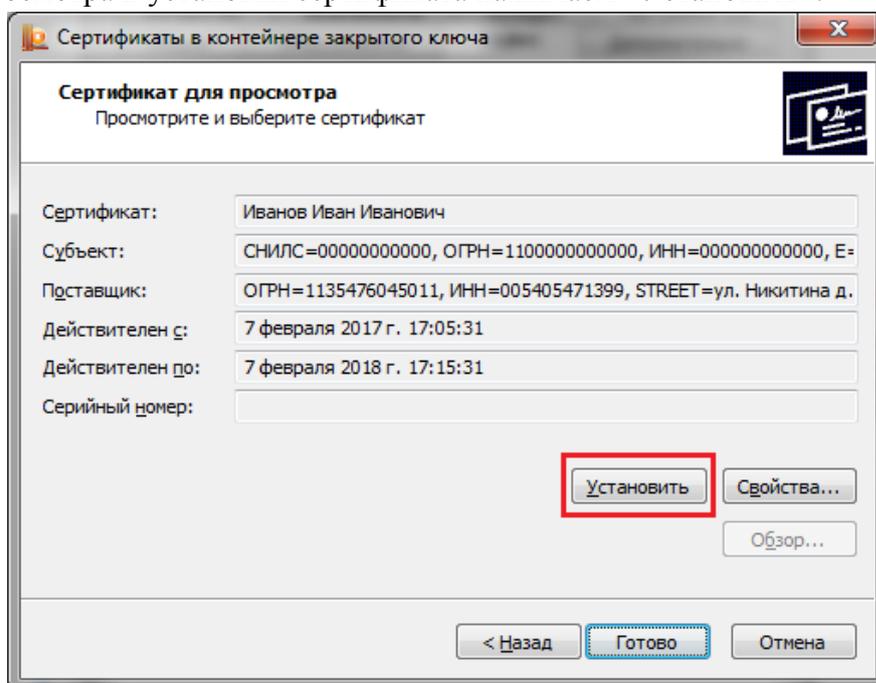
- В окне «Сертификаты в контейнере закрытого ключа» следует указать контейнер закрытого ключа, соответствующего выбранному сертификату. Для этого нажимаем кнопку «Обзор» и в открывшемся окне выбора в списке обнаруженных контейнеров указываем контейнер, соответствующий сертификату Вашей организации и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



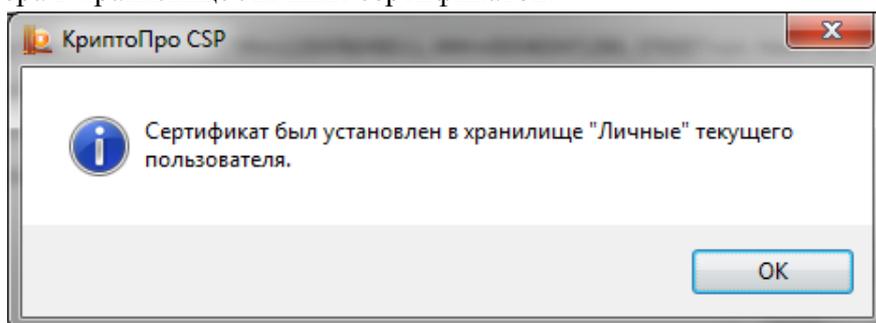
- Выбрав контейнер закрытого ключа, нажимаем кнопку «Далее».



