Федеральная служба по финансовому мониторингу

(Росфинмониторинг)

Инструкция по настройке рабочего места пользователя Портала Росфинмониторинга

Москва 2016 г.

**Содержание**

[1 Общие требования к настройке рабочего места 3](#_Toc468803971)

[2 Параметры рабочей станции 4](#_Toc468803972)

[2.1 Операционная система 4](#_Toc468803973)

[2.2 Доступ к сети Интернет 4](#_Toc468803974)

[3 Установка и настройка программного обеспечения 5](#_Toc468803975)

[3.1 Microsoft .NET Framework 5](#_Toc468803976)

[3.2 СКЗИ «КриптоПро CSP» 5](#_Toc468803977)

[3.3 КриптоПро ЭЦП Browser plug-in 6](#_Toc468803978)

[3.4 Браузер Internet Explorer версии 11 с настроенным режимом совместимости. 6](#_Toc468803979)

[3.5 Установка компонента SilverLight 9](#_Toc468803980)

[3.6 Драйвер носителя электронной подписи 10](#_Toc468803981)

[3.6.1 Установка драйвера носителя типа eToken 10](#_Toc468803982)

[3.6.2 Установка драйвера носителя типа Rutoken 14](#_Toc468803983)

[4 Настройка сертификатов на рабочем месте 16](#_Toc468803984)

[4.1 Сертификат должностного лица организации 16](#_Toc468803985)

[4.2 Корневой сертификат Головного удостоверяющего центра Министерства связи и массовых коммуникаций РФ 21](#_Toc468803986)

[4.3 Кросс-сертификаты «УЦ 1 ИС ГУЦ» и «УЦ 2 ИС ГУЦ» Министерства связи и массовых коммуникаций РФ 25](#_Toc468803987)

[4.4 Кросс-сертификат Вашего удостоверяющего центра. 27](#_Toc468803988)

[5 Проверка правильности установки сертификатов. 31](#_Toc468803989)

# Общие требования к настройке рабочего места

Компьютер, с которого будет осуществлять доступ к Порталу, должен соответствовать следующим требованиям:

1. [Установлена операционная система (ОС) Windows 7 или выше.](#_Операционная_система)
2. [Сделана отдельная учетная запись пользователя в Windows для взаимодействия с Порталом](#_Операционная_система)
3. [Обеспечен доступ к сети Интернет напрямую или произведены настройки прокси-сервера или межсетевого экрана согласно данной Инструкции.](#_Доступ_к_сети)
4. Установлены следующие ПО:

* [Microsoft Framework 4.5;](#_Microsoft_.NET_Framework)
* [СКЗИ «КриптоПро CSP» и ЭЦП Browser plug-in;](#_СКЗИ_«КриптоПро_CSP»)
* [Браузер Internet Explorer версии 11 с настроенным режимом совместимости.](#_Браузер_Internet_Explorer)
* [Компонент SilverLight.](#_Установка_компонента_SilverLight)
* [Драйвер для носителя электронной подписи (eToken или Rutoken)](#_Драйвер_Вашего_носителя)

1. Установлены и настроены сертификаты:

- [должностного лица организации;](#_Сертификат_должностного_лица)

- [корневой сертификат Головного удостоверяющего центра (УЦ) Минкомсвязи](#_Корневой_сертификат_Головного)

- [кросс-сертификаты «УЦ1 ИС ГУЦ» и «УЦ2 ИС ГУЦ» Минкомсвязи](#_Кросс-сертификаты_«УЦ_1)

- [кросс-сертификат Вашего УЦ](#_Кросс-сертификат_Вашего_удостоверяю)

# Параметры рабочей станции

## Операционная система

* Компьютер, с которого осуществляется доступ к Порталу, должен работать под управлением ОС Windows (рекомендуемая версия OC – Windows 7 или выше).

Внимание: При работе на портале с использованием Windows XP могут возникать трудности, по причине того, что данная ОС устарела и более не поддерживается Microsoft.

* Пользователь операционной системы Windows должен иметь права администратора, если таких прав нет, то обратитесь к вашему системному администратору.
* Если с данного компьютера происходит отправка отчётов с использованием сертификата (ЭП) в другие органы, то необходимо использовать другой отдельный ПК или на этом же сделать другую учётную запись (второго пользователя) в Windows.

## Доступ к сети Интернет

Доступ к сети Интернет на компьютере, на котором планируется настроить рабочее место пользователя Портала, должен осуществляться напрямую, т.е. без использования прокси-сервера.

В случае если доступ в Интернет осуществляется через корпоративную сеть использующую прокси-сервер или межсетевой экран (файервол, брандмауэр), необходимо открыть порт **8081 (TCP/IP)** для доступа к IP адресам:

- **195.16.102.197** - Web-сайт Росфинмониторинга (**www.fedsfm.ru**)

- **195.16.102.200** - Портал Росфинмониторинга ([https://portal.fedsfm.ru](https://portal.fedsfm.ru/)) для обмена информацией в электронном виде через **Личный кабинет организаций**.

Также для доступа к сайту и Порталу Росфинмониторинга должны быть открыты порты  **80, 8080, 443, 8443 (TCP/IP)**

# Установка и настройка программного обеспечения

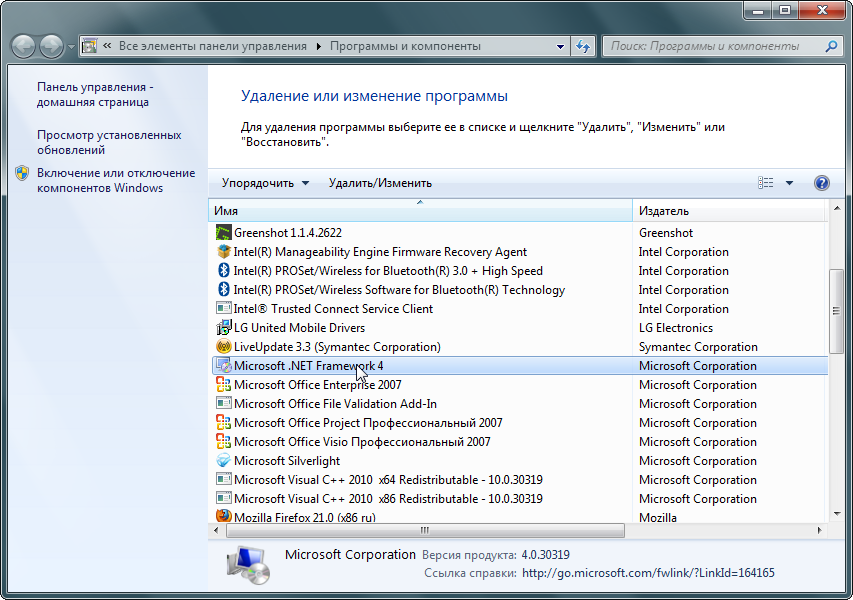
## Microsoft .NET Framework

Наличие последней версии Microsoft Framework для вашей ОС. В случае отсутствия пакет необходимо скачать и установить с официального сайта:

.NET Framework 4 (Для Windows XP) - <https://www.microsoft.com/ru-ru/download/details.aspx?id=17718>

.NET Framework 4.5 (Для Windows более высокой версии) - <https://www.microsoft.com/ru-ru/download/details.aspx?id=30653>

Список установленной версии .NET Framework на можно просмотреть, открыв Пуск – Панель управления – Программы и компоненты(Установка и удаление программ):



## СКЗИ «КриптоПро CSP»

Для использования механизма подписания документов средствами электронной подписи на Вашем компьютере должен быть установлено средство криптографической защиты информации (СКЗИ) «КриптоПро CSP» версии 3.6 или выше.

