РАБОТА С ЭЦП (ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСЬЮ) В ПОДСИСТЕМЕ «ВЕДЕНИЕ»

МСПИ (Система) позволяет устанавливать ЭЦП на хранящиеся в банках документы и пакеты обновления. Для этого в состав системы входит подсистема электронной подписи, обеспечивающая доступ к программному обеспечению криптозащиты. С помощью данной подсистемы можно реализовать следующие функции:

- **Подпись блока данных с помощью установленного в системе закрытого ключа;**
- **Проверка подписи блока данных;**
- **Установка сертификата открытого ключа электронной подписи;**
- **Установка списка отозванных сертификатов.**

Система не содержит средств для создания открытых и закрытых ключей электронных подписей и списков отозванных сертификатов. Эти функции возлагаются на внешнее программное обеспечение криптопровайдера (удостоверяющего центра).

Подсистема электронной подписи доступна как из подсистемы ведения, так и из подсистемы доступа.

Для работы с подсистемой ведения необходимо выполнение следующих действий:

1) Установить и настроить на сервере программное обеспечение криптопровайдера и корневой сертификат (ключа) электронной цифровой подписи;
2) Установить и настроить программное обеспечение криптопровайдера на компьютерах операторов, которые имеют право устанавливать подписи на редакции документов и пакеты обновления;
3) Установить на компьютерах операторов, которые имеют право устанавливать подписи на редакции документов и пакеты обновления, корневые сертификаты ключа электронной цифровой подписи и сертификаты закрытого ключа электронной цифровой подписи, которая будет использоваться данным оператором;
4) На рабочих местах операторов, которые имеют право устанавливать подписи на редакции документов и пакеты обновления, произвести настройку программного обеспечения. При этом указывается сертификат закрытого ключа электронной подписи, который будет использоваться для подписи редакций документов и пакетов обновления.

После установки и настройки в подсистеме ведения банков данных становятся доступны следующие функции:

1. проверка подписи редакции документа;
2. установка сертификатов ключей электронной подписи и списков отзывов сертификатов при выполнении операции обновления;
3. проверка подписи пакетов обновления;
4. установка подписи на редакцию документов;
5. установка подписи на пакеты обновления, помещение сертификатов ключей и списков отзыва сертификатов в пакеты обновления;
6. удаление ЭЦП с редакции документа;
7. проверка ЭЦП выборки документов;
8. подготовка отчётов по установке, проверке и удалении ЭЦП.

Подпись редакции документа производится сотрудником, обеспечивающим обработку документов.

Подпись устанавливается отдельно для каждой редакции документа, возможна установка подписи на выбранные или на все редакции. При этом будут произведены следующие действия:

1) для текущей редакции и всех, включаемых в нее иллюстраций и других объектов, будет сгенерирован блок данных подписи и идентификатора подписавшего пользователя;

2) данный блок будет помещен в банк данных в одну запись с документом;

3) оператор может вызывать данную операцию произвольное число раз.

Проверка подписи редакции документа производится при открытии редакции документа. При этом в зависимости от результата проверки возможны следующие ситуации:

«Подписи нет» — система отображает в области информации о версии пиктографический значок, предупреждающий об отсутствии электронной подписи;

«Подпись невозможно проверить» — система отображает специальный пиктографический значок, предупреждающий о наличии непроверенной электронной подписи;

«Подпись верна» — система отображает специальный пиктографический значок, уведомляющий о наличии проверенной электронной подписи. В справке о документе отображается информация о том, кем были подписаны редакции (данные из сертификата открытой электронной подписи, установленной в системе);

«Подпись неверна» — система отображает специальный пиктографический значок, предупреждающий о нарушении электронной подписи. В справке о документе отображается информация о том, кем были подписаны редакции.

Удаление подписи редакции документа доступно оператору, который вносит изменения в документ.

Эта операция позволяет удалить блок электронной подписи у данной редакции документа.

Проверка подписи выборки документов доступна оператору в подсистеме ведения банка данных.

При выполнении этой операции система проверяет электронную цифровую подпись у документов, которые отмечены в данной выборке. Формируется один из следующих видов отчетов:

1) Отчет для каждого документа, который содержит ссылку на документ и результат проверки, соответствующий сообщению при проверке отдельного документа.
2) Отчет для каждого сертификата открытого ключа или идентификатора владельца электронной подписи (Signer ID). Каждая строка этого отчета содержит информацию о сертификате или данные идентификатора пользователя и количество документов, подписанных этим пользователем.

