

Инструкция для Уполномоченного лица

1 ПОДГОТОВКА К РАБОТЕ

1.1 УСТАНОВКА КРИПТОПРО CSP

Перед началом работы необходимо выполнить установку программного обеспечения КриптоПро CSP и выполнить установку сертификата с носителя ключевой информации в личное хранилище сертификатов пользователя. Для установки необходим дистрибутив КриптоПро CSP 3.6.

Необходимо выполнить следующие действия:

- запустить дистрибутив КриптоПро CSP 3.6. Откроется форма приветственного сообщения (Рисунок 1);

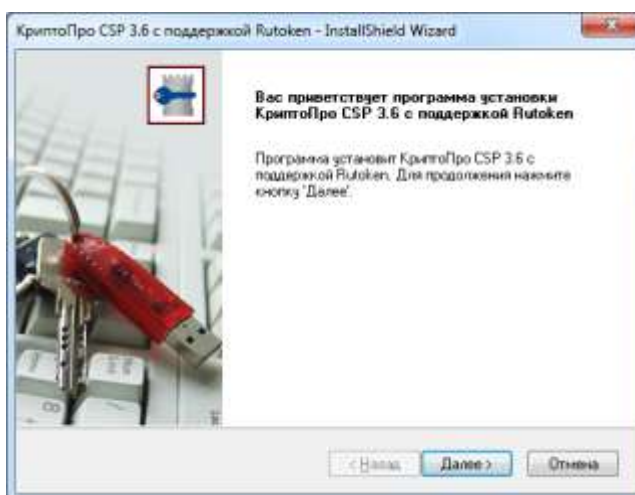


Рисунок 1 – Приветственное сообщение

- нажать кнопку «Далее (Next)». Откроется форма подтверждения начала установки (Рисунок 2);

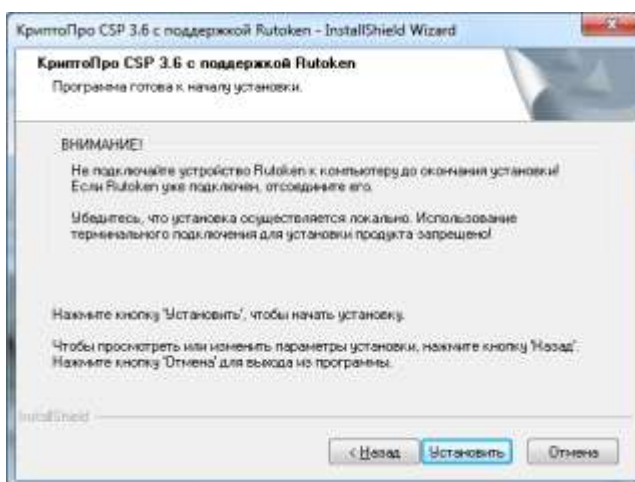


Рисунок 2 – Подтверждения начала установки

- нажать кнопку «**Установить**». Начнется установка дистрибутива КриптоПро CSP 3.6 (Рисунок);

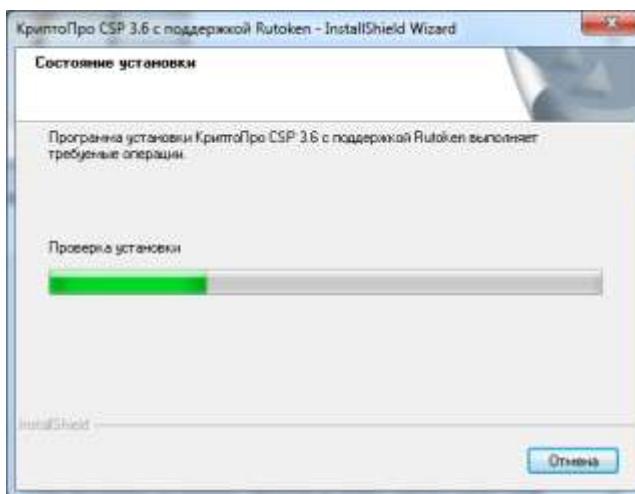


Рисунок 3 – Процесс установки дистрибутива КриптоПро CSP 3.6

После окончания установки откроется форма завершения установки с установленным признаком необходимости перезагрузки компьютера (**Ошибка! Источник ссылки не найден.**).

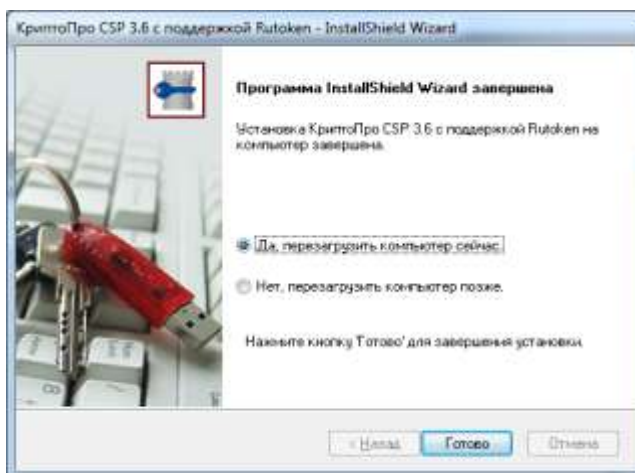


Рисунок 4 – Форма завершения установки

- установить признак «**Да, перезагрузить компьютер сейчас**» и нажмите на кнопку «**Готово**».

Будет произведена перезагрузка компьютера. После перезагрузки установка КриптоПро CSP 3.6 будет завершена.

Затем необходимо выполнить следующие действия для импорта сертификата в личное хранилище пользователя:

- подключить носитель ключевой информации с контейнером закрытого ключа ЭП к USB-разъёму АРМ;

– в меню **Пуск – Все программы – Крипто-Про** выбрать утилиту **КриптоПро CSP**. Откроется форма утилиты на вкладке **«Общие»**. Перейти на вкладку **«Сервис»** (Рисунок 5);