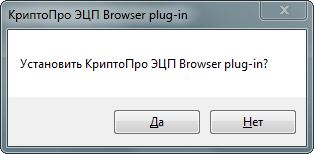
СКЗИ «КриптоПро CSP» является платным и может быть получено следующими способами:

* В удостоверяющем центре, при получении сертификата квалифицированной ЭП.
* У компании-разработчика СКЗИ «КриптоПро CSP» (на сайте разработчика можно скачать условно-бесплатную версию с периодом бесплатной пробной эксплуатации 3 месяца по ссылке <http://www.cryptopro.ru/products/fkc/etoken/downloads>) или у официального дилера.
* Более подробную информацию по установке и использованию СКЗИ «КриптоПро CSP» можно получить в <http://www.cryptopro.ru/sites/default/files/docs/csp36r3/instruction_csp_r3.pdf>.

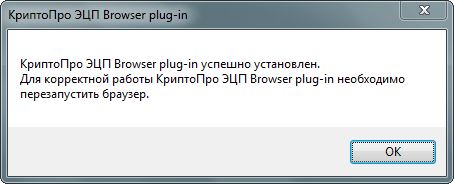
## КриптоПро ЭЦП Browser plug-in

Установочный файл плагина можно скачать http://www.cryptopro.ru/products/cades/plugin/get\_2\_0

Для установки запустите скачанный файл и нажмите кнопку **Да**.

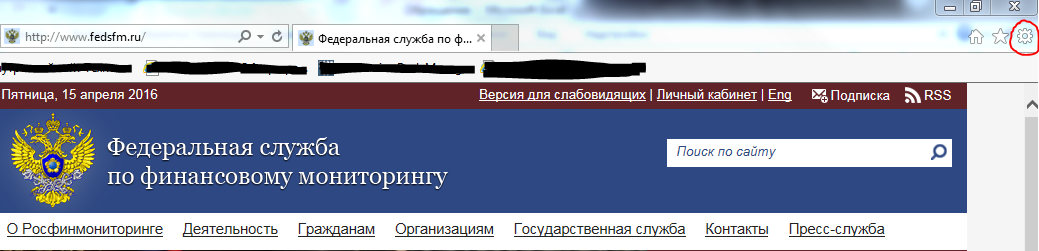


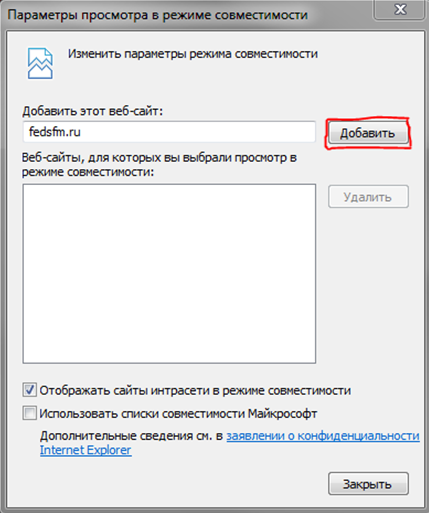
После нажатия кнопки **Да** на ваш компьютер будет установлен Browser plug-in:



## Браузер Internet Explorer версии 11 с настроенным режимом совместимости.

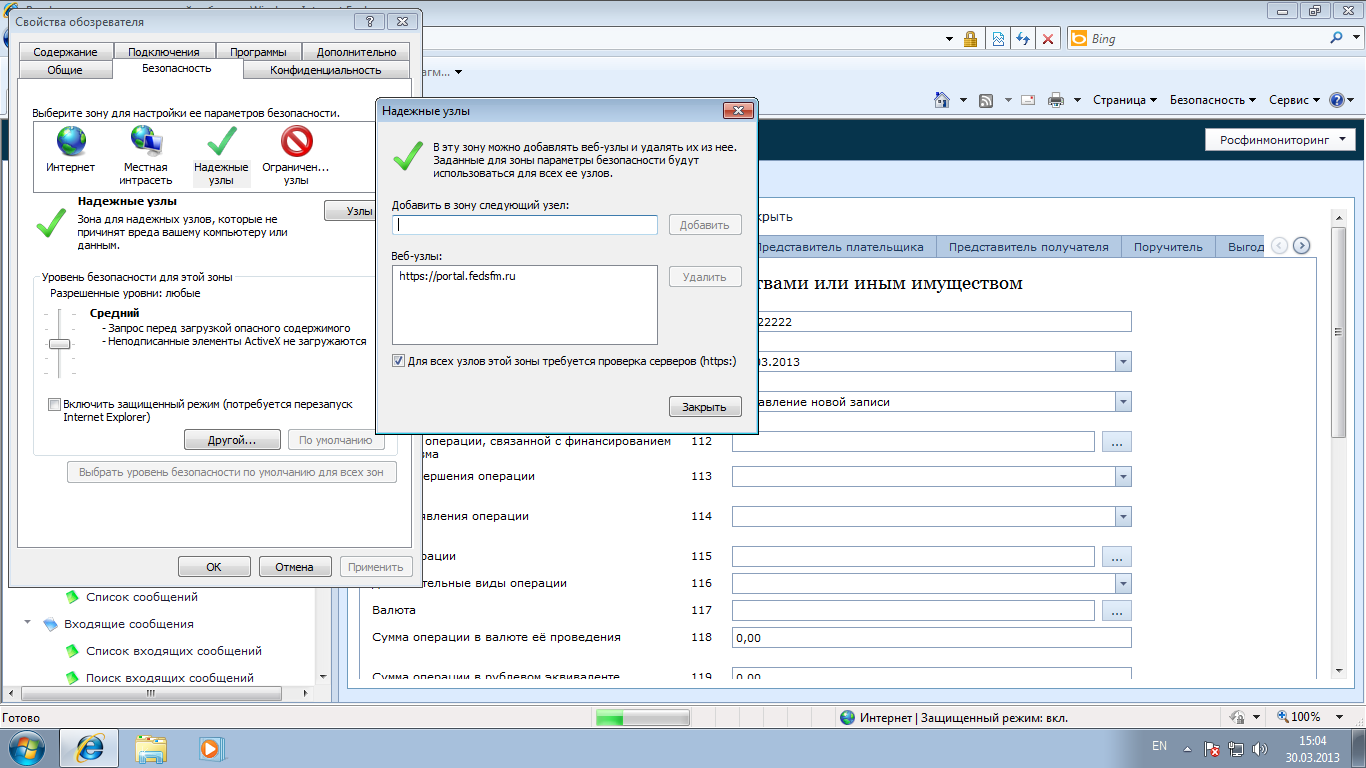
* Для корректной работы портала рекомендуется использовать браузер Internet Explorer версии 11. В прочих версиях браузера при работе портала могут возникать затруднения.
* Для работы в браузере Internet Explorer версии 11 требуется настроить режим совместимости.

Зайдите на сайт <http://www.fedsfm.ru/>. В правом верхнем углу браузера нажмите кнопку в виде шестерёнки (Сервис)  и в появившемся меню “Параметры просмотра в режиме совместимости”. Нажмите Добавить и перезагрузите браузер.



