**Данная инструкция предназначена для установки и настройки ЭП, выпущенных при помощи криптопровайдера КриптоПРО CSP**.

Список используемых терминов и определений.

|  |  |
| --- | --- |
| ЭП - | электронная подпись. |
| СКЗИ - | средство криптографической защиты информации |
| Криптопровайдер - | независимый модуль, позволяющий осуществлять криптографические операции в операционных системах [Microsoft](https://ru.wikipedia.org/wiki/Microsoft" \o "Microsoft), управление которым происходит с помощью функций [CryptoAPI](https://ru.wikipedia.org/wiki/CryptoAPI" \o "CryptoAPI) |

**Перед началом настройки ЭП** на рабочем месте в случае использования вновь приобретенного специализированного носителя   
Рутокен Lite/ЭЦП 2.0 необходимо установить [соответствующее программное обеспечение](https://www.rutoken.ru/support/download/get/rtDrivers-exe.html) для вашего носителя.

Для начала установки и настройки ЭП на рабочем месте, требуется скачать и установить СКЗИ КриптоПРО CSP в соответствии [документацией по установке и использованию КриптоПро CSP](https://www.cryptopro.ru/products/cryptopro-csp).

**Установка электронной подписи в хранилище компьютера в КриптоПРО CSP**

1. Подключите к USB-порту компьютера устройство c ЭП.
2. Запустите криптопровайдер КриптоПРО CSP (ПУСК -> КРИПТОПРО   
   -> КриптоПРО CSP) и перейдите во вкладку «*Сервис*». В окне «*Сервис*» кликните «*Просмотреть сертификаты в контейнере…*» (см. рис. 1)

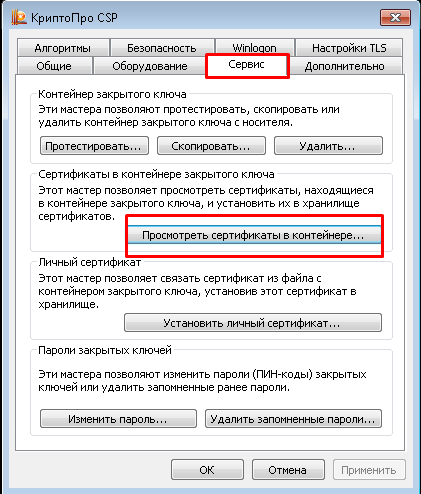


Рис.1 – Установка личного сертификата.

1. В Окне мастера установке личного сертификата кликните на вкладку «*Обзор*» (см. рис. 2)

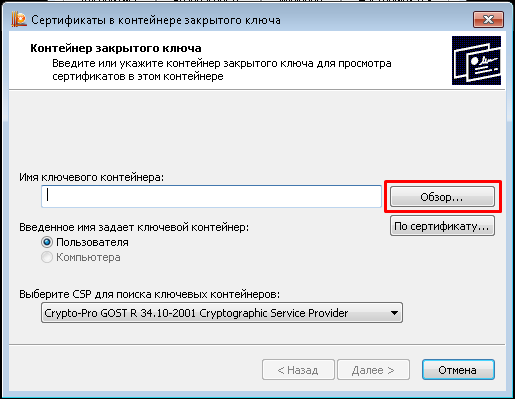


Рис.2 –Выбор контейнера закрытого ключа.

1. В окне выбора ключевого контейнера выберете ваш носитель ЭП\* (см. рис. 3) и затем нажмите «*ОК*»

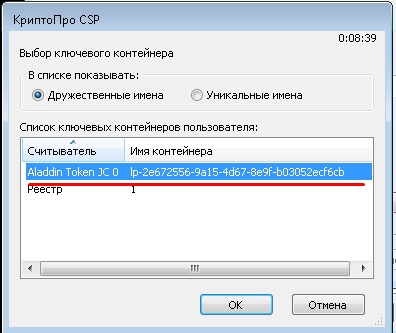


Рис.3 –Выбор ключевого контейнера.

\*В разделе «Считыватель» будет находиться наименование вашего носителя

(JaCarta, RuToken, eToken и пр.)