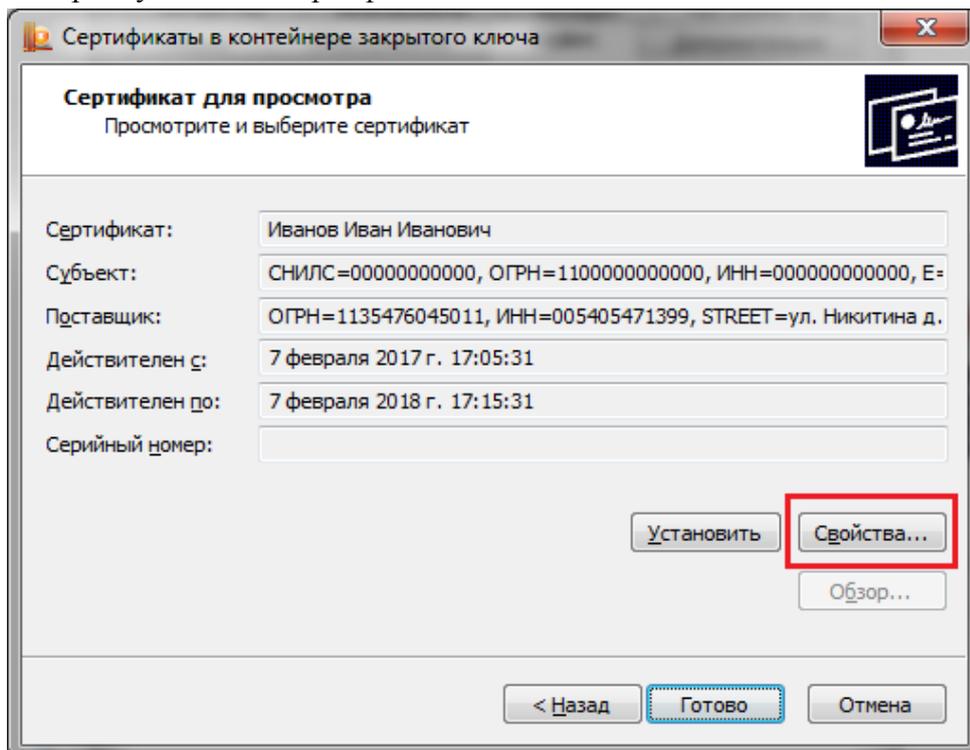
- В окне просмотра и установки сертификата нажимаем «Установить».



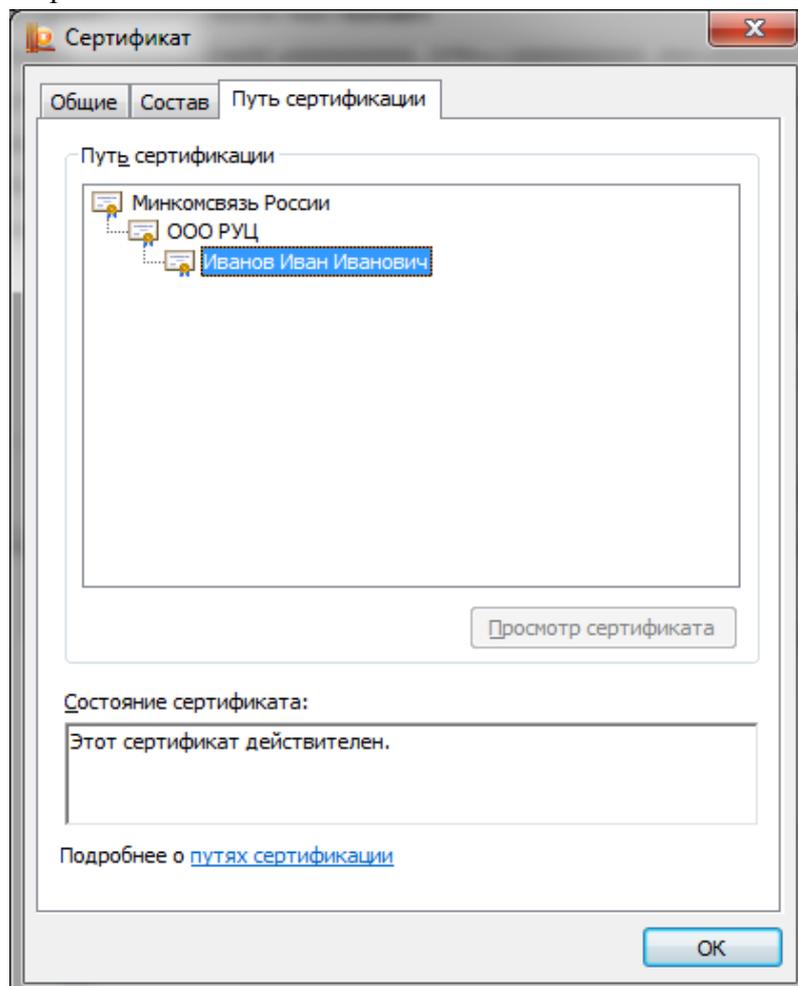
- Нажатием кнопки «Установить» будет выполнена установка сертификата выбранного ключевого контейнера в хранилище Личных сертификатов.



После установки личного сертификата необходимо проверить цепочку доверия. Для этого в окне просмотра и установки сертификата нажимаем «Свойства».