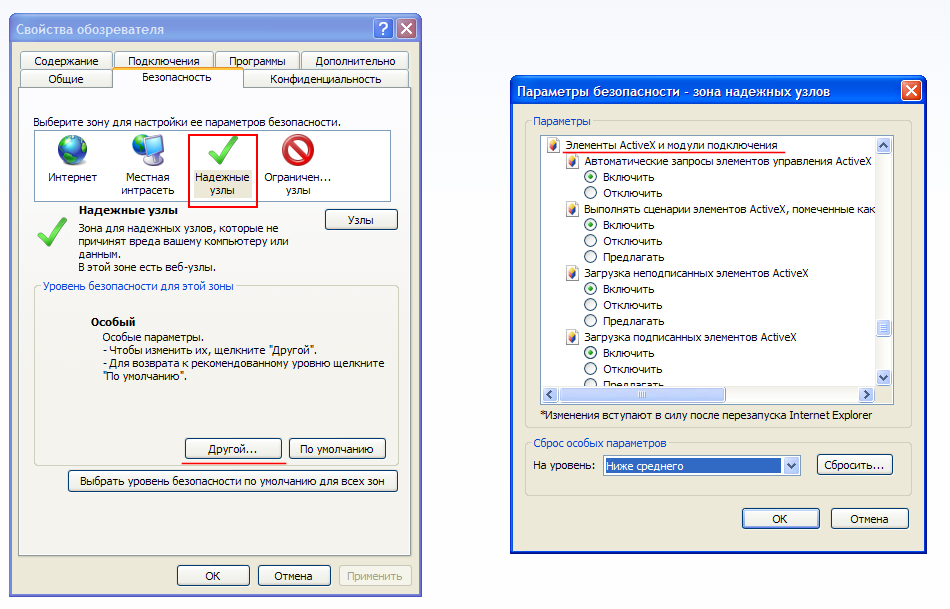
* Портал Росфинмониторинга должен быть добавлен в надежные узлы

В браузере Internet Explorer в «Свойствах обозревателя» на вкладке «Безопасность» должен быть добавлен в список «Надежные узлы» адрес: https://portal.fedsfm.ru

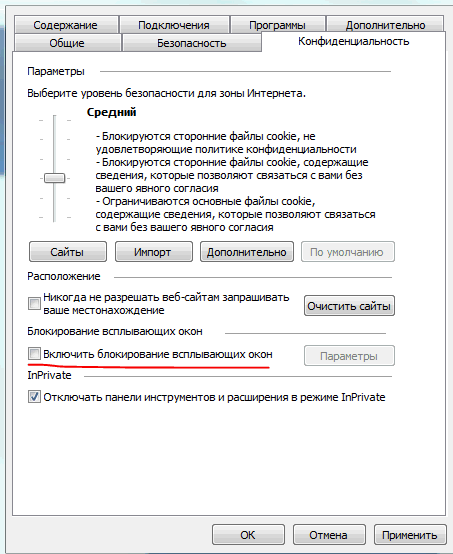


«Уровень безопасности для данной зоны» для надежных узлов должен быть установлен в положение «ниже среднего».

В браузере Internet Explorer для зоны **Надежные узлы** должен быть разрешен запуск ActiveX приложений:



После перейдите во вкладку “Конфиденциальность” и уберите галочку с поля “Включить блокирование всплывающих окон”.



Во время первого запуска браузер может сообщать о блокировке всплывающих окон, при появлении таких надписей выбрать – «Всегда разрешать запуск всплывающих окон с узла», после чего система предложит добавить узел Портала в исключения безопасности, при появлении такого сообщения необходимо подтвердить исключение.

При возникновении сообщений о блокировке всплывающих окон или внутреннего содержания сайта необходимо добавить соответствующие узлы в список доверенных узлов.

## Установка компонента SilverLight

Требуется пройти по ссылке <http://go.microsoft.com/fwlink/?linkid=149156> и установить SilverLight.

## Драйвер носителя электронной подписи

Как правило, драйвер носителя Вашей электронной подписи предоставляется удостоверяющим центром непосредственно при выдаче подписи. Если Вы по каким-либо причинам не получили драйвер, Вы можете загрузить и установить его самостоятельно. Ниже приведены инструкции по установке наиболее часто встречающихся типов носителей – eToken и Rutoken.

Если Вы получили подпись на носителе какого-либо другого типа или не можете определить тип своего носителя, пожалуйста, обратитесь за рекомендациями в техническую поддержку своего удостоверяющего центра.

*Примечание: если Вы получили электронную подпись без носителя (на обычной флешке), драйвер устанавливать* ***не нужно****.*

Для работы с порталом используется квалифицированный сертификат руководителя организации или специального должностного лица, ответственного за реализацию правил внутреннего контроля. Сертификат записывается на персональные идентификаторы (далее – носители). Для работы с Порталом рекомендуется использовать сертифицированные ФСТЭК России носители ключевой информации типа eToken или Rutoken.

Настройка рабочего места пользователя производится в зависимости от типа используемого носителя. Как правило, тип используемого носителя можно определить визуально по надписи на носителе.

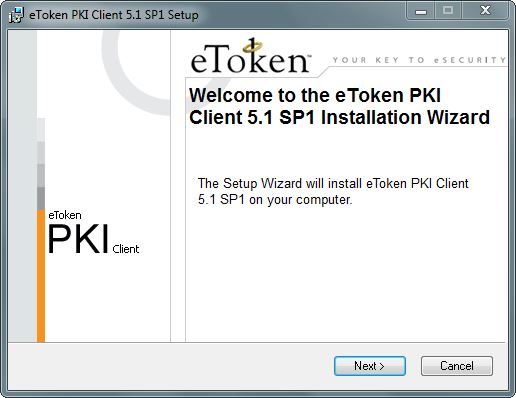
|  |  |
| --- | --- |
| http://www.rutoken.ru/images/content/rutoken_s_max.png | http://www.hwp.ru/Soft/Etoken.winxp/image002.jpg |

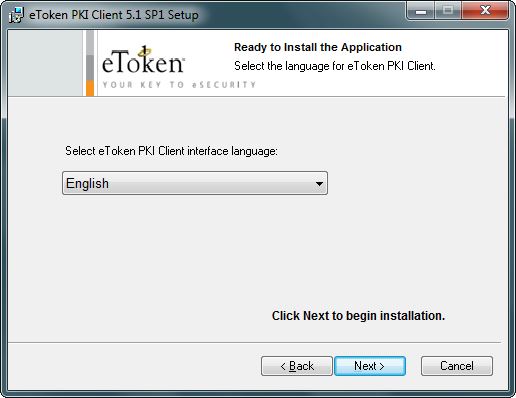
Также тип указывается в документах при получении сертификата электронной подписи. Кроме этого его можно уточнить в удостоверяющем центре, выдавшем сертификат.

### Установка драйвера носителя типа eToken

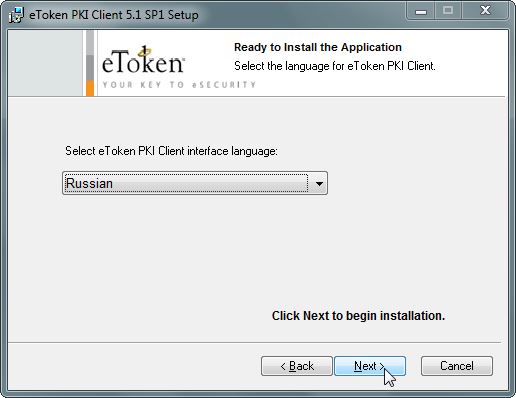
Драйвер для носителей типа eToken называется eToken PKI Client и обычно поставляется в комплекте с eToken, также его можно скачать [здесь](http://www.aladdin-rd.ru/support/downloads/26037/).

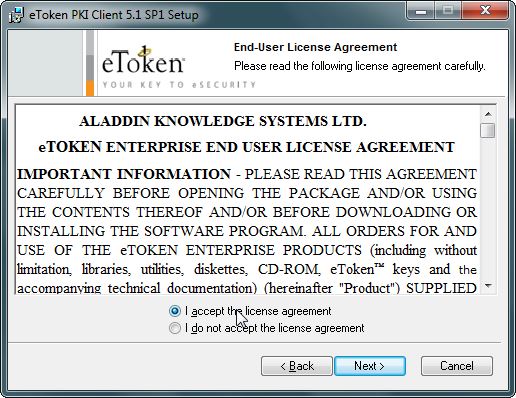
Для установки запустите скачанный файл и следуйте указаниям установщика.



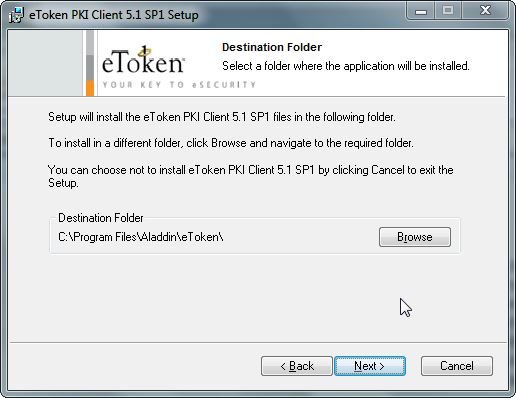


Выберите в списке русский язык и нажмите **Next** для продолжения установки.