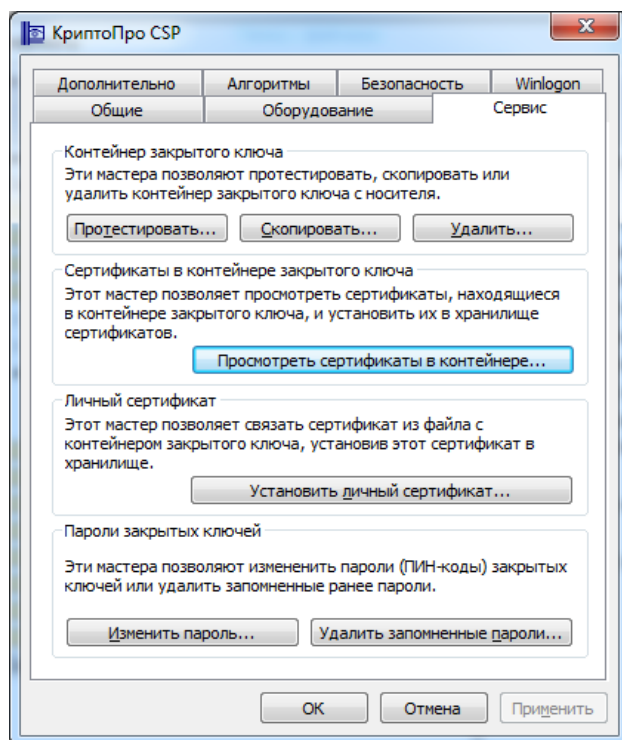


Рисунок 5 - КриптоПро CSP

– нажать кнопку **«Просмотреть сертификаты в контейнере»**. Откроется форма выбора контейнера закрытого ключа (Рисунок 6);

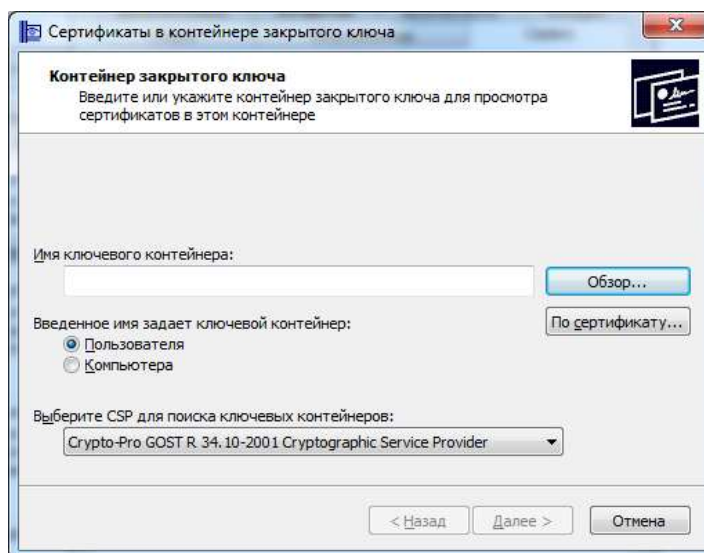


Рисунок 6 - Выбор контейнера закрытого ключа ЭП

– нажать кнопку **«Обзор»**. Откроется форма выбора ключевого контейнера (Рисунок 7);

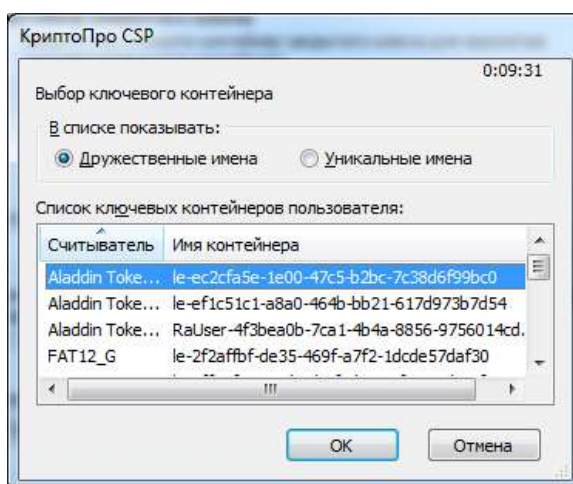


Рисунок 7 - Выбор ключевого контейнера

- выбрать контейнер и нажать кнопку «**ОК**». Затем нажать кнопку «**Далее**». Откроется форма просмотра данных сертификата ЭП (Рисунок 8);

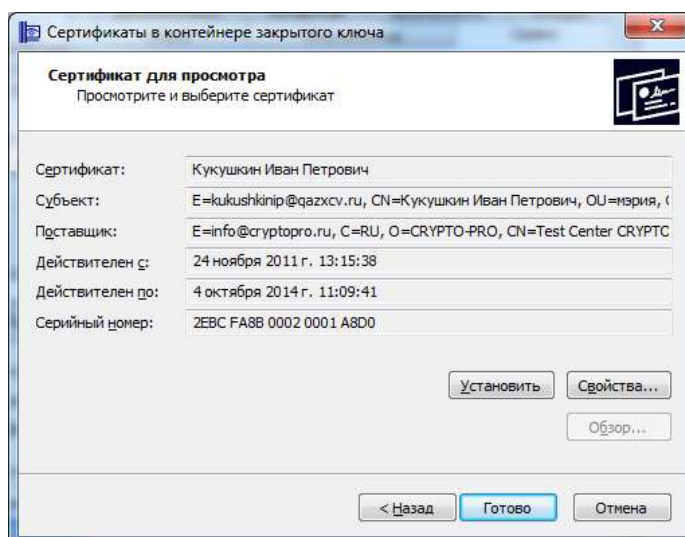


Рисунок 8 - Данные сертификата ЭП

- нажать кнопку «**Установить**». Откроется форма с сообщением об успешной установке сертификата (Рисунок 9);

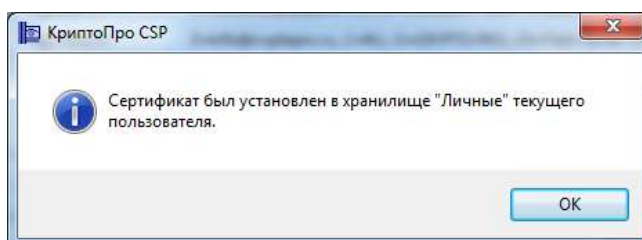


Рисунок 9 - Успешное завершение установки сертификата

- нажать кнопку «**ОК**». Затем нажать кнопку «**Готово**». Установка электронной подписи завершена.

1.2 НАСТРОЙКА БРАУЗЕРА

Перед началом работы необходимо выполнить следующие настройки браузера. Работа с Системой может осуществляться в любом из следующих браузеров:

- Internet Explorer версии не ниже 8;
- Mozilla Firefox версии не ниже 11;
- Google Chrome версии не ниже 18.0.1025.

Описанные настройки должны быть выполнены на всех рабочих местах перед началом работы с Системой.