1. После выбора ключевого контейнера его имя должно отобразиться в строке «Имя ключевого контейнера» (см. рис 4), затем нажмите «Далее».

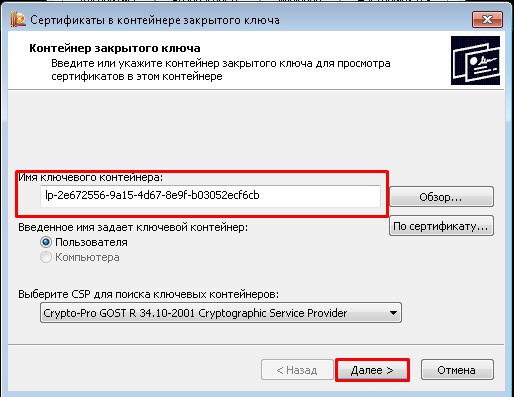


Рис.4 –Выбор контейнера закрытого ключа.

1. В окне «Сертификат для просмотра» кликните «Свойства» (см. рис5)

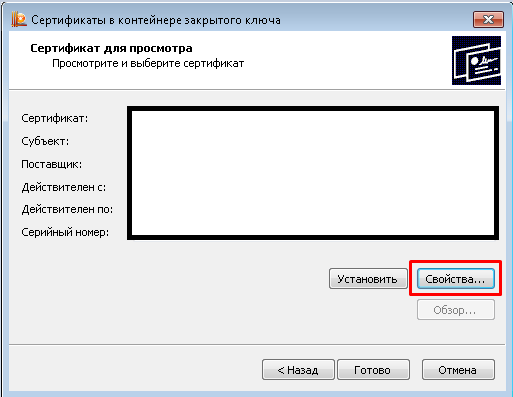


Рис.5 – Просмотр сертификата.

1. В открывшемся окне нажмите кнопку «Установить сертификат» (см. рис 6)

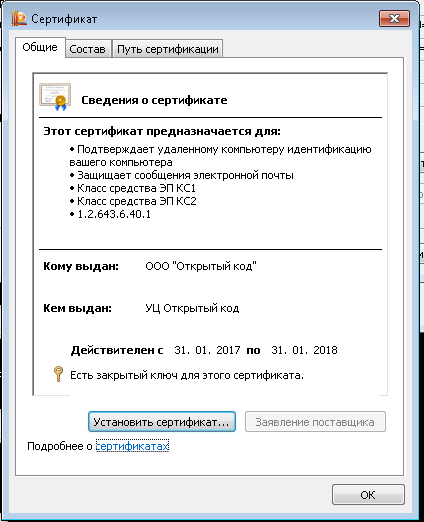


Рис.6 –Просмотр сертификата.

1. Запустится Мастер установки сертификатов (см.рис 7). Нажмите «Далее».

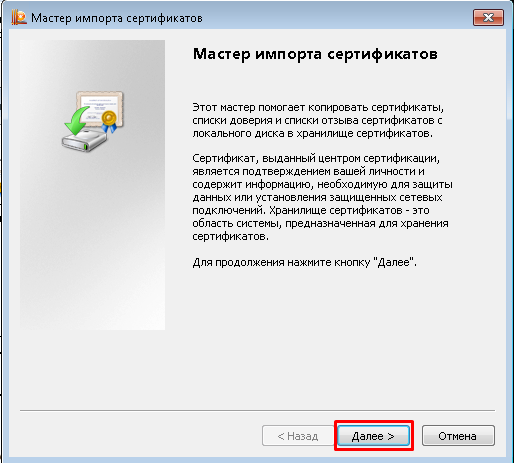


Рис.7 –Мастер импорта сертификатов.

1. В открывшемся окне установите радиоточку «Автоматически выбрать хранилище на основе типа сертификата» (см. рис 9) и нажмите «Далее».