Система позволяет производить **подпись пакетов обновления**, для чего в формате обновления есть соответствующие поля, в которые помещается блок данных подписи и идентификатора подписавшего пользователя.

Подпись пакета производится при его создании, если на данной машине установлено и настроено соответствующее программное обеспечение криптопровайдера и разрешена соответствующая функция.

Возможен режим работы МСПИ, когда обрабатываются только подписанные пакеты.

Внутри пакета обновления могут быть переданы сертификаты открытых ключей электронной подписи и/или списки отозванных сертификатов.

Администратор при создании пакета обновления может указать файлы, содержащие сертификаты открытых ключей, и списки отзыва сертификатов.

Система при обработке пакета обновления с сертификатами и списками отзыва производит установку сертификатов и списков отзыва сертификатов, переданных в пакете при выполнении следующих **условий**:

1) установлено и настроено программное обеспечение криптопровайдера;

2) установлен и действует корневой (root) сертификат для передаваемого сертификата.

При нарушении этих условий система записывает в протокол обновления сообщение о невозможности установки сертификата и причину отказа в установке. Обработка данного пакета продолжается вне зависимости от результата установки сертификатов и списков доступа.

При обработке пакета обновления система производит обработку блока электронной подписи и, в зависимости от результата, следующие ситуации:

«Подписи нет» и разрешено обновление неподписанными пакетами — система производит обновление, поместив в протокол обновления запись «**Пакет не подписан**»;

«Подпись невозможно проверить» и разрешено обновление неподписанными пакетами — система производит обновление, поместив в протокол обновления запись «**Пакет подписан, источник не проверен**»;

«Подпись верна» — система производит обновление, поместив в протокол обновления запись «**Пакет подписан. Автор пакета <данные из сертификата открытой электронной подписи, установленной в системе>**»;

«Подпись неверна» — система не производит обновление данным пакетом, поместив в протокол обновления запись «**Пакет с нарушенной подписью. Автор пакета <данные из сертификата открытой электронной подписи, установленной в системе>**».

Как уже отмечалось, для работы с цифровыми подписями необходимо:

1) Установить соответствующее ПО (например, *КриптоПро CSP*);
2) Установить корневой сертификат, имеющий связь с закрытым ключом, в системное хранилище сертификатов.
3) Список отзыва сертификатов.

Для установки ПО (например, *КриптоПро CSP*) на компьютер требуются **права администратора**.

Для установки КриптоПро CSP необходимо запустить файл КриптоПро CSP\Setup.exe и следовать инструкциям установки.

При работе с цифровыми подписями (подписывании, проверке подписи) **требуется**:

- наличие ключевого контейнера;
- наличие в системном хранилище сертификатов корневого сертификата для тех сертификатов, которыми будет производиться постановка ЭЦП.

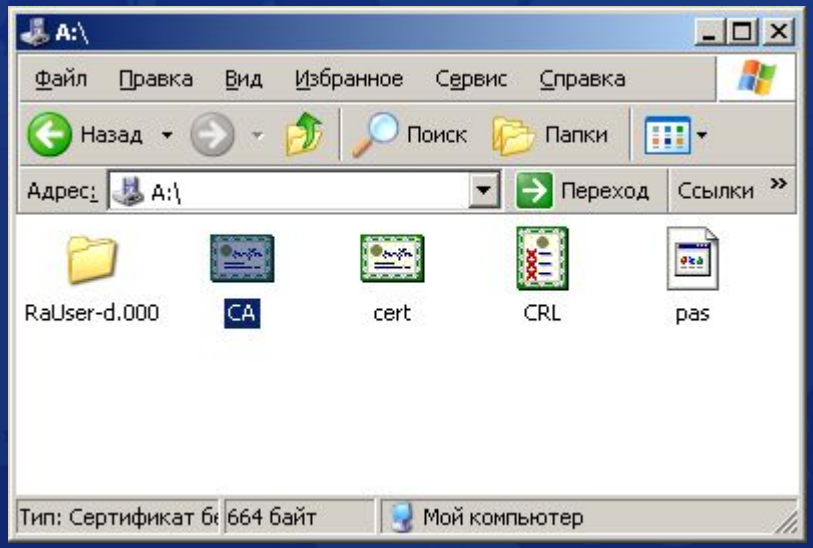
В настоящий момент ключевой контейнер – это дискета (флэш-карта, CD, E-токен) с сертификатом ЭЦП и ключевыми парами.
При работе с ЭЦП дискета (или другой сменный носитель) должна быть вставлена в дисковод.