Mozilla Firefox и Google Chrome используют настройки Internet Explorer. Поэтому достаточно один раз задать настройки для Internet Explorer (который входит по умолчанию в состав установочного пакета поддерживаемых Системой операционных систем), после чего можно использовать предпочитаемый браузер из вышеперечисленного списка.

Для настройки Internet Explorer нужно выполнить следующие операции:

- открыть в браузере сайт Автоматизированной системы «Система массовой выдачи сертификатов ключей подписи» (СМВ) набрав в адресной строке *smv.mos.ru*;
- выбрать в меню браузера «Сервис» пункт «Свойства обозревателя» и открыть вкладку «Безопасность» (Рисунок 7);

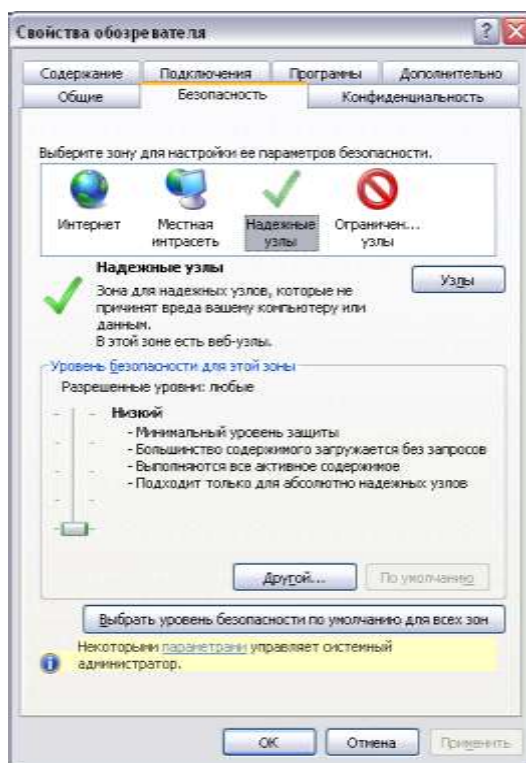


Рисунок 7 - Настройка обозревателя

- добавить адрес портала в список надежных узлов:
 - выбрать зону безопасности «**Надежные узлы**» и нажать кнопку **Узлы**;
 - в открывшемся окне (Рисунок 8) снять галочку «**Для всех узлов этой зоны требуется проверка серверов (https:)**» и нажать кнопку **Добавить** справа от поля «**Добавить в зону следующий узел:**»;

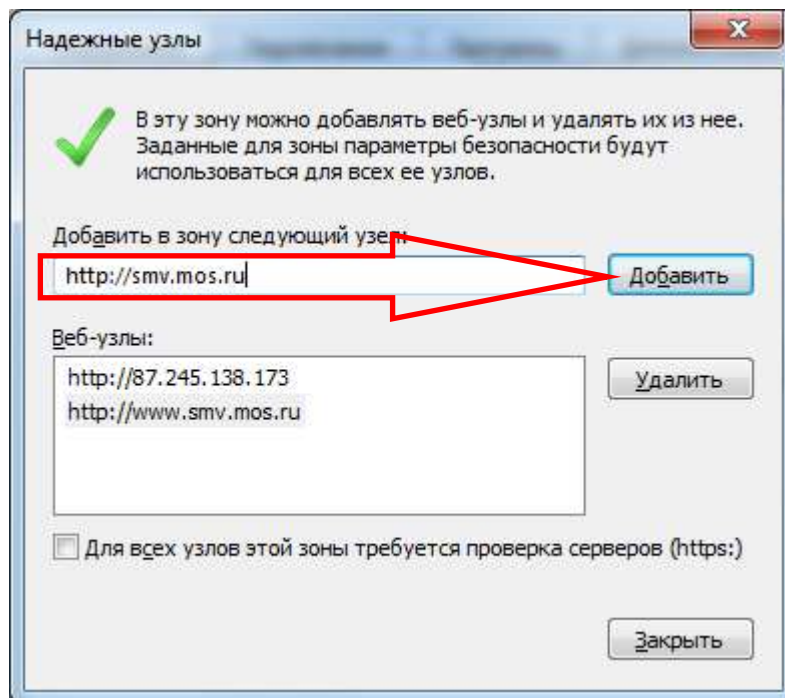


Рисунок 8 - Настройка обозревателя – Надежные узлы

- нажать кнопку **Закреть** для возврата в окно «Свойства обозревателя»;

Примечание:

Для добавления надежных узлов необходимо иметь соответствующие права.

Добавлять нужно именно сайт smv.mos.ru

- установить уровень безопасности для зоны надежных узлов в положение «**Низкий**»;
- нажать кнопку «**Другой**» и в открывшемся окне «**Параметры безопасности**» (Рисунок 12-- Настройка обозревателя – Параметры безопасности) установить следующие настройки в разделе «**Загрузка неподписанных элементов ActiveX**» переключатель в положение «**Включить**» и нажать кнопку «**ОК**»;

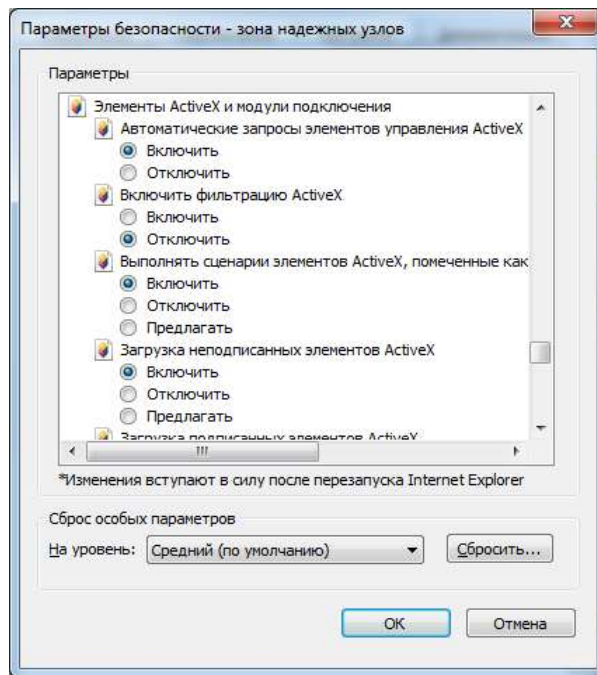


Рисунок 9 - Настройка обозревателя – Параметры безопасности

– для сохранения сделанных настроек в окне «Свойства обозревателя» нажать кнопку «ОК».