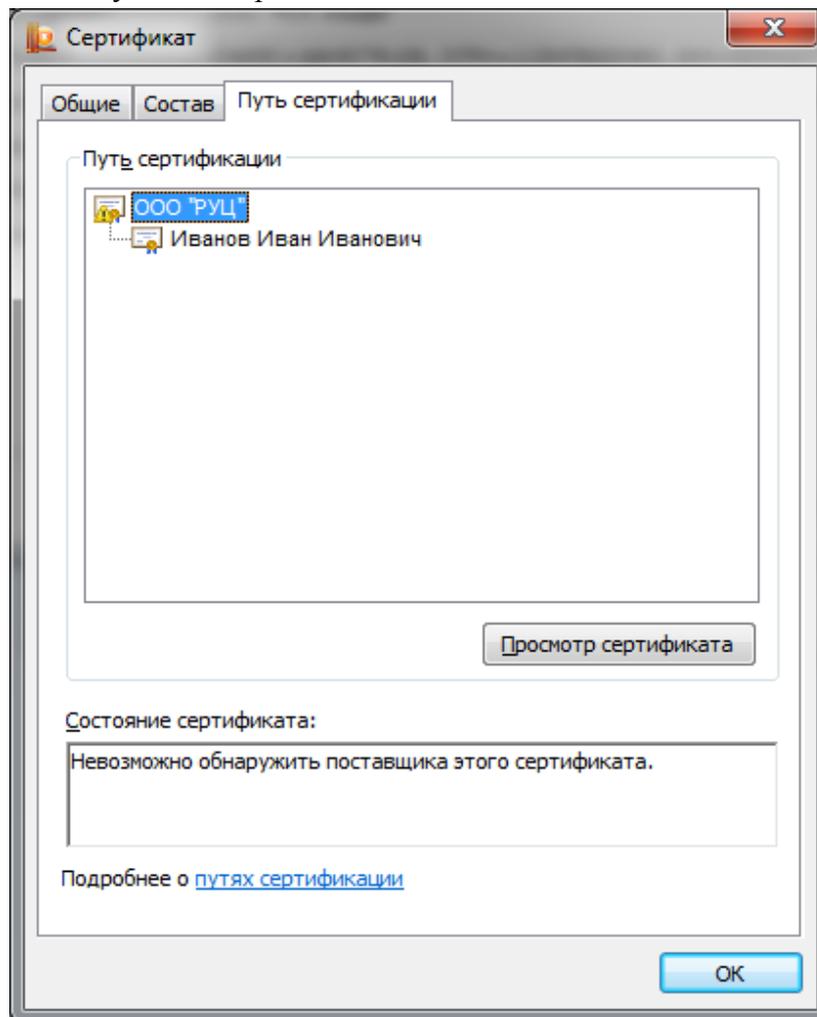


Далее переходим на вкладку «Путь сертификации». Путь сертификации должен выглядеть следующим образом:



Если установка Личного сертификата прошла успешно, закрываем окна «Сертификат» и «КриптоПро CSP». Далее переходим к 6 разделу «Настройка безопасности Internet Explorer».

Если при обработке одного из сертификатов в пути возникает проблема или не удается найти сертификат, путь сертификации считается ненадежным. Путь сертификации в данном случае может выглядеть следующим образом:

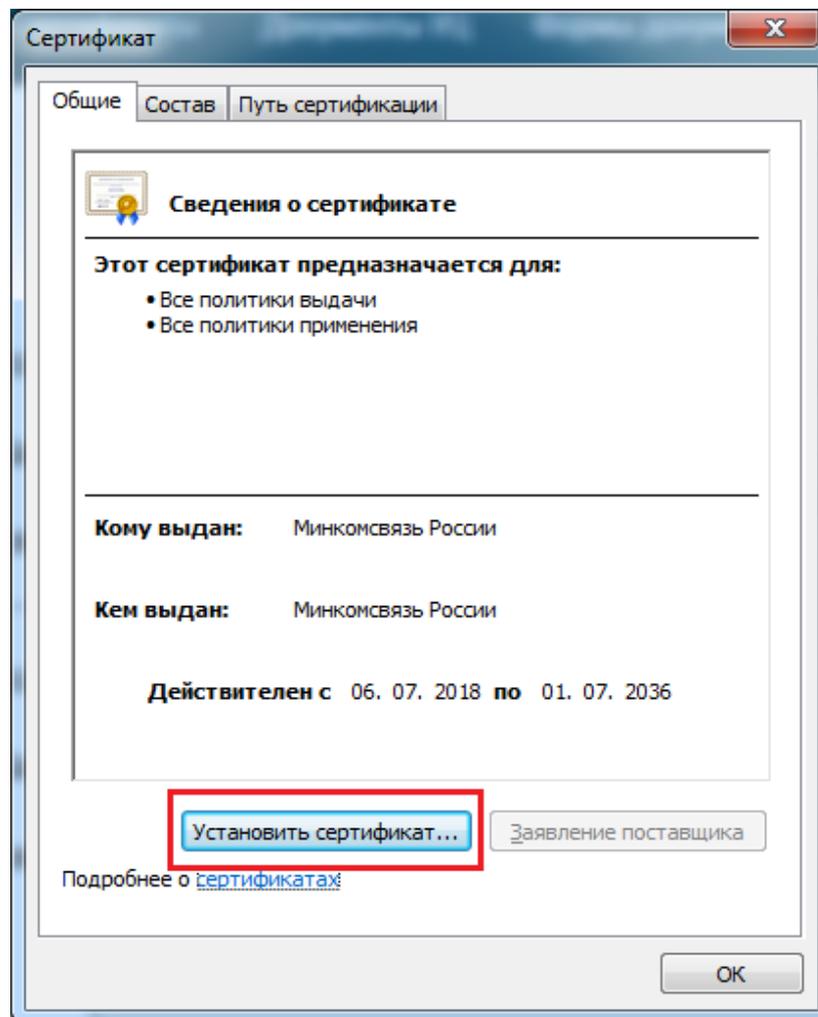


Для подтверждения подлинности личного сертификата, необходимо установить корневой сертификат Минкомсвязи России. Тогда переходим к 5 разделу «Установка Корневого сертификата ПАК «Минкомсвязь России»»

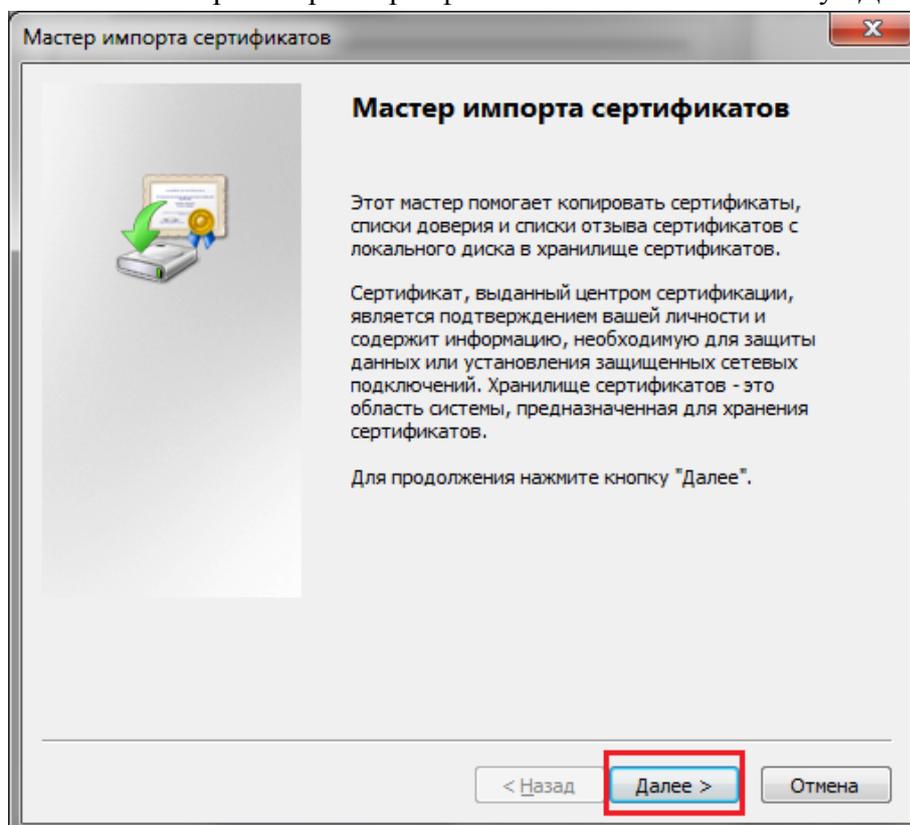
5. Установка Корневого сертификата ПАК «Минкомсвязь России»

Загрузка и установка корневого сертификата «Минкомсвязь России»:

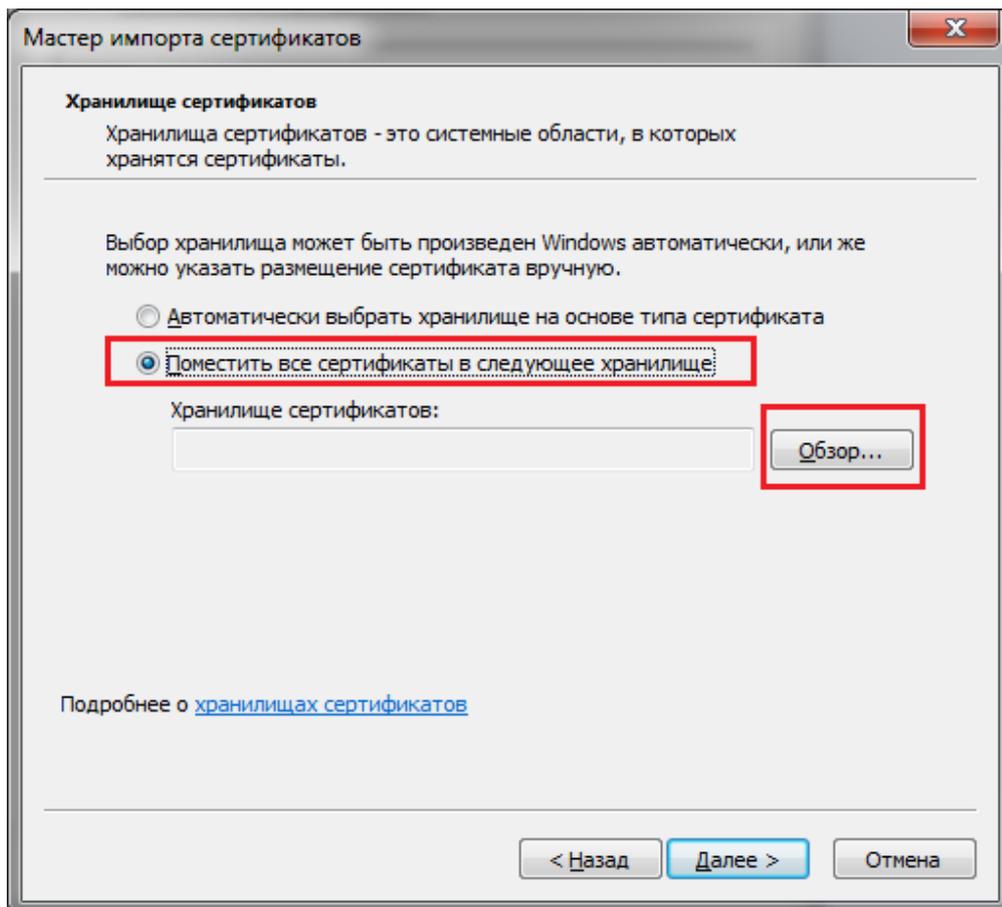
- Загрузить файл «Минкомсвязь России» можно по прямой ссылке с сайта портала уполномоченного федерального органа в области использования электронной подписи: <https://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=4BC6DC14D97010C41A26E058AD851F81C842415A>
- В открывшемся окне сертификата нажимаем кнопку «Установить сертификат».



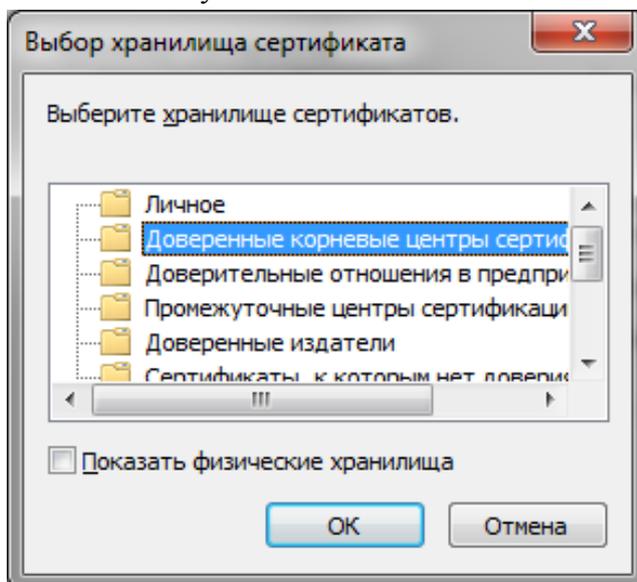
- Откроется окно «Мастер импорта сертификатов». Нажимаем кнопку «Далее».