Для того, чтобы **установить в системное хранилище корневой сертификат** под учетной записью того пользователя, который будет работать в системе, необходимо проделать следующее:

1) Открыть окно программы *Проводник (Обзор)* в ОС Windows;

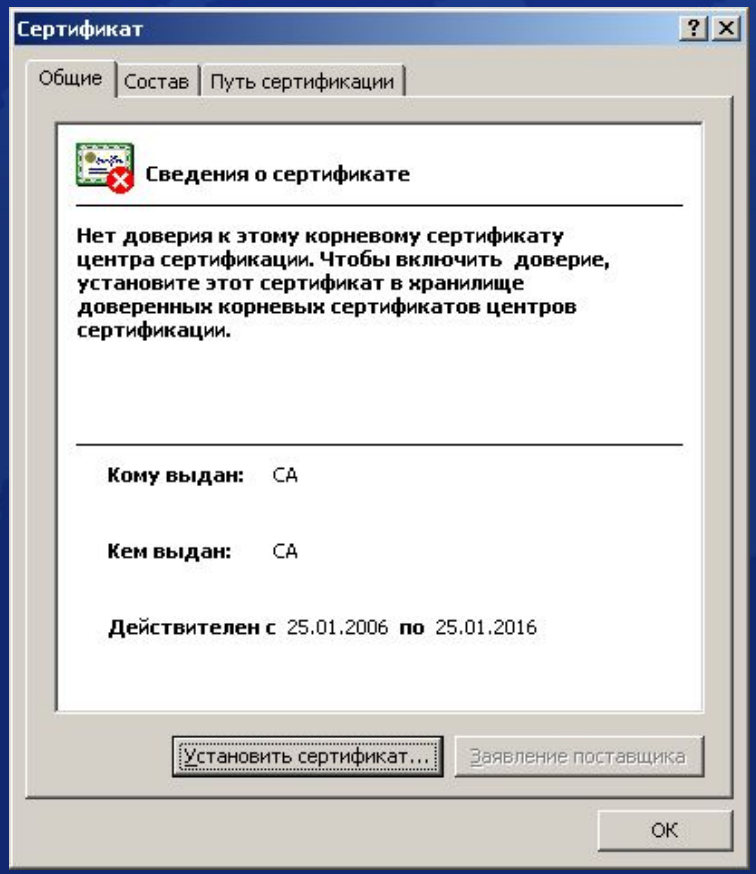
Для того, чтобы **установить в системное хранилище корневой сертификат** под учетной записью того пользователя, который будет работать в системе, необходимо проделать следующее:

2) В открывшемся окне найти и дважды щелкнуть мышью по имени файла сертификата (например, *A:\CA.cer*);



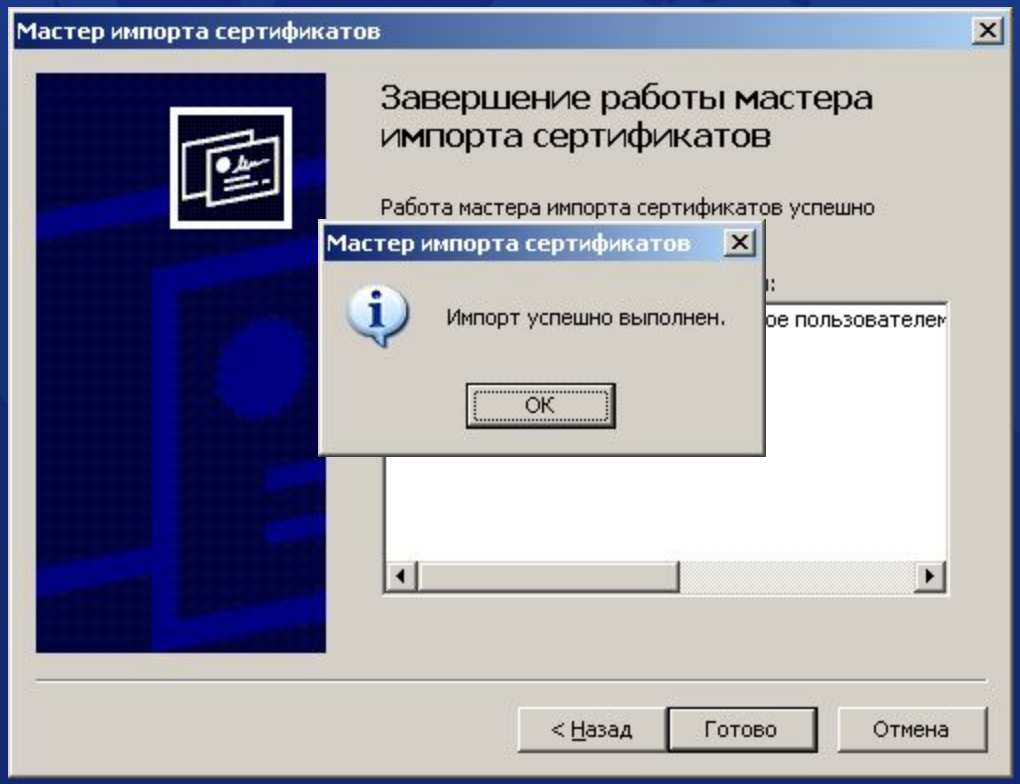
Для того, чтобы **установить в системное хранилище корневой сертификат** под учетной записью того пользователя, который будет работать в системе, необходимо проделать следующее:

3) В открывшемся окне **Сертификат** нажать кнопку **Установить сертификат**;



Для того, чтобы **установить в системное хранилище корневой сертификат** под учетной записью того пользователя, который будет работать в системе, необходимо проделать следующее:

4) В открывшихся окнах мастера установки выбрать нужное хранилище (“Доверенные корневые центры сертификации”, “Trusted Root Certification Authorities”).



После установки сертификата в системное хранилище им можно подписывать документы.

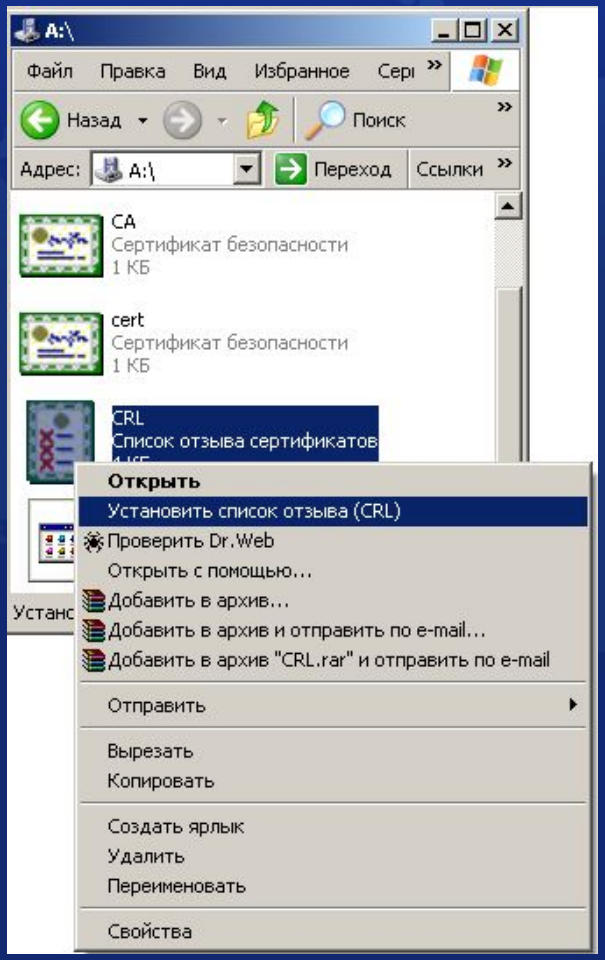
Для того, чтобы **установить в системное хранилище список отзывов сертификатов**, необходимо сделать следующее:

1) Открыть окно программы **Проводник (Обзор)** или окно папки **Мои документы** в ОС **Windows**;

2) В открывшемся окне, найти и щелкнуть правой кнопкой мыши по имени файла со списком отзывов сертификатов (с расширением CRL, например, *A:\CRL.crl*);