– выбрать в меню браузера «Сервис» пункт «Параметры режима представления совместимости» (Рисунок 10);

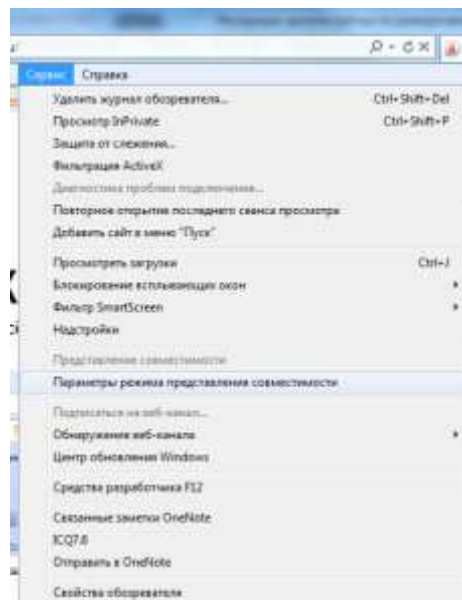


Рисунок 10- Параметры режима представления совместимости

- откроется форма настройки параметров (Рисунок 11);

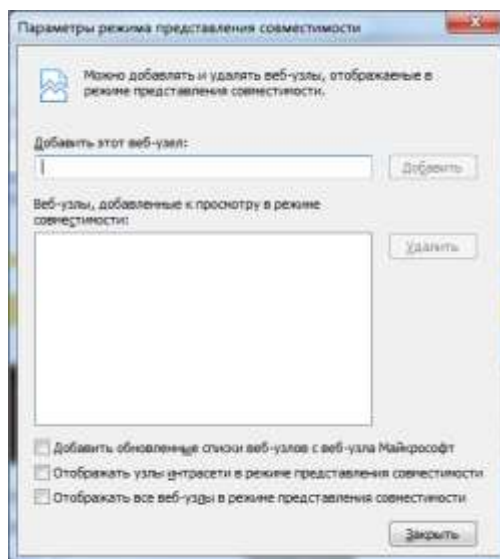


Рисунок 11 - Параметры режима представления совместимости

- удалить веб-узел страницы Системы из списка **«Веб-узлы, добавленные к просмотру в режиме совместимости»** (только в случае, если он там присутствует).
- снять галочки **«Отображать все веб-узлы в режиме представления совместимости»** (только в случае, если они проставлены).

1.3 УСТАНОВКА КРИПТО КОМПОНЕНТЫ.

При первом запуске потребуется установка крипто компоненты, для этого зайдите на сайт <http://smv.mos.ru> и нажмите кнопку «Авторизация» на главной странице (Рисунок 12).

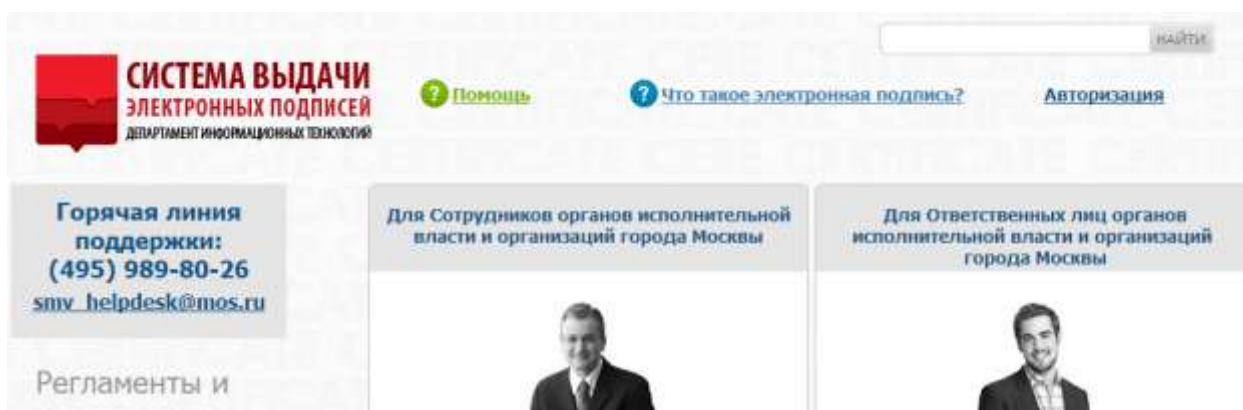


Рисунок 12 – Главная страница Системы

Откроется окно с предложением обновления крипто компоненты (Рисунок 13)

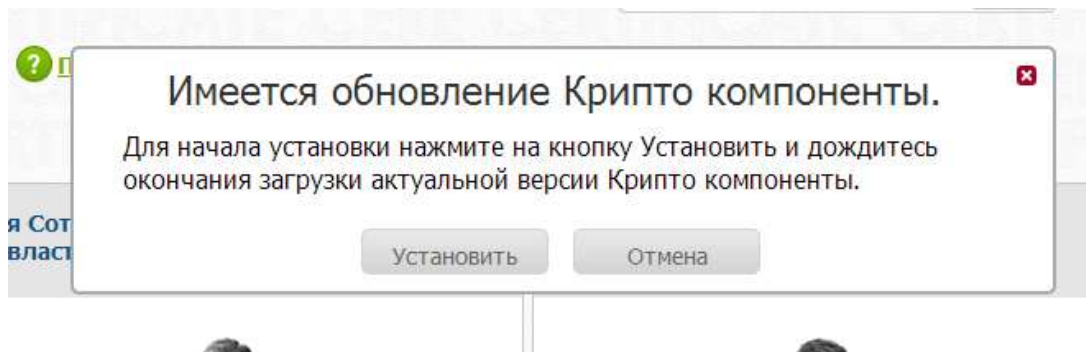


Рисунок 13 – Окно с предложением установки крипто компоненты

Необходимо нажать кнопку «Установить», откроется окно Сообщение с веб-страницы (Рисунок 14), нажмите кнопку ОК и сохраните установочный файл.

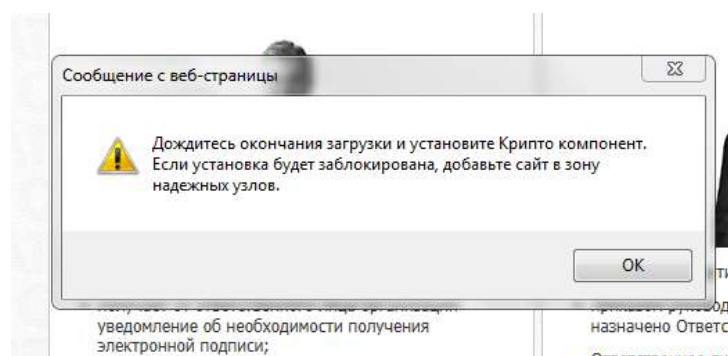


Рисунок 14 – Сообщение с веб-страницы

Закройте браузер, запустите сохраненный файл и следуйте диалогу установки (Рисунок 15).