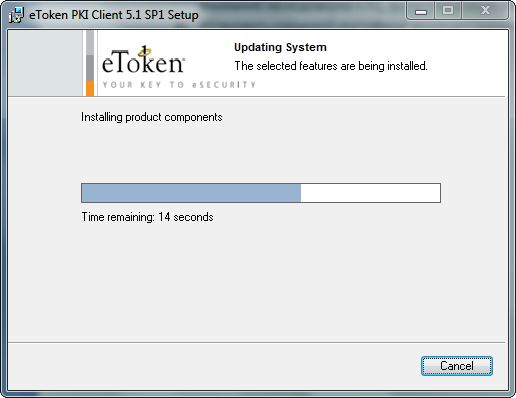


Далее нужно выбрать пункт I accept the license agreement и нажать Next.

На следующем шаге необходимо выбрать папку для установки программного обеспечения либо согласиться с параметрами по умолчанию:



После нажатия Next запустится процесс инсталляции приложения:



по завершении которого установщик завершит свою работу:

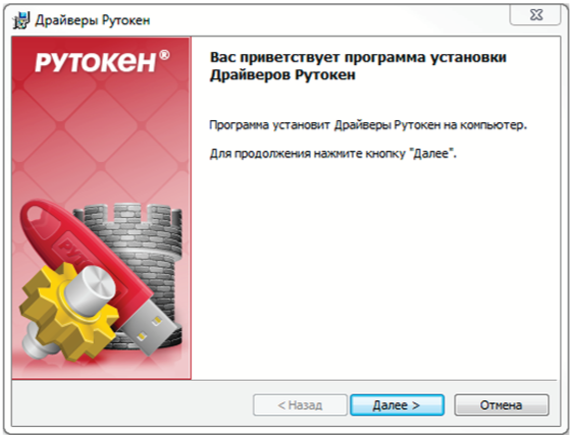


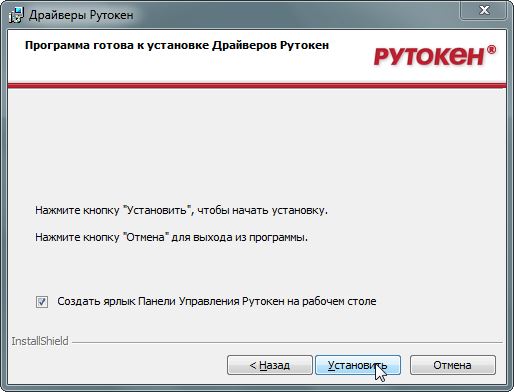
Для выхода из программы установки следует нажать кнопку **Finish**.

### Установка драйвера носителя типа Rutoken

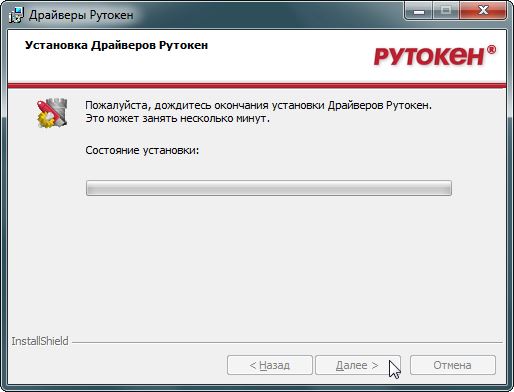
Установочный файл обычно поставляется в комплекте с носителем электронной подписи, также его можно скачать с официального [сайта](http://www.rutoken.ru/support/download/drivers-for-windows/) разработчика.

Запустите скачанный файл и следуйте указаниям установщика.

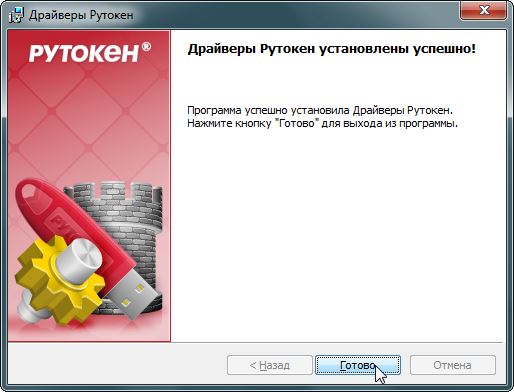




Нажмите **Установить** и подождите завершения установки.



По завершении установки нажмите **Готово**.

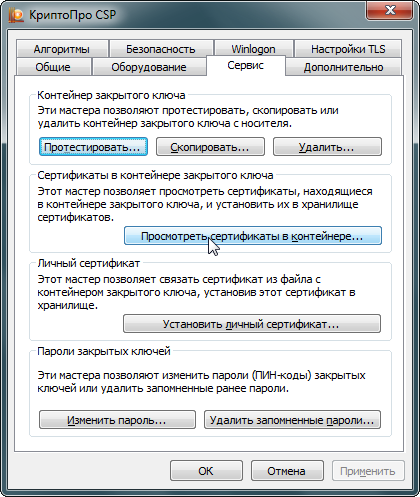


# ****Настройка сертификатов на рабочем месте****

## Сертификат должностного лица организации

Для работы с Порталом Росфинмониторинга необходимо провести установку личного сертификата на Ваш компьютер. Под установкой личного сертификата понимается установка сертификата в хранилище Личные с формированием ссылки на закрытый ключ, соответствующий данному сертификату.

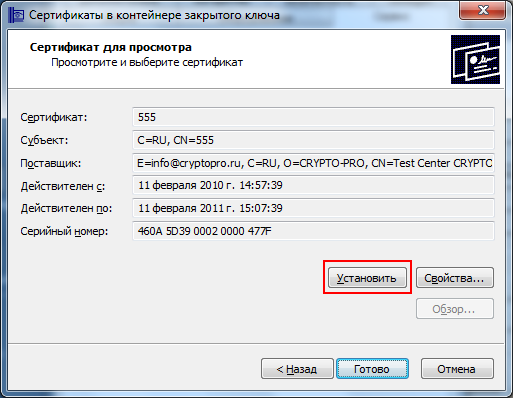
Выполните Пуск ⇒Программы ⇒ КриптоПро ⇒ КриптоПро CSP и перейдите на вкладку Сервис:



и нажмите кнопку **Просмотреть сертификаты в контейнере**. Система отобразит окно «Сертификаты в контейнере закрытого ключа».

