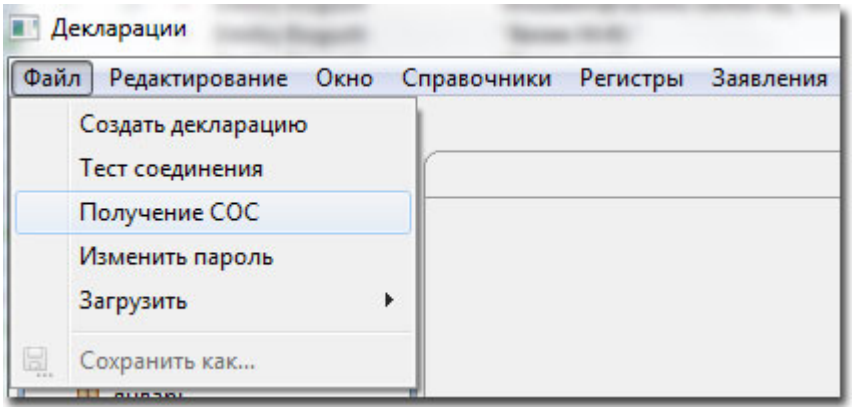
Импорт списка отозванных сертификатов

Список отозванных сертификатов (СОС) можно обновить двумя способами:

I. Через программу **АРМ "Плательщик" (Edeclaration):**

- Запустить программу АРМ "Плательщик".
- Выбрать пункт меню "**Файл**" - "**Получение СОС**" (для загрузки СОС необходимо Интернет-соединение):



- Нажать кнопку **"Ок"**.

II. При помощи программы **"Персональный менеджер сертификатов Авест":**

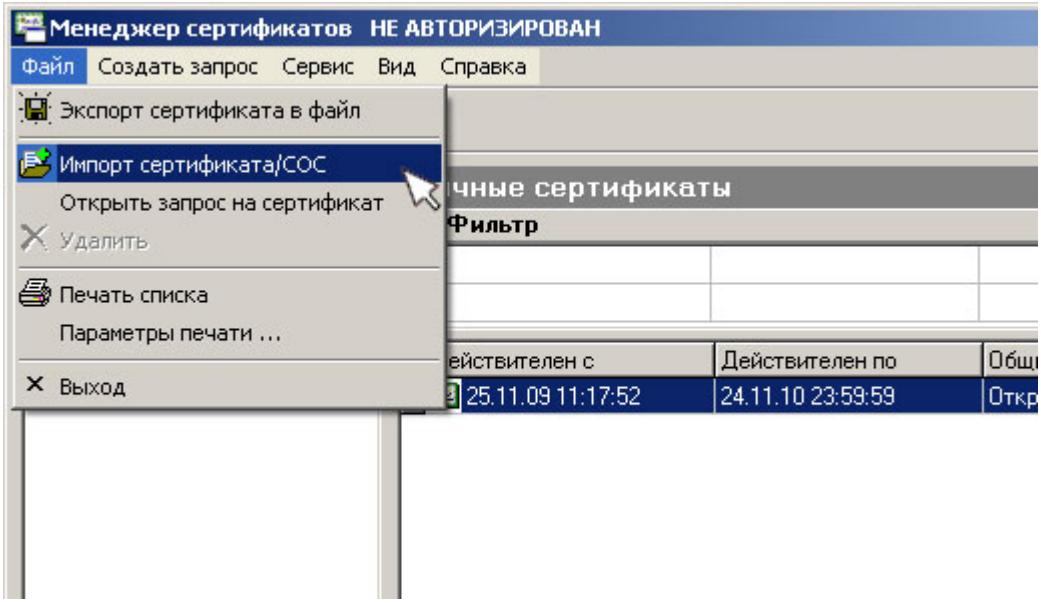
Если на компьютере установлено другое криптографическое ПО (ФСЗН, Клиент-Банк), необходимо убедиться, что импорт СОС производится в нужный персональный менеджер (который по умолчанию находится в директории **C:\Program Files\Avest\AvPCM_MNS**).

Чтобы проверить ярлык программы на рабочем столе, нужно выделить его правой кнопкой мыши, в контекстном меню выбрать «Свойства». Далее в открывшемся окне проверить строки **«Объект»** (должно быть **C:\ProgramFiles\Avest\AvPCM_MNS\MngCert.exe**) и **«Рабочая папка»** (должно быть **C:\ProgramFiles\Avest\AvPCM_MNS**).