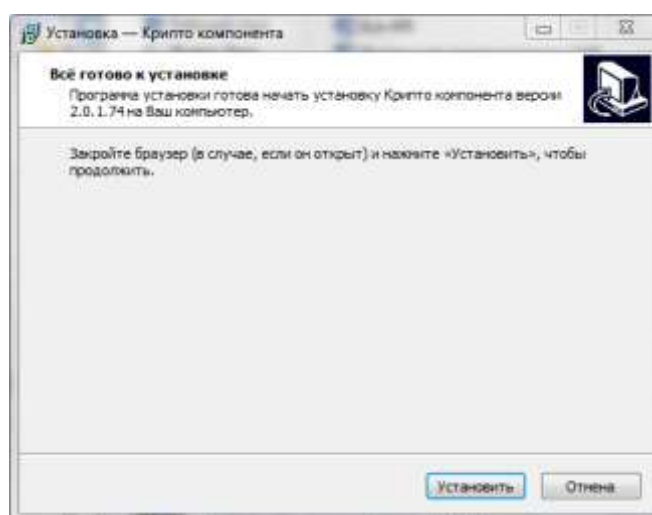


Рисунок 15 – Установка Крипто компоненты

2 ВХОД В ЛИЧНЫЙ КАБИНЕТ

Доступ Уполномоченного лица к личному кабинету осуществляется по персональному имени пользователя (логину) и паролю (до получения сертификата ключа электронной подписи) и с использованием электронной подписи (после получения сертификата).

Для входа в личный кабинет пользователь должен ввести адрес страницы Системы <http://smv.mos.ru> и нажать кнопку браузера «Переход» или клавишу «Enter». Затем на главной странице Системы нажать на ссылку **Авторизация** в верхней части экрана (Рисунок 16- Главная страница Системы).

СИСТЕМА ВЫДАЧИ ЭЛЕКТРОННЫХ ПОДПИСЕЙ
ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Помощь

Авторизация

Что такое электронная подпись?

Горячая линия поддержки:
(495) 961-13-61
smv_helpdesk@mos.ru

Регламенты и нормативные документы

[Инструкция по получению ЭЦП Ответственным лицом](#)

[Инструкция для Уполномоченного лица](#)

[Руководство Администратора](#)

[Руководство пользователя ПК СВЭ](#)

[Инструкция для Ответственного лица](#)

Все документы

Новости

02.11.2013

[Правительство РФ утвердило положение о едином портале госуслуг и требованиях к региональным порталам](#)

Для Сотрудников органов исполнительной власти и организаций города Москвы

Для получения сертификата:

- получает от ответственного лица организации уведомление об необходимости получения электронной подписи;
- получает у ответственного лица организации ключевой носитель, а также логин и пароль к личному кабинету системы выдачи электронных подписей;
- согласует данные заявления на изготовление сертификата электронной подписи в личном кабинете системы выдачи электронных подписей;
- генерирует запрос на выдачу сертификата в личном кабинете системы выдачи электронных подписей и сохраняет его на полученном ключевом носителе;
- печатает и подписывает бумажный оригинал заявления на изготовление сертификата электронной подписи и передает его ответственному лицу организации;
- после получения уведомления о готовности сертификата электронной подписи сохраняет его на ключевой носитель из личного кабинета системы выдачи электронных подписей;

Для Ответственных лиц органов исполнительной власти и организаций города Москвы

Для получения сертификата:

- приказом руководителя организации должно быть назначено Ответственное лицо;
- Ответственное лицо направляет письмо в Департамент информационных технологий (ДИТ) Сведения о назначении ответственного лица по работе с сертификатами ключей подписей органами власти, муниципального органа или организации в соответствии с приложением №4 к Регламенту реализации мероприятий по организации выдачи сертификатов ключей электронных цифровых подписей, утвержденным распоряжением Департамента информационных технологий от 27 декабря 2011 года №04-16-1045/11. Способы отправки – с курьером на бумажных носителях по адресу г.Москва, ул.Новая Басманная, дом 10, стр.1 (www.dit.mos.ru/contacts/), либо скан-копии на имя Ермолаева А.В. через электронный документооборот (www.mosdo.ru/);
- готовит необходимый пакет документов в соответствии с инструкцией по получению электронной цифровой подписи для Ответственных лиц, размещенной на портале smv.mos.ru, и направляет его для проверки в электронном виде в Удостоверяющий центр по адресу adm@uc-moskva.ru (Телефон +7 (495) 988-22-78)
- после получения Сведений о назначении ответственного лица из Департамента информационных технологий г. Москвы отправляет

Рисунок 16 – Главная страница Системы

В открывшемся окне (Рисунок 17) необходимо выполнить одно из следующих действий:

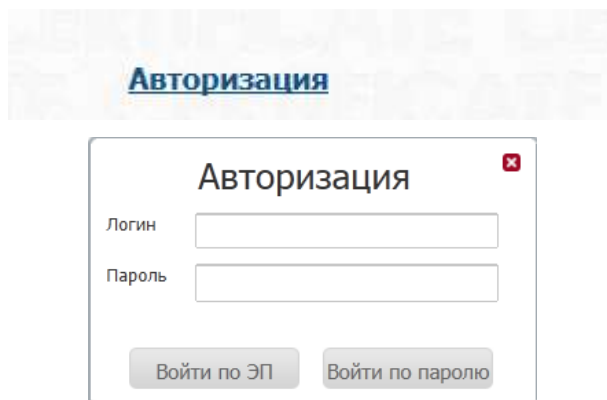
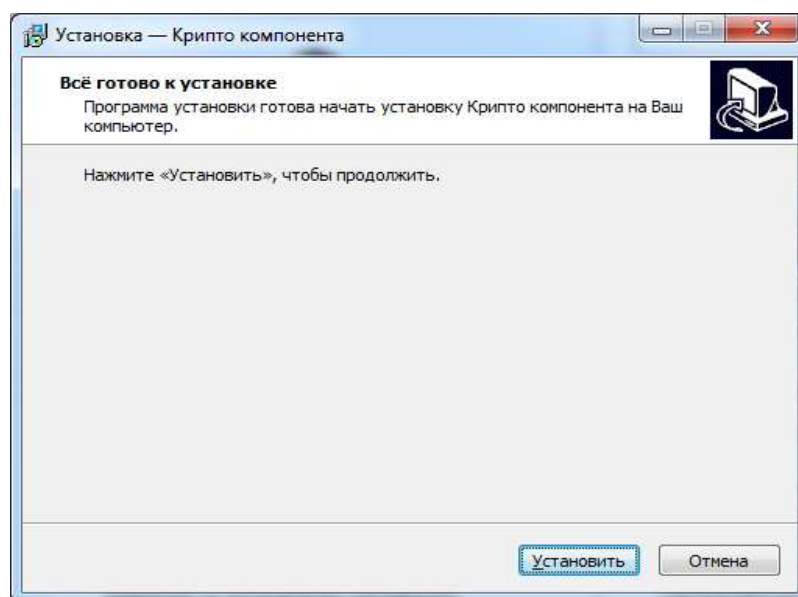