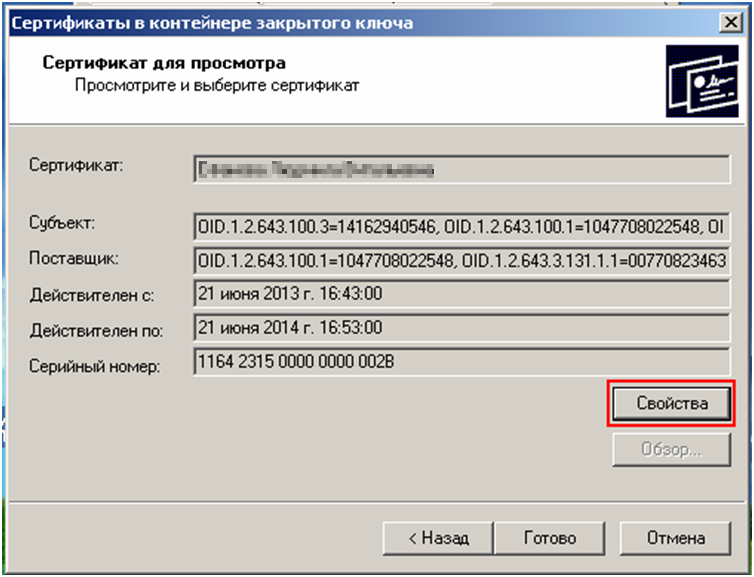


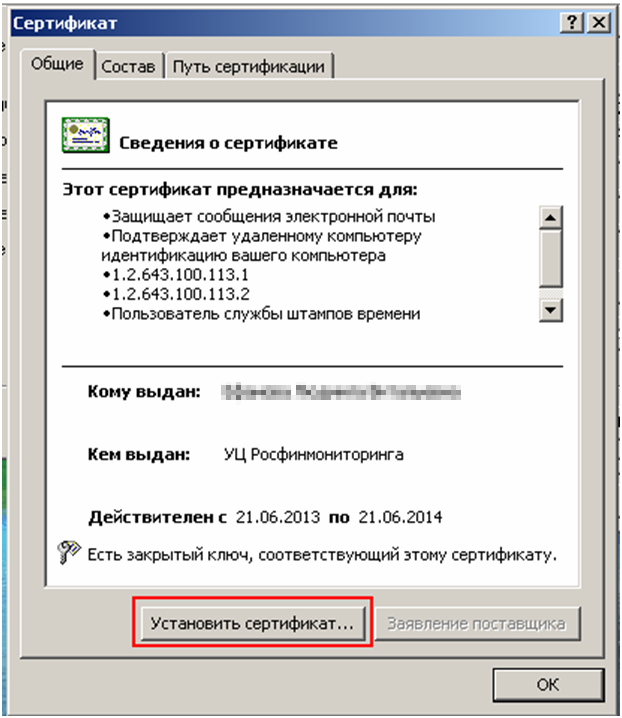
При этом **Имя ключевого контейнера** вводится вручную или выбирается из списка при помощи кнопки **Обзор.** После нажатия кнопки **Далее** система отобразит окно **«Сертификаты в контейнере закрытого ключа»**.



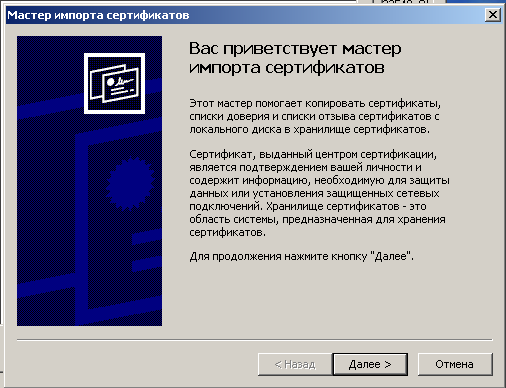
Нажмите кнопку **Установить**. Сертификат будет установлен в хранилище «Личные» текущего пользователя.

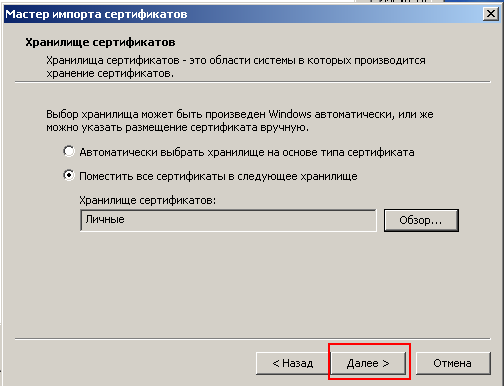
*Примечание: если вы используете Windows XP или Windows Vista, в открывшемся окне может отсутствовать кнопка* ***Установить****. В этом случае следует еще раз нажать* ***Свойства****:*

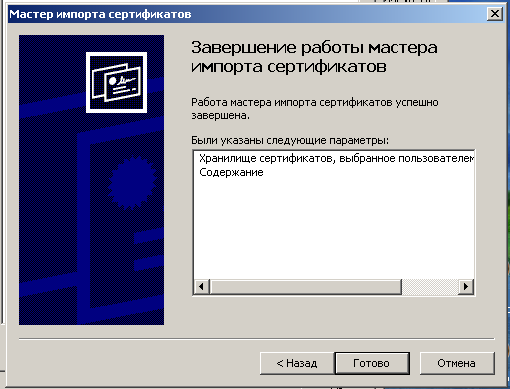




*Дальше следуйте указаниям мастера импорта сертификатов:*









Если сертификат уже есть в хранилище, будет выдано предупреждение о перезаписи прежнего сертификата.



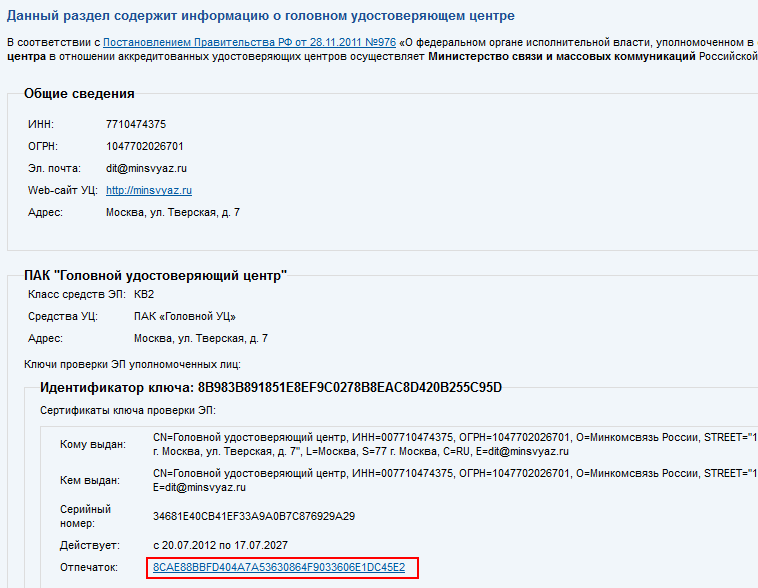
В этом случае следует нажать **Да**.

Более подробная инструкция по установке, настройке и проверке личного сертификата пользователя приведена в [официальной инструкции](http://www.cryptopro.ru/sites/default/files/docs/csp36r3/instruction_csp_r3.pdf) по использованию СКЗИ «КриптоПро CSP».

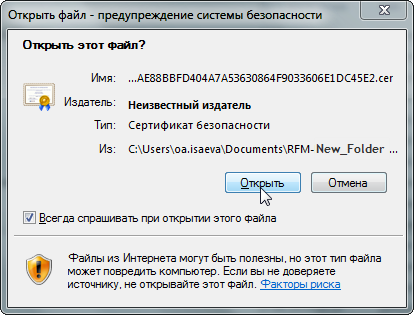
## Корневой сертификат Головного удостоверяющего центра Министерства связи и массовых коммуникаций РФ

Файл сертификата можно скачать [здесь.](http://e-trust.gosuslugi.ru/MainCA)

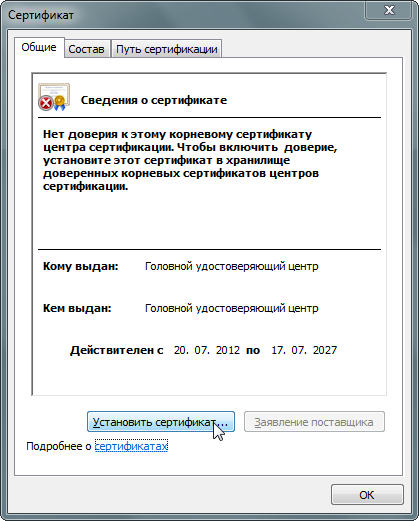
Для скачивания нужно в открывшемся окне нажать на ссылку **Отпечаток**.



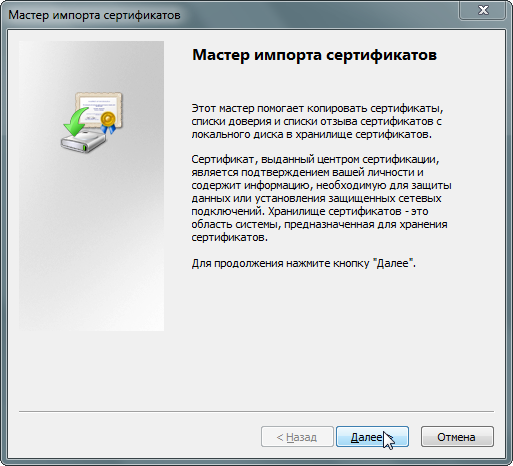
Для запуска процесса установки Вам необходимо дважды щелкнуть левой кнопкой мыши по скачанному файлу корневого сертификата.