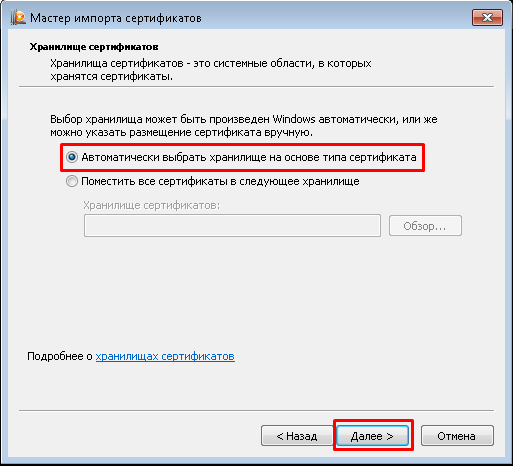


Рис.9 – Выбор хранилища сертификатов.

1. В открывшемся окне нажмите кнопку «Готово».
2. **Установка корневого сертификата УЦ «Открытый код» и списка аннулированных сертификатов.**
3. Перейдите по ссылке:

<http://www.o-code.ru/services/informationsecurity/signaturecenter/root_sertificat/>

1. На открывшемся сайте необходимо развернуть рамку:   
   первая строчка – для сертификатов, выпущенных до 10.01.2020  
   вторая строчка – для сертификатов, выпущенных после 10.01.2020

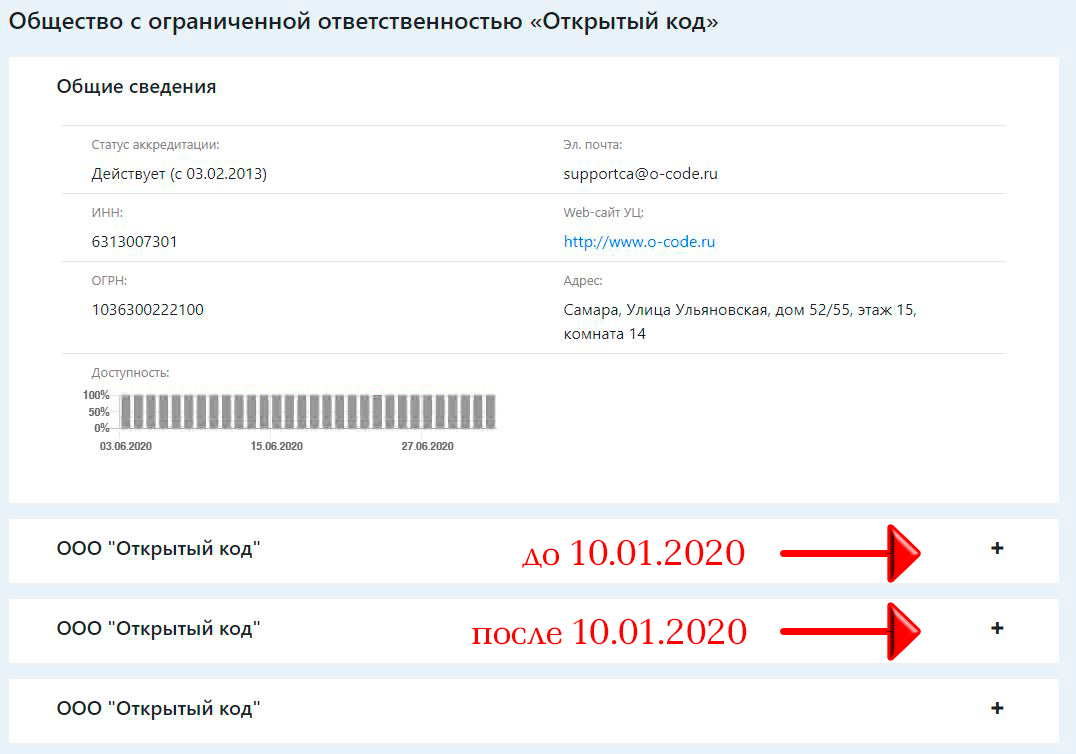


Рис.10 - Окно скачивания корневого сертификата и списка отозванных сертификатов.