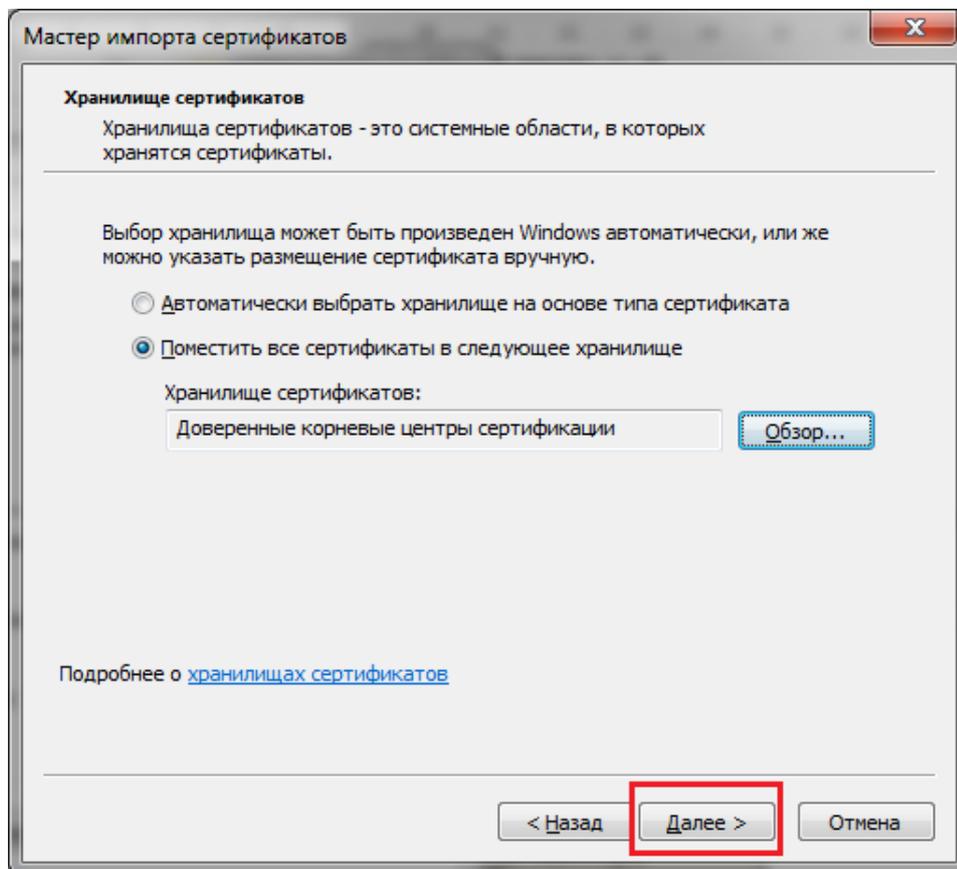
- Выбираем пункт «Поместить все сертификаты в следующее хранилище» и нажимаем кнопку «Обзор».



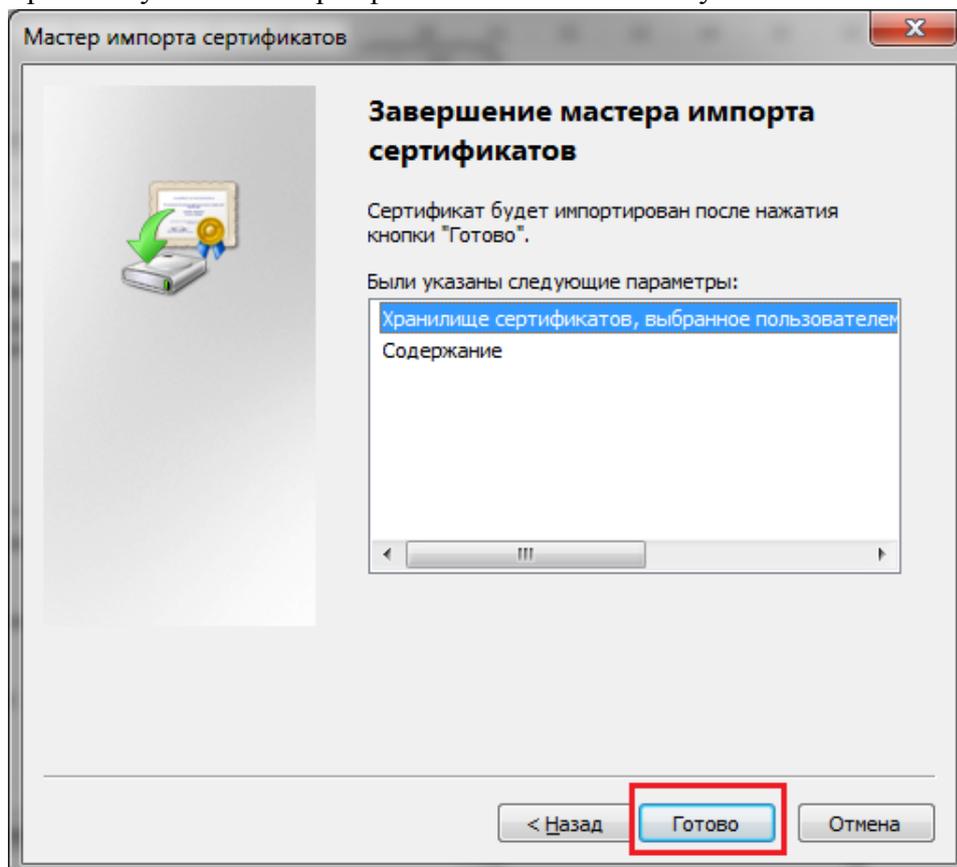
- В окне «Выбор хранилища сертификата» выбираем папку «Доверенные корневые центры сертификации» и нажимаем кнопку «ОК».