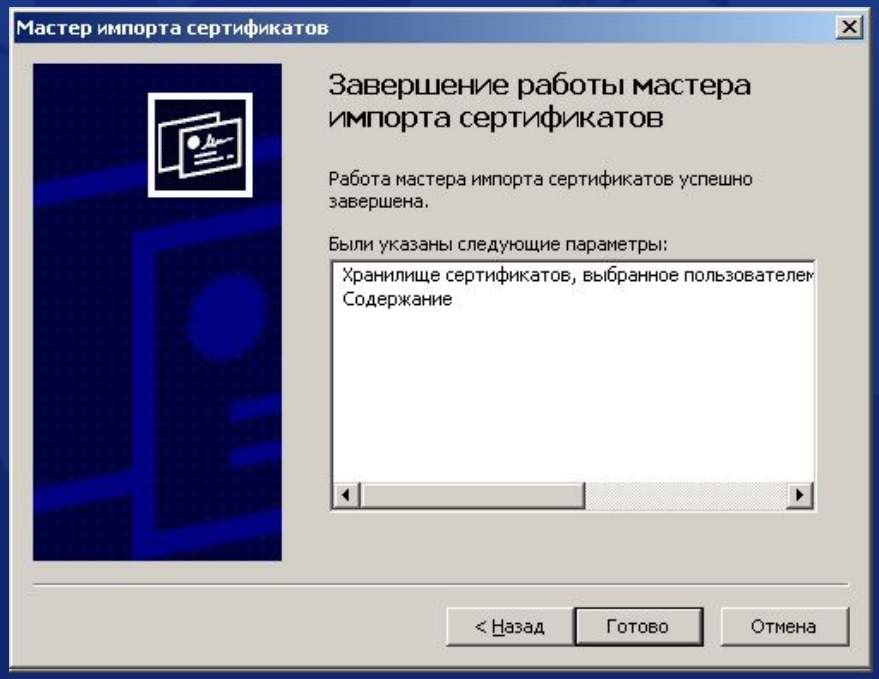
Для того, чтобы **установить в системное хранилище список отзывов сертификатов**, необходимо сделать следующее:

3) В открывшемся контекстном меню выбрать команду **Установить список отзыва**;



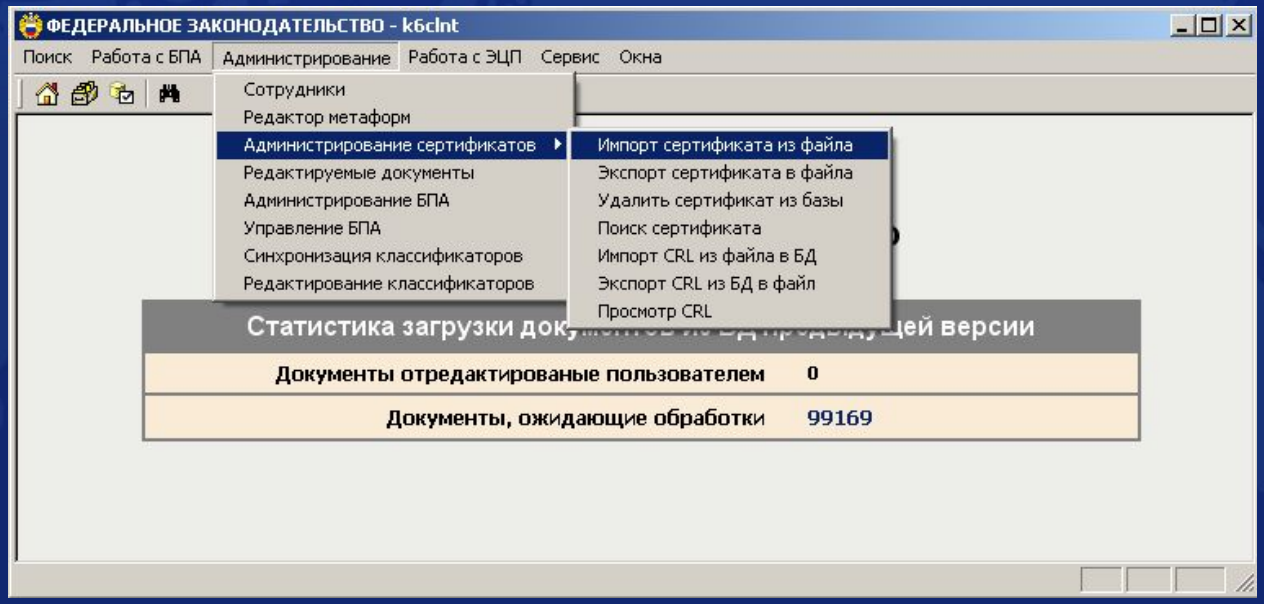
Для того, чтобы **установить в системное хранилище список отзывов сертификатов**, необходимо сделать следующее:

4) В открывшемся окне мастера установки выбрать нужное хранилище (“Доверенные корневые центры сертификации”, “Trusted Root Certification Authorities”).