1. В открывшейся рамке скачайте (одинарным кликом) **Отпечаток** (по клику скачается корневой сертификат). Под подзаголовком «**Адреса публикации списков аннулированных сертификатов»** необходимо выбрать любую ссылку из двух предложенных, по одинарному клику по ссылке скачается список аннулированных сертификатов.

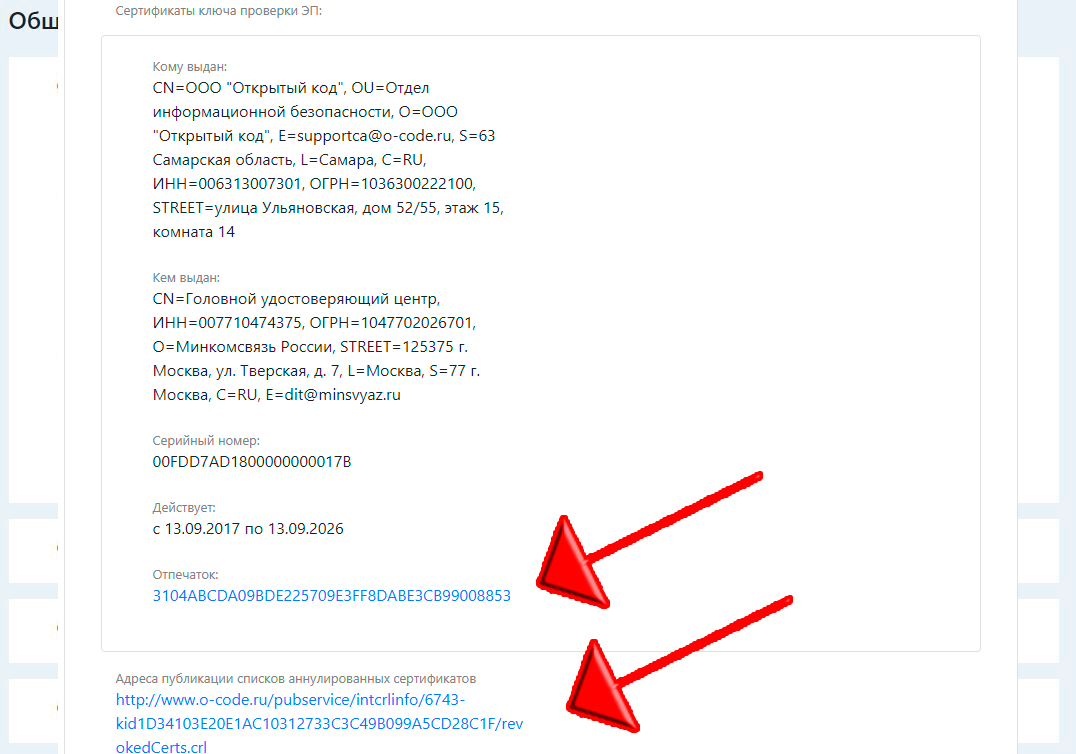


Рис.11 - Окно скачивания корневого сертификата и списка отозванных сертификатов.

1. Кликните правой кнопкой по скачанному файлу revokedCert.crl (П.3) – найти его можно в директории «**Загрузки**». В выпавшем списке выберите «*Установить список отзыва*» (см.рис 12)

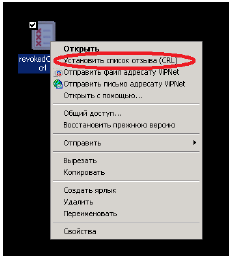


Рис.12 - Установка списка отзыва.

1. В окне Мастера импорта сертификатов нажмите «*Далее*» (Рис.13)

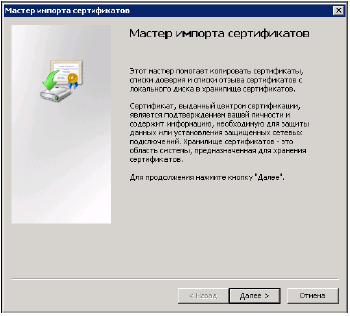


Рис.13 - Мастер импорта сертификатов.