- Выбрав хранилище, нажимаем кнопку «Далее».



- Для завершения установки сертификата нажимаем кнопку «Готово».

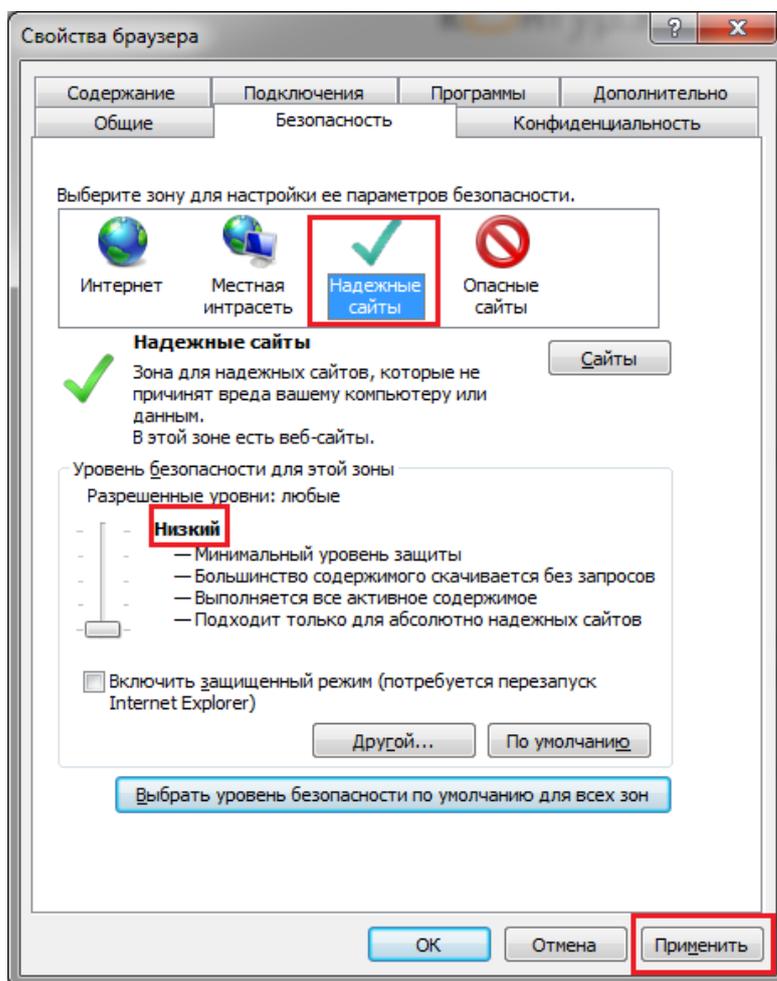


- Соглашаясь с предупреждением системы безопасности Windows, нажимаем «Да». После Мастером будет выдано сообщение об успешном импорте сертификата.