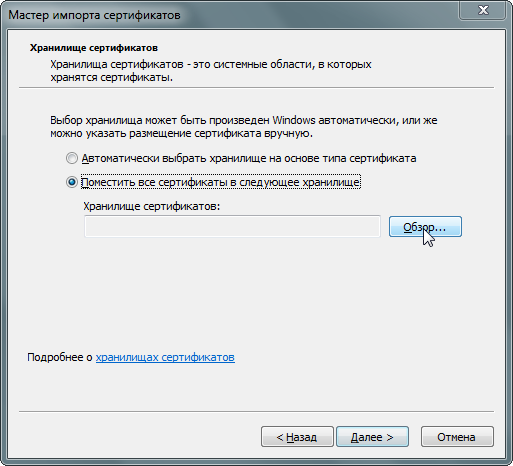


В открывшемся окне свойств сертификата нажмите кнопку **Установить сертификат**.

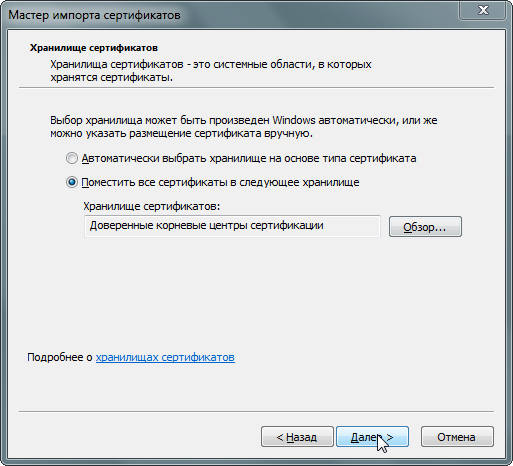


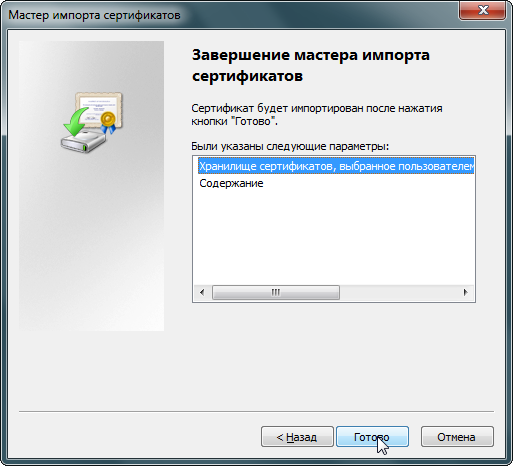
Далее следуйте указаниям мастера импорта сертификатов.

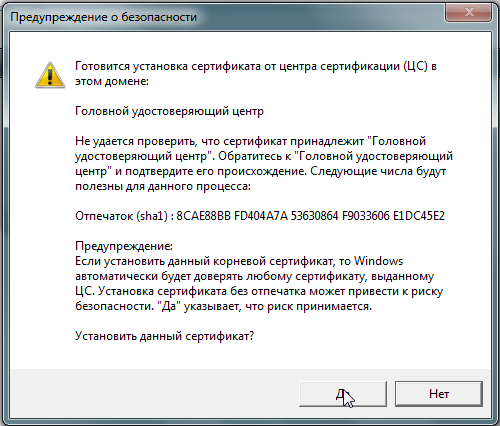


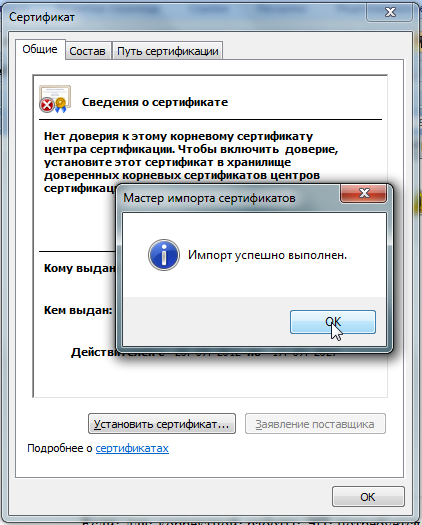


Сертификат следует установить в хранилище **«Доверенные корневые центры сертификации»**.









## Кросс-сертификаты «УЦ 1 ИС ГУЦ» и «УЦ 2 ИС ГУЦ» Министерства связи и массовых коммуникаций РФ

Файлы кросс-сертификатов можно скачать на той же странице, что и корневой сертификат Головного УЦ, а именно <http://e-trust.gosuslugi.ru/MainCA>.

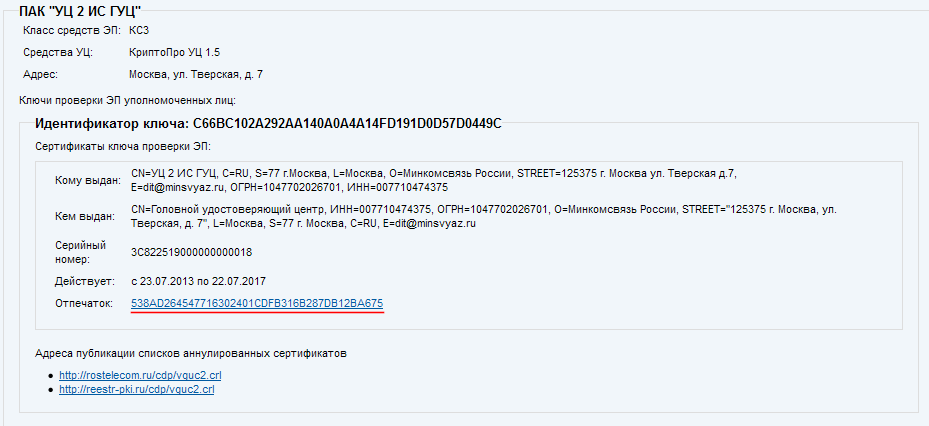
В открывшейся вкладке следует найти раздел ПАК "УЦ 1 ИС ГУЦ" и нажать на ссылку **Отпечаток**:



*Требуется установить все такие же сертификаты* ПАК "УЦ 1 ИС ГУЦ".

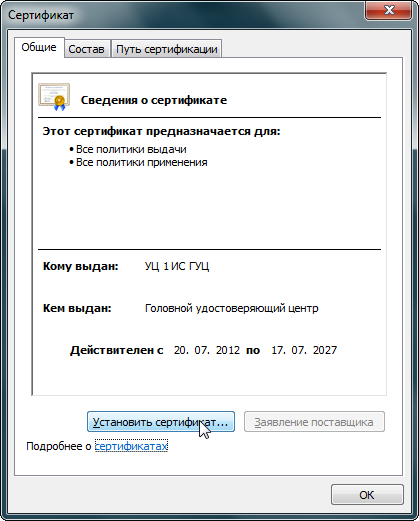
Процесс установки сертификатов производится аналогично пункту 3.5, однако, кросс-сертификаты «УЦ 1 ИС ГУЦ» следует установить в хранилище **«Промежуточные центры сертификации»**.

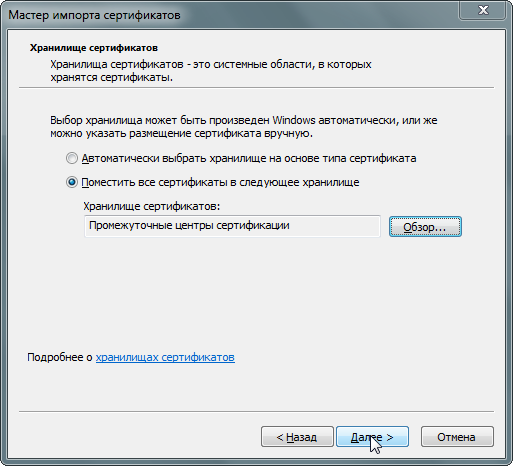
Далее на этой же странице <http://e-trust.gosuslugi.ru/MainCA>. следует найти раздел ПАК «УЦ 2 ИС ГУЦ» и нажать на ссылку **Отпечаток**:



*Требуется установить все такие же сертификаты* ПАК "УЦ 2 ИС ГУЦ".