Рисунок 17 – Авторизация

- если у пользователя еще нет электронной подписи – ввести логин и пароль и нажать кнопку **Войти по паролю**;

- если у пользователя есть электронная подпись:

- подключить к USB-порту носитель с электронной подписью и нажать на кнопку **Войти по ЭП**. Откроется форма установки Крипто компонента (Рисунок 18);



Примечание:

Форма установки Крипто компонента открывается только в случае, если Крипто компонент не установлен. После установки Крипто компонента эта форма открываться не будет. Крипто компонент необходим для работы с Системой. Форма установки открывается при первичном входе в личный кабинет или при изменении версии Крипто компоненты.

- нажать на кнопку **«Установить»**. Начнётся установка Кристо компонента, а по окончании процесса установки откроется форма завершения установки;
- нажать кнопку **«Завершить»**. Отобразится главная страница Системы;
- щелкнуть мышью по ссылке **«Войти по ЭП»**. Откроется форма выбора сертификата электронной подписи (**Ошибка! Источник ссылки не найден.**18- Форма выбора сертификата);

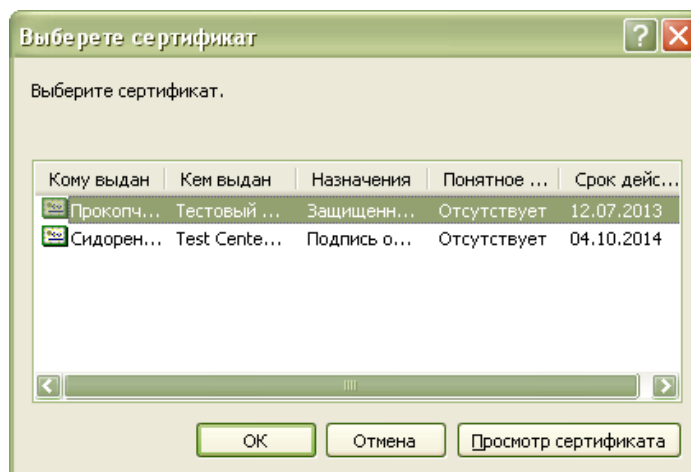
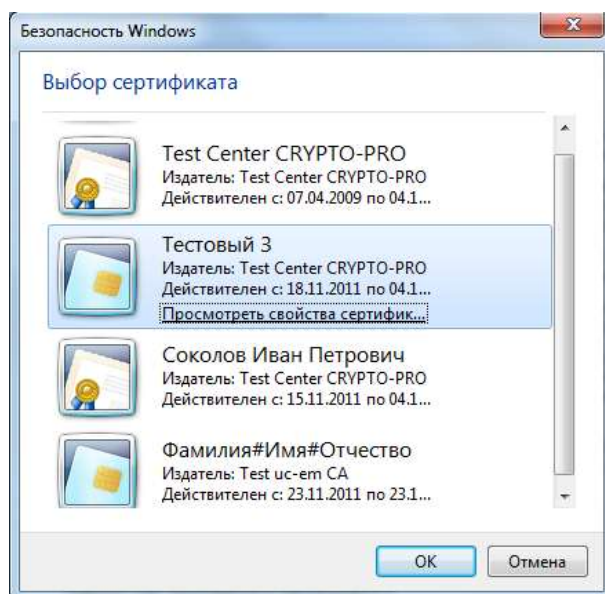


Рисунок 18 – Форма выбора сертификата

- выбрать в списке полученный от УЦ сертификат и нажать кнопку **«OK»**. Откроется форма ввода пароля для контейнера закрытого ключа ЭП (Рисунок 19).
- в открывшемся диалоге ввести пароль/ПИН-код для контейнера и нажать кнопку **«OK»**. Произойдет вход в личный кабинет.

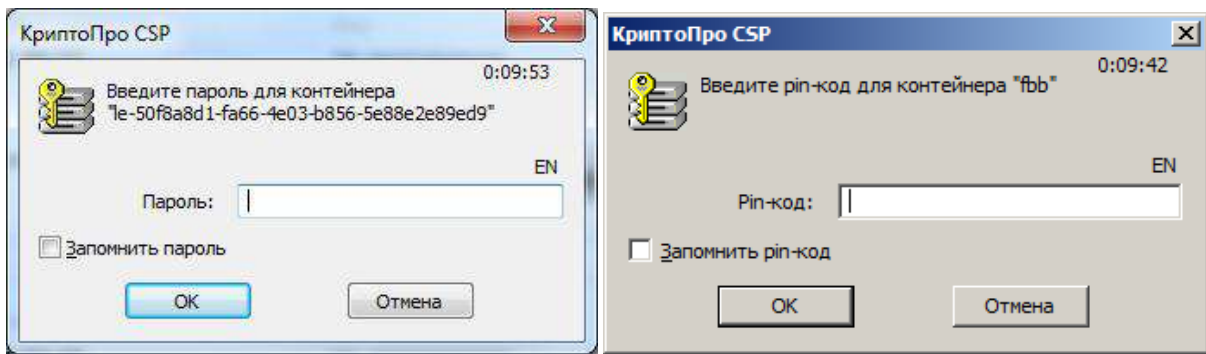


Рисунок 19 – Диалог ввода пароля/ ПИН-кода в различных версиях браузера

Примечание:

При желании можно установить отметку «Запомнить пароль/ПИН-код», тогда при последующем использовании электронной подписи пароль/ПИН-код для контейнера запрашиваться не будет.

ЭКСПОРТ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

Для экспорта необходимо :

1. Открыть Internet Explorer. В пункте меню «Сервис» выбрать «Свойства обозревателя» (Рисунок 71).