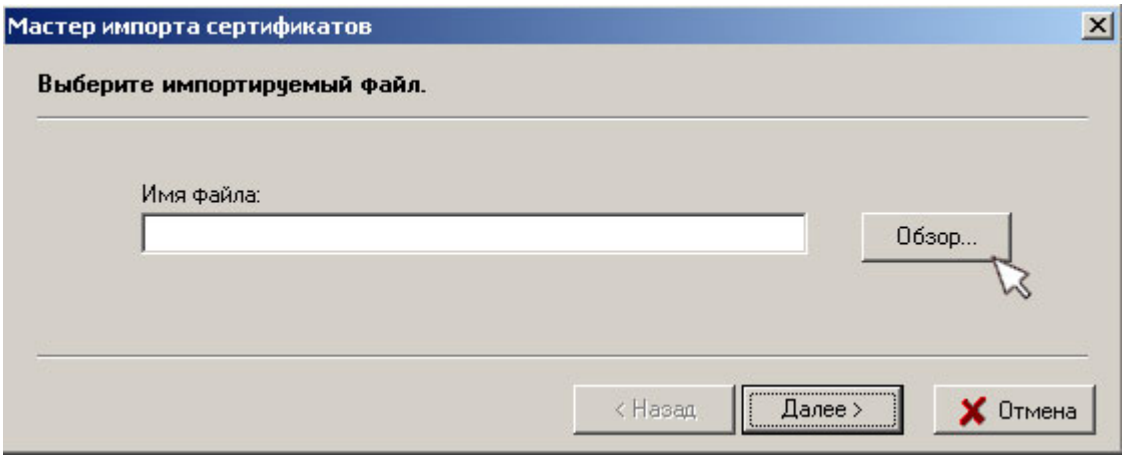
1. В браузере открыть страницу с сертификатами.
2. Загрузить на компьютер 3 файла СОС (КУЦ МНС, ПУЦ МНС, КУЦ РУП).
3. Открыть "Персональный менеджер сертификатов Авест" (войти без авторизации, поставив галку напротив записи «Войти в систему без авторизации»):

- при помощи ярлыка на рабочем столе;
- «Пуск» → « Программы» → «Авест» → «Персональный менеджер сертификатов Авест»;
- запустить персональный менеджер непосредственно из рабочей папки (**C:\Program Files\Avest\AvPCM_MNS\MngCert.exe**).

4. В меню «**Файл**» выбрать «**Импорт сертификата/COC**»:

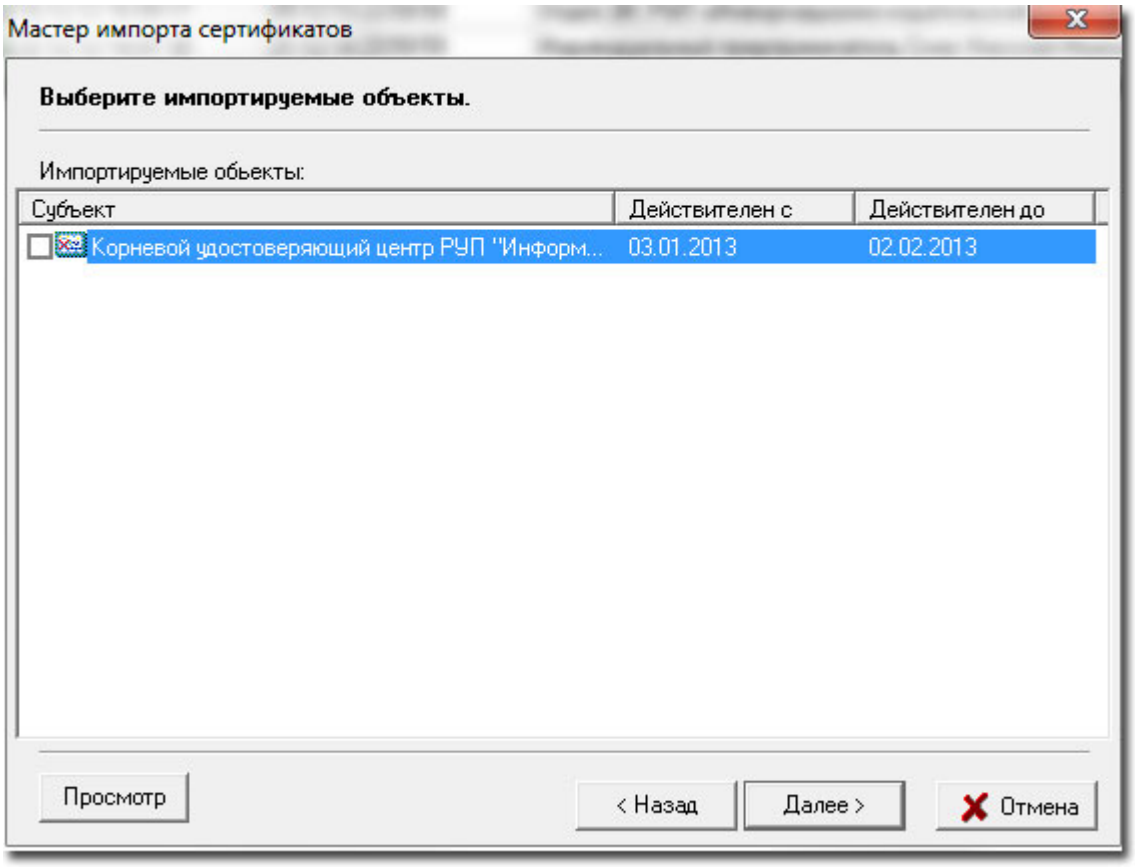


5. В открывшемся окне «**Мастер импорта сертификатов**» нажать «**Обзор**»:

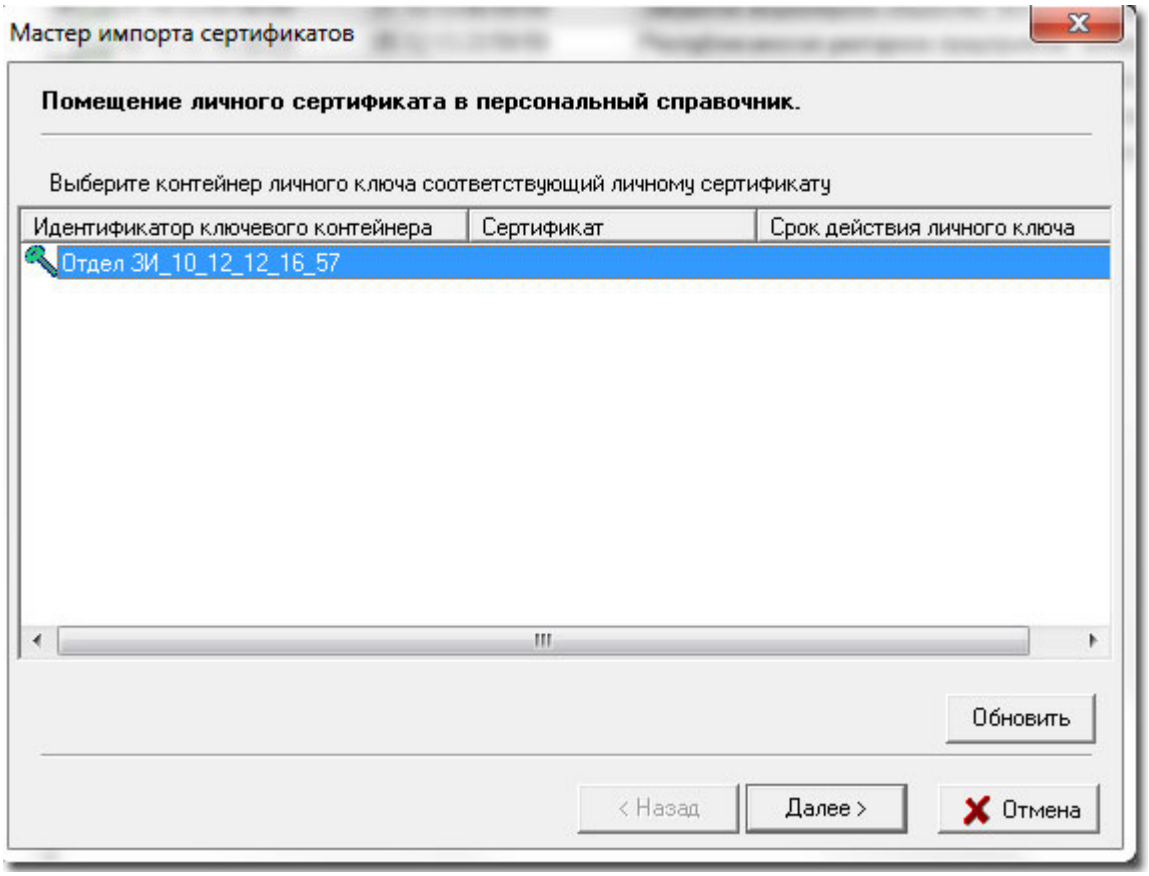


6. Открыть папку, в которую были сохранены 3 файла COC, выбрать один из этих файлов и нажать кнопку **"Открыть"**.

7. В следующем окне «**Мастера импорта сертификатов**» отобразится список импортируемых сертификатов. Нажать "**Далее":**



8. На следующем шаге нужно вставить Ваш USB-ключ (AvToken/AvPass/Ikey) в USB разъем и нажать **"Далее"**.
9. Далее выбрать контейнер:



10. Система запросит пароль доступа к контейнеру. Необходимо ввести пароль (который был введен Вами в регистрационном центре при создании данного сертификата) и нажать «**ОК**».
11. На следующем шаге устанавливается доверие сертификату корневого УЦ. Нажать «**Далее**» и «**ОК**».
12. Пункты 4-11 повторить для каждого из трех файлов СОС.