1. В окне выбора места хранения проверьте наличие радиоточки в пункте «*Автоматически выбрать хранилище на основе типа сертификата*» и нажать «*Далее*» (Рис.14)

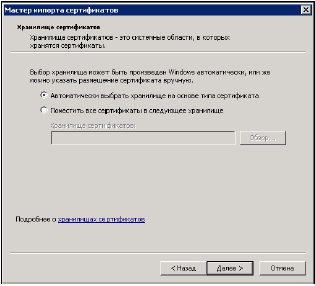


Рис.14 - Мастер импорта сертификатов.

1. В окне Завершения мастера импорта сертификатов нажмите «Готово»
2. Перейдите к директории, куда был сохранен корневой сертификат («**Загрузки»**). Необходимо кликнуть правой кнопкой мыши по файлу с именем CE703E7CB8647BECE9F6613665C1613D1EA05CF4.cer (либо с именем E0C704A198EB24ED4375B8CD9CD0660E603FEBEA.cer) и в выпавшем списке выберите «*Установить сертификат*» (рис.14)

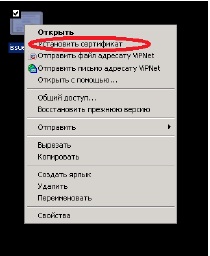


Рис.15 – Установка корневого сертификата.

1. В открывшемся окне мастера импорта сертификатов нажмите «*Далее*». В окне выбора места хранилища сертификатов (Рис.15) установите радиоточку в положение «*поместить все сертификаты в следующее хранилище*» и нажмите кнопку «*Обзор*» (Рис.16)

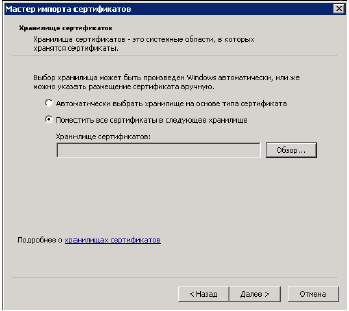


Рис.16 – Установка корневого сертификата.

1. В окне выбора хранения сертификата выберите «*промежуточные центры сертификации*» и нажмите «*ОК*» (Рис.17).

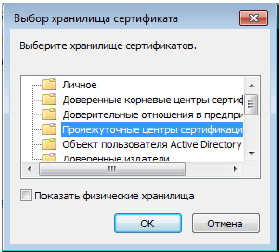


Рис.17 – Выбор места хранения корневого сертификата.

1. В окне завершения мастера импорта сертификатов нажмите «*Готово*»
2. **Корневой сертификат Головного удостоверяющего центра Министерства связи и массовых коммуникаций РФ**
3. Файл корневого сертификата и списки аннулированных сертификатов можно скачать по ссылке:

<https://e-trust.gosuslugi.ru/#/portal/mainca>

1. Из списка необходимо выберите «**ПАК Минкосвязь России»**

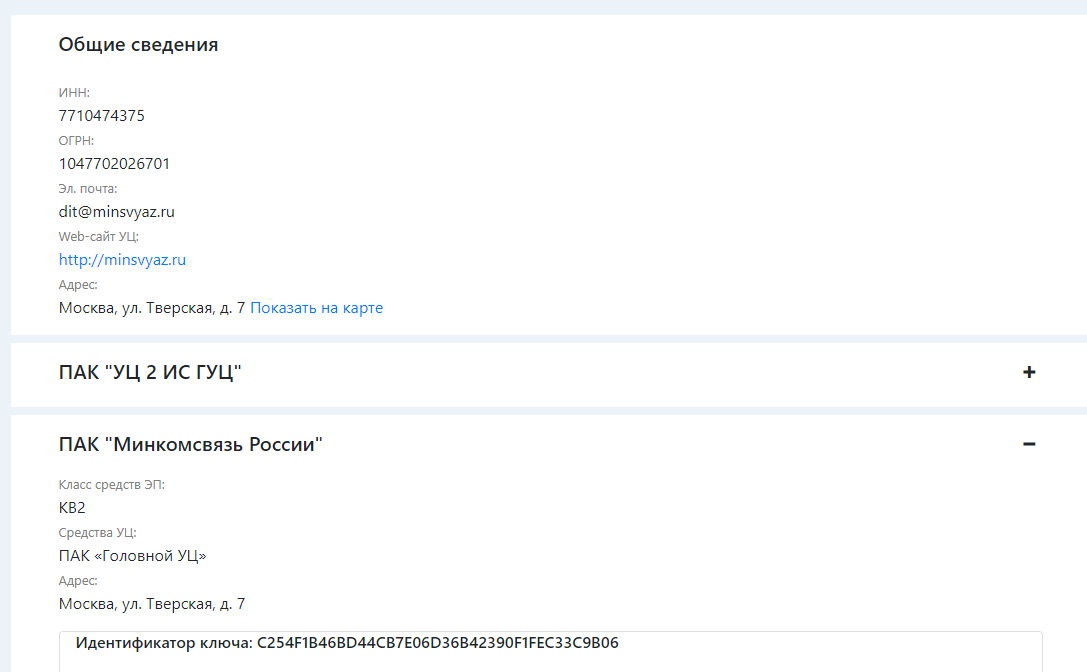


Рис.18 – Окно скачивания корневого сертификата и списка отозванных сертификатов.

1. На странице необходимо скачать Корневой сертификат и Список аннулированных сертификатов – скачивание можно осуществить одинарным кликом (рис. 19)

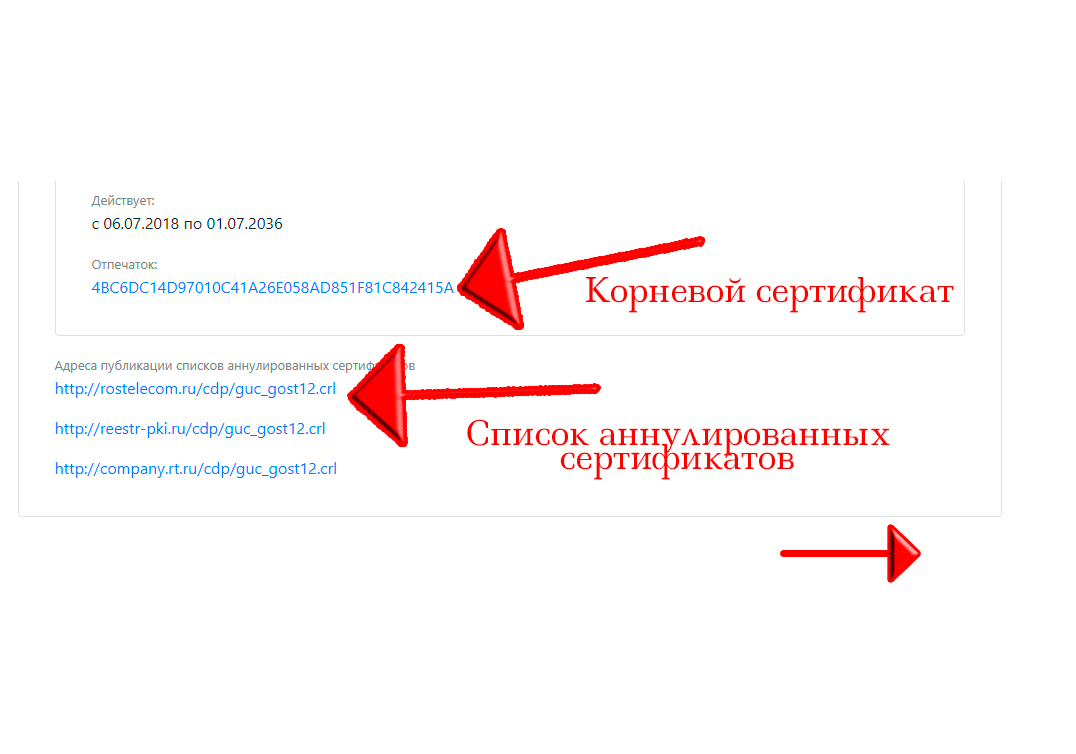


Рис.19 – Окно скачивания корневого сертификата и списка отозванных сертификатов.