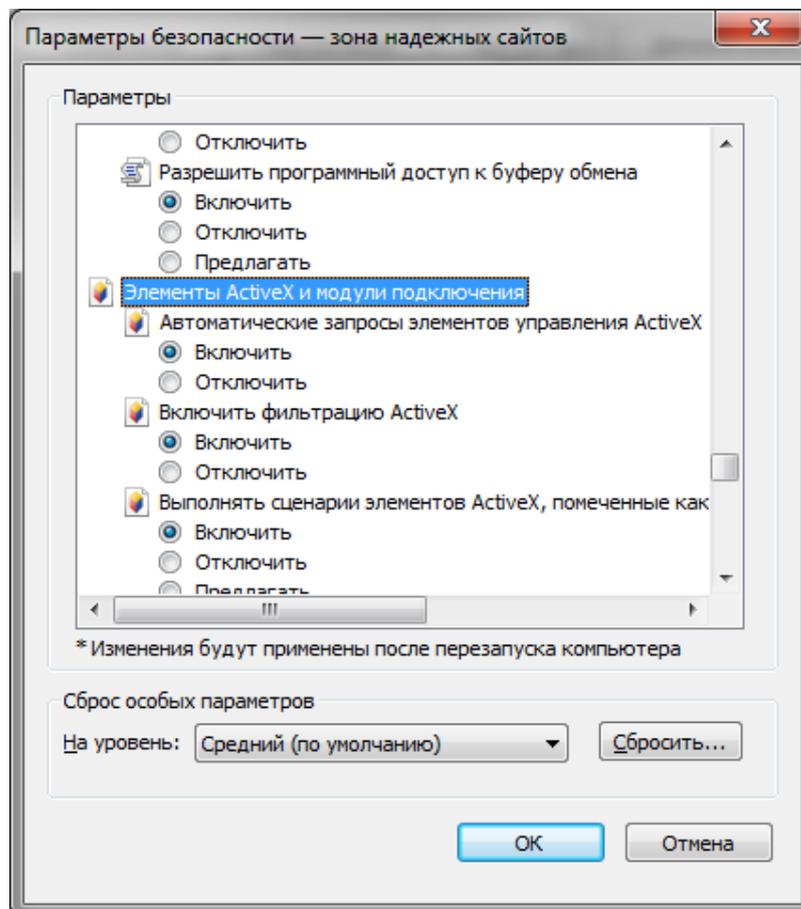
6. Настройка безопасности Internet Explorer

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

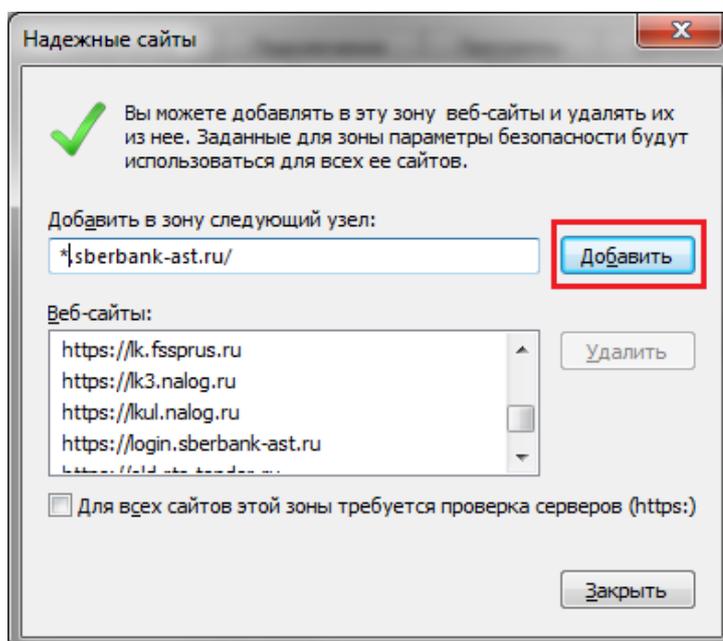
- Открываем «Свойства обозревателя» и, переключившись на вкладку «Безопасность», выбираем зону «Надежные сайты». Уровень безопасности установить «Низкий». Далее нажимаем «Применить».



- 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.

Заключение

Если у вас возникли вопросы или проблемы, связанные с выполнением каких-либо из вышеперечисленных установок и/или настроек, Вы можете обратиться в службу технической поддержки пользователей ООО «РУЦ» в рабочие дни с 9:00 до 18:00 (в пятницу с 9:00 до 17:00) по электронной почте sales@rcarus.ru или по телефону (383) 216-47-48.

При обращении в техническую поддержку желательно предварительно скачать и запустить программу удаленного доступа. Скачать можно по ссылке <https://download.teamviewer.com/download/TeamViewerQS.exe>