Установка аналогично ПАК "УЦ 1 ИС ГУЦ".

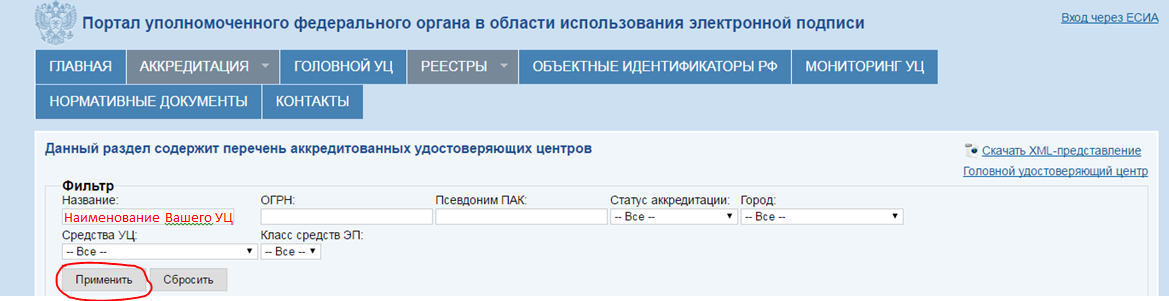




## Кросс-сертификат Вашего удостоверяющего центра.

Кросс-сертификат удостоверяющего центра, выпустившего Вашу электронную подпись, Вы можете самостоятельно скачать с [портала уполномоченного федерального органа в области использования электронной подписи](http://e-trust.gosuslugi.ru/CA).

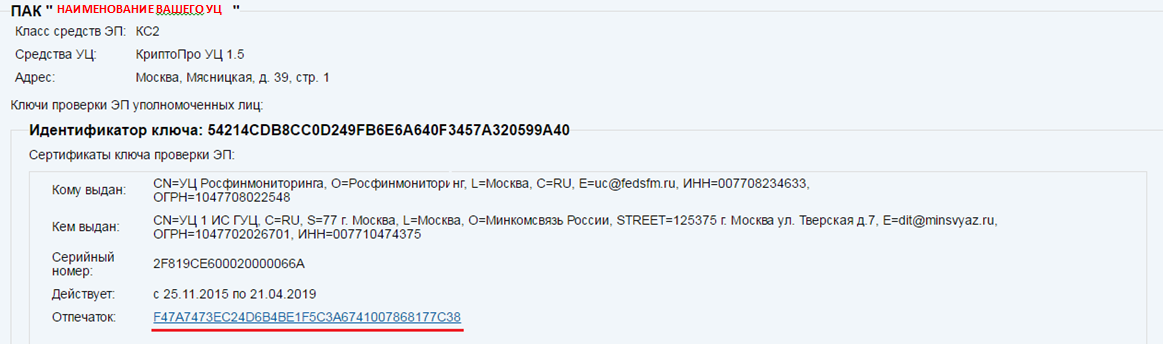
Для этого на открывшейся странице в разделе «Аккредитация» далее «Аккредитованные УЦ» в поле **Название** введите название своего удостоверяющего центра и нажмите **Применить**.



В открывшемся окне с результатами поиска нажмите на значок лупы слева от названия Вашего удостоверяющего центра:



Дождитесь загрузки страницы Вашего удостоверяющего центра на Портале УФО и нажмите на Отпечаток кросс-сертификата Вашего удостоверяющего центра.



*Примечание: если на странице Вашего удостоверяющего центра на Портале УФО указано несколько ПАКов и вы затрудняетесь в выборе правильного, можно скачать и установить все действующие сертификаты. Установку следует производить только в хранилище Промежуточные центры сертификации.*

Для скачивания и установки выбирать следует только тот сертификат, срок действия которого уже наступил и еще не истек:

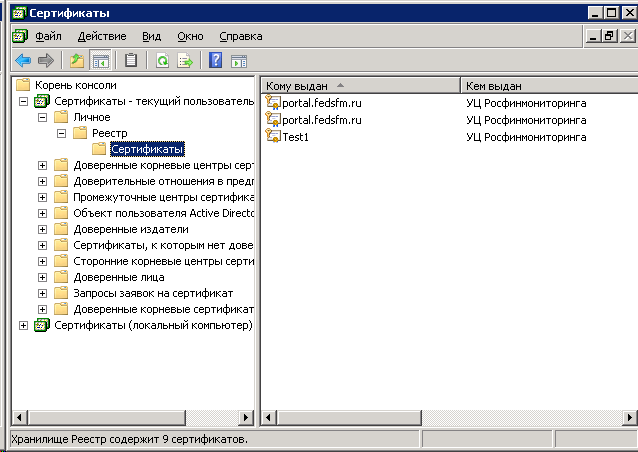


Если на странице у всех кросс-сертификатов Вашего удостоверяющего центра срок действия еще не наступил или уже истек, обратитесь за разъяснениями в техническую поддержку удостоверяющего центра.

Установка кросс-сертификата производится аналогично пункту [3.7](#_Кросс-сертификаты_«УЦ_1), сертификат устанавливается в хранилище «**Промежуточные центры сертификации**».

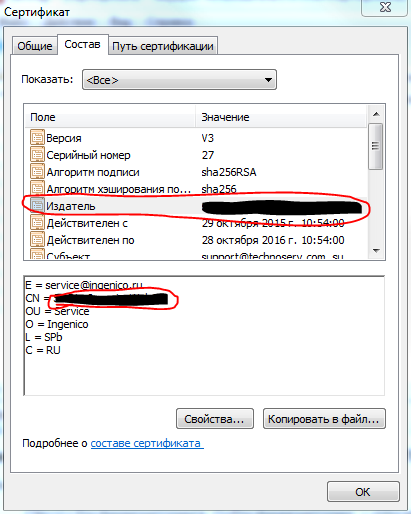
*Примечание: если Вы не знаете, как называется Ваш удостоверяющий центр или не можете найти его в результатах поиска, попробуйте искать по псевдониму ПАКа. Сделать это можно следующим образом:*

*Выполните Пуск – Все программы – КриптоПро – Сертификаты. Откройте вкладку Сертификаты – текущий пользователь – Личное – Реестр – Сертификаты:*

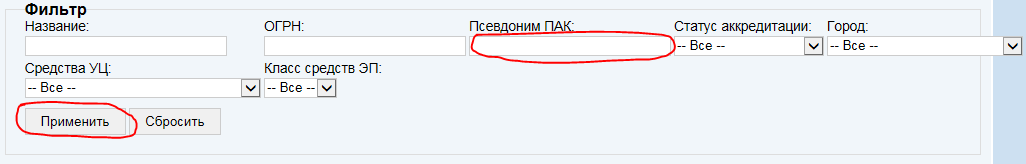


*Дважды щелкните левой кнопкой мыши по строке с Вашим сертификатом и откройте вкладку* ***Состав****.*