1. Для запуска процесса установки корневого сертификата необходимо найти скачанный файл (имя файла 4BC6DC14D97010C41A26E058AD851F81C842415A.cer), Дважды щелкните левой кнопкой мыши по скачанному файлу корневого сертификата

(Рис. 20)

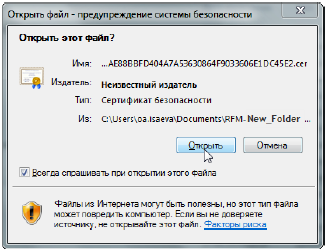


Рис.20 – Установка корневого сертификата Головного удостоверяющего центра Министерства связи и массовых коммуникаций РФ

1. В открывшемся окне свойств сертификата нажмите кнопку «*Установить* *сертификат*» (Рис. 21)

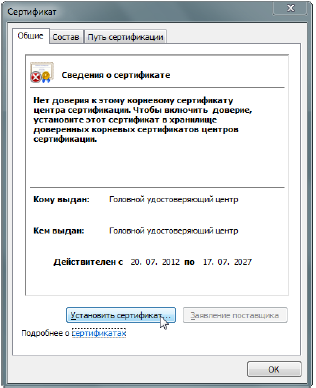


Рис.21 – Установка корневого сертификата Головного удостоверяющего центра.

1. В открывшемся окне мастера импорта сертификатов нажмите «*Далее*». В окне выбора места хранилища сертификатов установите радиоточку в положение «поместить все сертификаты в следующее хранилище» и нажмите кнопку «Обзор» (Рис.15)
2. Установите Сертификат в хранилище **«Доверенные корневые центры сертификации»** (Рис. 22).

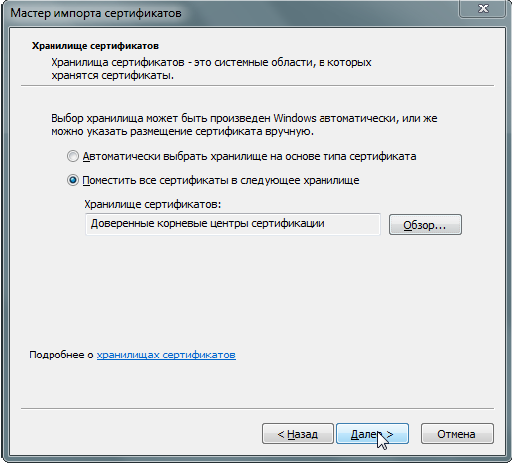


Рис.22 – Установка корневого сертификата.

1. В окне завершения мастера импорта сертификатов нажмите «*Готово*».
2. В диалоговом окне предупреждения о безопасности нажмите «*Да*» (Рис.23).

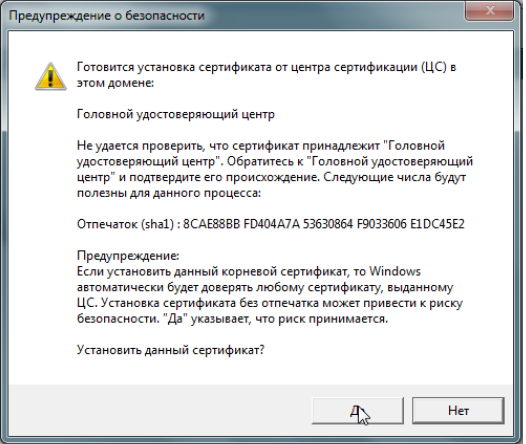


Рис.23 – Установка корневого сертификата.

1. Кликните правой кнопкой по скаченному файлу списка аннулированных сертификатов (П.3) В выпавшем списке выберите *Установить список отзыва* (Рис. 11)
2. В окне Мастера импорта сертификатов нажмите «Далее» (Рис.12)
3. В окне выбора места хранения проверьте наличие радиоточки в пункте «*Автоматически выбрать хранилище на основе типа сертификата*» и нажмите «*Далее*» (Рис.13)
4. В окне Завершения мастера импорта сертификатов нажмите «*Готово*»