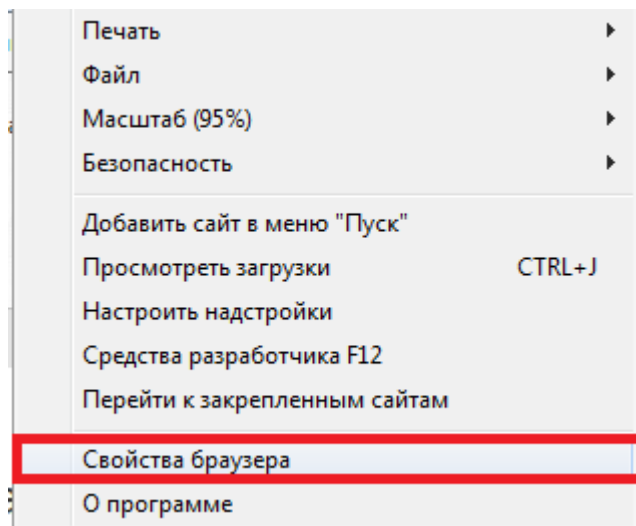


Рисунок 71 – Свойства обозревателя

2. Выбрать вкладку «Содержание». Нажать кнопку «Сертификаты» (Рисунок 72).

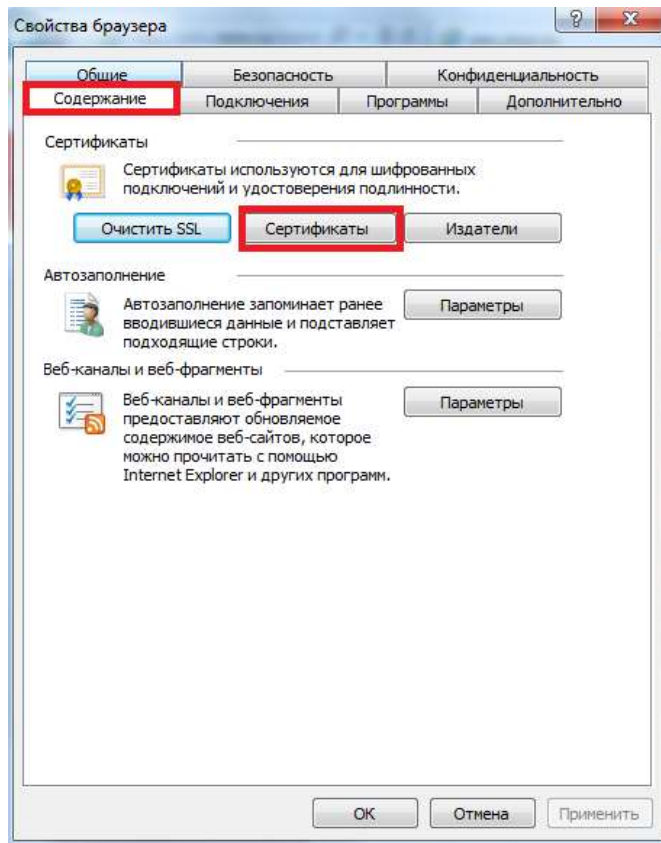


Рисунок 72 – Вкладка «Содержание» свойств обозревателя

3. В появившемся списке выбрать требуемый сертификат. Нажать кнопку «Экспорт». Появится новое окно «Мастер экспорта сертификатов». Нажать кнопку «Далее» (Рисунок 73).

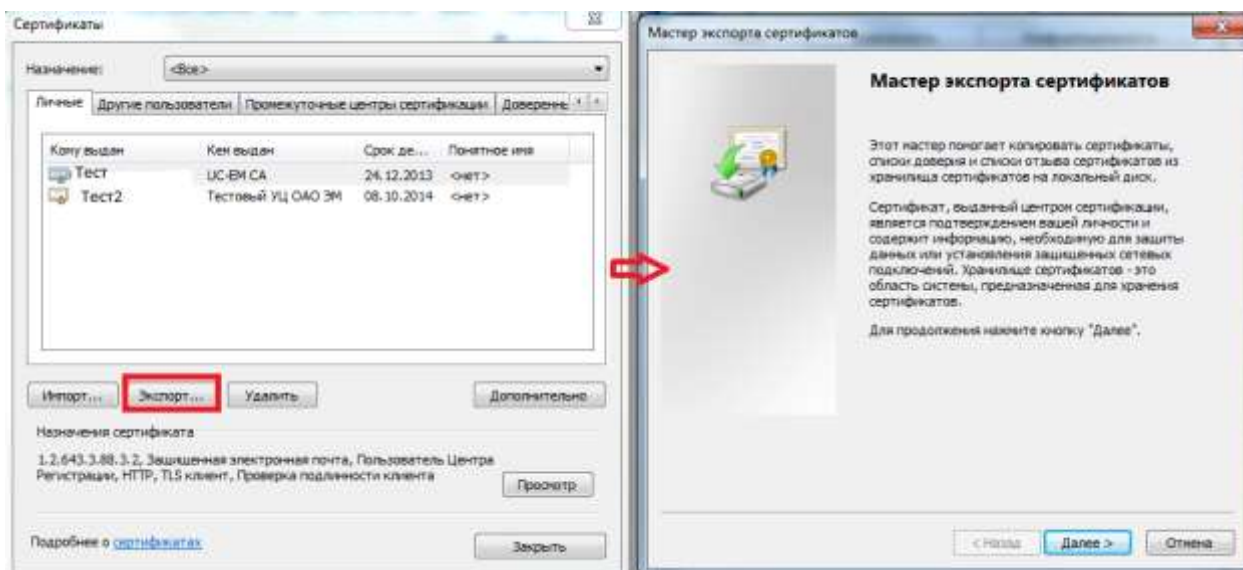


Рисунок 73 – мастер экспорта сертификатов

4. Выбрать «Нет, не экспортировать закрытый ключ» и нажать кнопку «Далее» (Рисунок 74).