*Выберите поле* ***Издатель*** *и скопируйте значение параметра* ***CN****:*



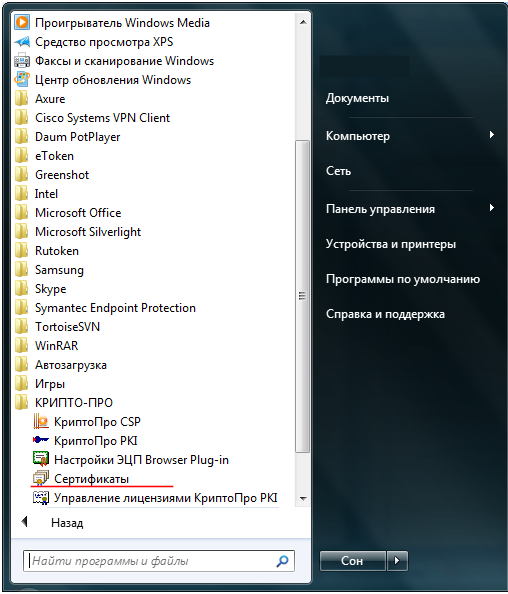
*Вставьте скопированное значение в поле* ***Псевдоним ПАКа*** *на Портале УФО и нажмите* ***Применить****:*



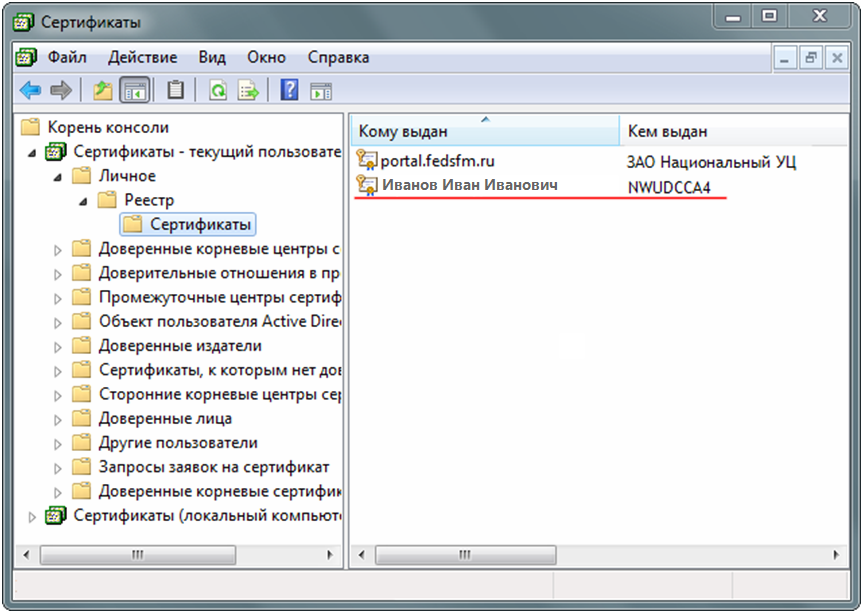
*Если результаты поиска пусты, проверьте, правильно ли вы скопировали значение поля CN и повторите попытку. Если значение скопировано верно, но в результатах поиска по-прежнему ничего не отображается, обратитесь в техническую поддержку своего удостоверяющего центра.*

# Проверка правильности установки сертификатов.

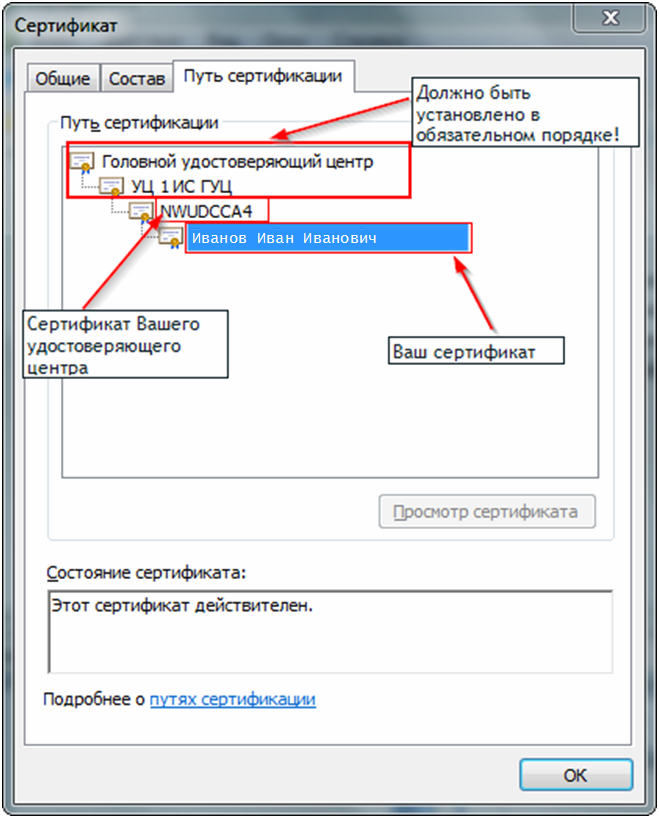
Откройте Пуск – Все программы – КриптоПро – Сертификаты



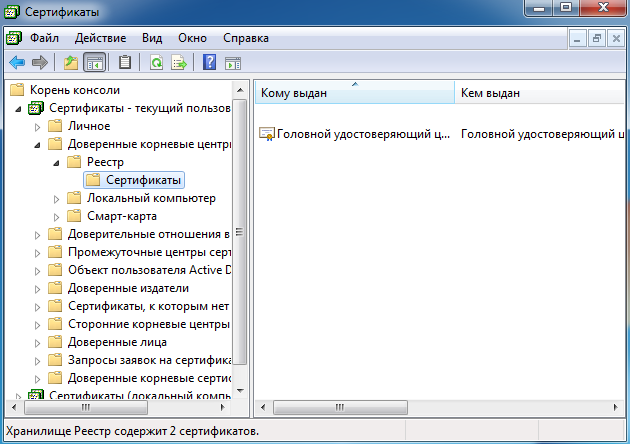
Перейдите на вкладку **Личные** хранилища **Сертификаты – текущий пользователь**:



Дважды щелкните по Вашему сертификату в списке, перейдите на вкладке Путь сертификации и убедитесь, что цепочка выстроена правильно:



Перейдите на вкладку **Доверенные корневые центры** и убедитесь, что в списке присутствует Головной удостоверяющий центр. Если присутствуют корневые сертификаты Вашего удостоверяющего центра, удалите их.



*Примечание: иногда наличие корневого сертификата удостоверяющего центра требуется для корректной работы с другими приложениями, использующими электронную подпись (например, в системах электронного документооборота). В таком случае в операционной системе Windows нужно создать отдельного пользователя с правами администратора или использовать другой компьютер для работы ТОЛЬКО на Портале РФМ и настраивать рабочее место только для этого пользователя в соотвествии с инструкцией.*

Перейдите на вкладку **Промежуточные центры сертификации** и убедитесь, что в списке присутствуют кросс-сертификаты УЦ 1 ИС ГУЦ, УЦ 2 ИС ГУЦ и Вашего удостоверяющего центра.

Если какой-либо из этих параметров не соответствует действительности (наименования нечитаемые, ошибки в названии вашего УЦ или неправильное имя организации либо ФИО сотрудника, которому выдан сертификат), Вам следует обратиться в техническую поддержку Вашего удостоверяющего центра.

Если не помогло, то ВО ВСЕХ ПАПКАХ удалите сертификат Вашего удостоверяющего центра и

повторно установите его в соответствии с инструкцией п. 3.8

(строго в хранилище "Промежуточные центры сертификации")

Если все вышеперечисленные шаги не выявили ошибок настройки, рабочее место пользователя готово для работы с Личным кабинетом на Портале Росфинмониторинга.

Если все вышеперечисленные шаги не помогли, то зарегистрируйте заявку в техническую поддержку через портал https://portal.fedsfm.ru/account/supportpost.aspx, приложив скриншоты следующих вкладок, войдя в программу Пуск -> Все программы -> КриптоПро -> Сертификаты:

Сертификаты - текущий пользователь: 1) Доверенные корневые центры сертификации-> Реестр-> Сертификаты; 2) Промежуточные центры сертификации-> Реестр-> Сертификаты; 3) Личное –> Реестр-> Сертификаты; двойной щелчок по Вашему сертификату – вкладки: а-Общие; б-Путь сертификации; в-Состав-> идентификатор ключа центра сертификатов (кликнуть по нему);

В результате получится 5 скриншотов.