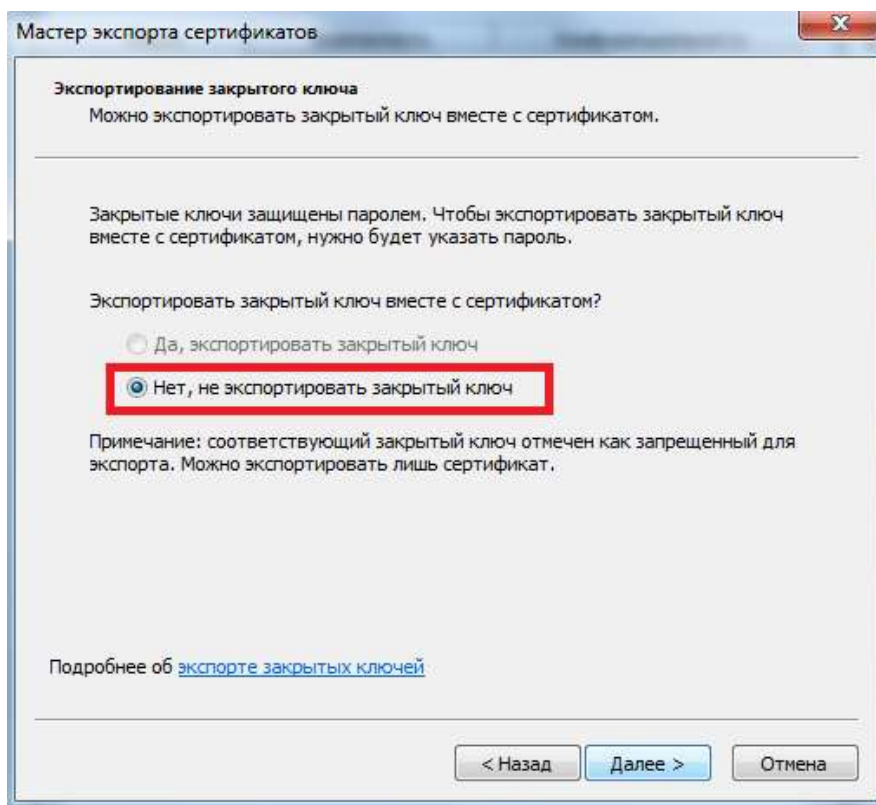


Рисунок 74 – Экспорт закрытого ключа

5. Выбрать «Файлы X.509 (.CER) в кодировке Base-64». Нажать кнопку «Далее» (Рисунок 75).

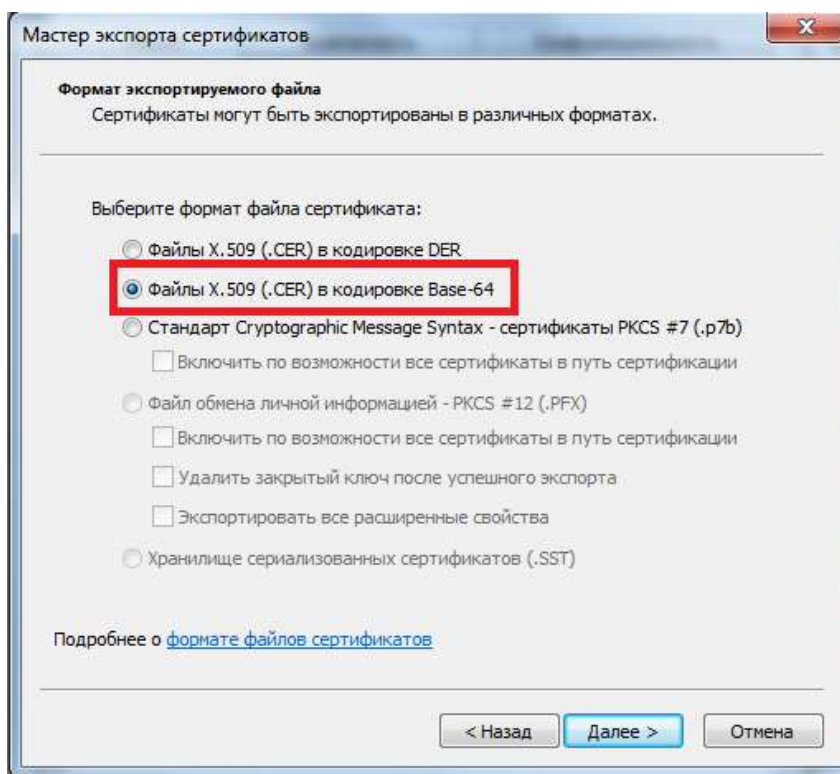


Рисунок 75 – Формат файла сертификата

6. Указать имя экспортируемого файла. Нажать кнопку «Далее» (Рисунок 76).

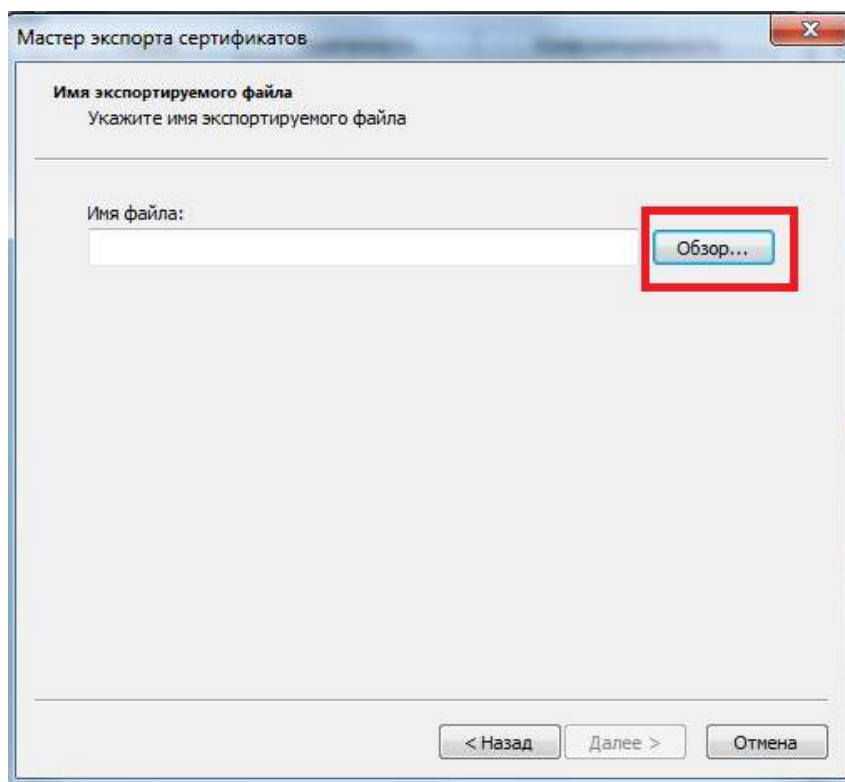


Рисунок 76 – Указание имени экспортируемого файла