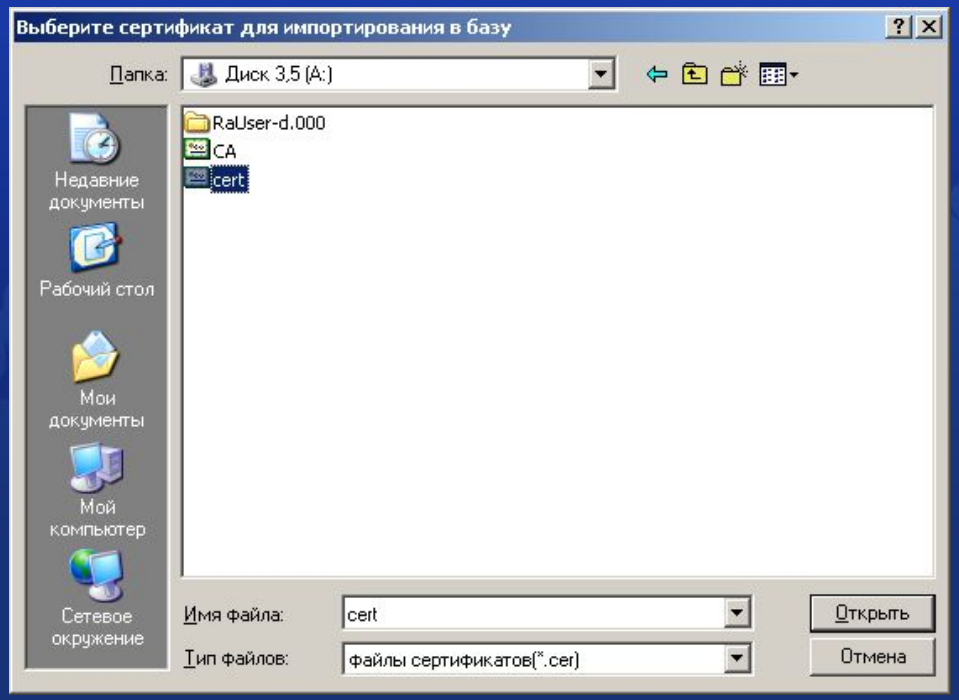


Подписывание документов ЭЦП возможно теми сертификатами, которые импортированы в банк. Предварительно необходимо импортировать во все тома (БПА) банки данных, документы которых надо подписывать.

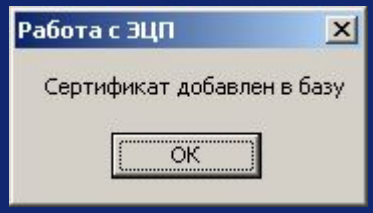
Для импортирования сертификатов в клиентском приложении выберите в меню *Администрирование* пункт *Импорт сертификата из файла*.



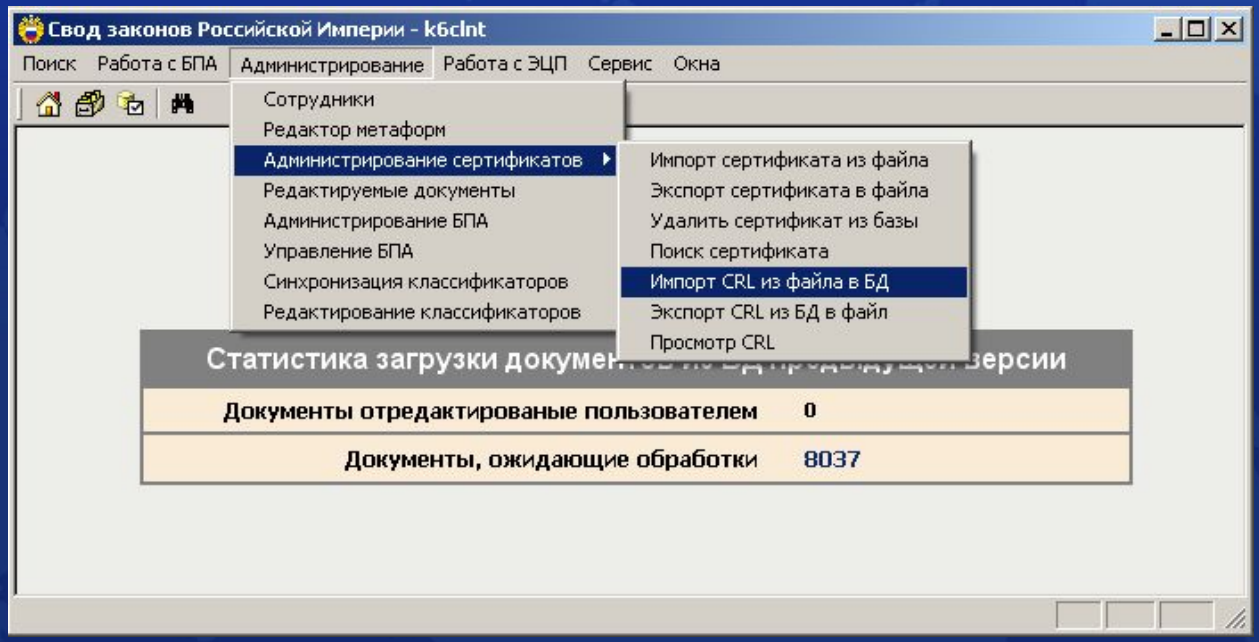
Затем укажите сертификат, с которым планируется работа:



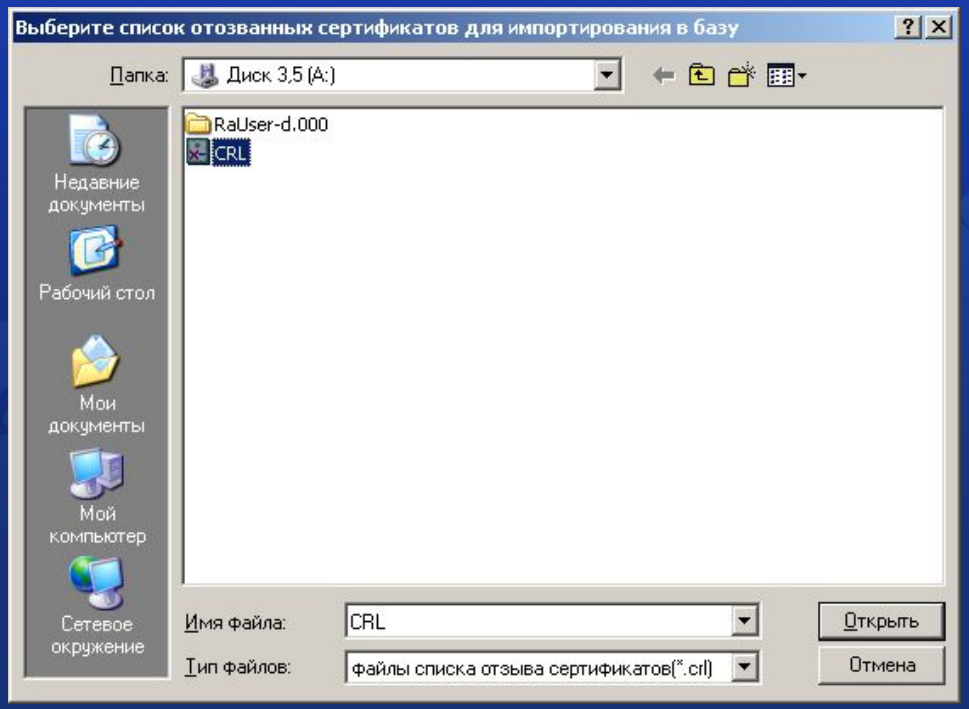
Не забудьте вставить носитель ключевого контейнера в устройство считывания. При успешном завершении процесса появится диалог (отчёт) с сообщением о том, что операция прошла успешно.



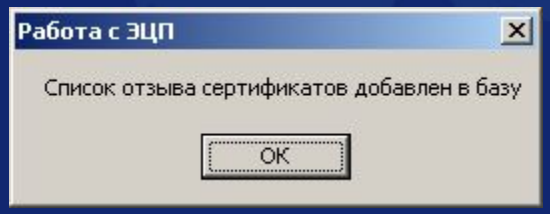
Для импортирования списка отозванных сертификатов в клиентском приложении выберите в меню *Администрирование* пункт *Импорт CRL из файла БД*.



Затем укажите сертификат, который следует отозвать.



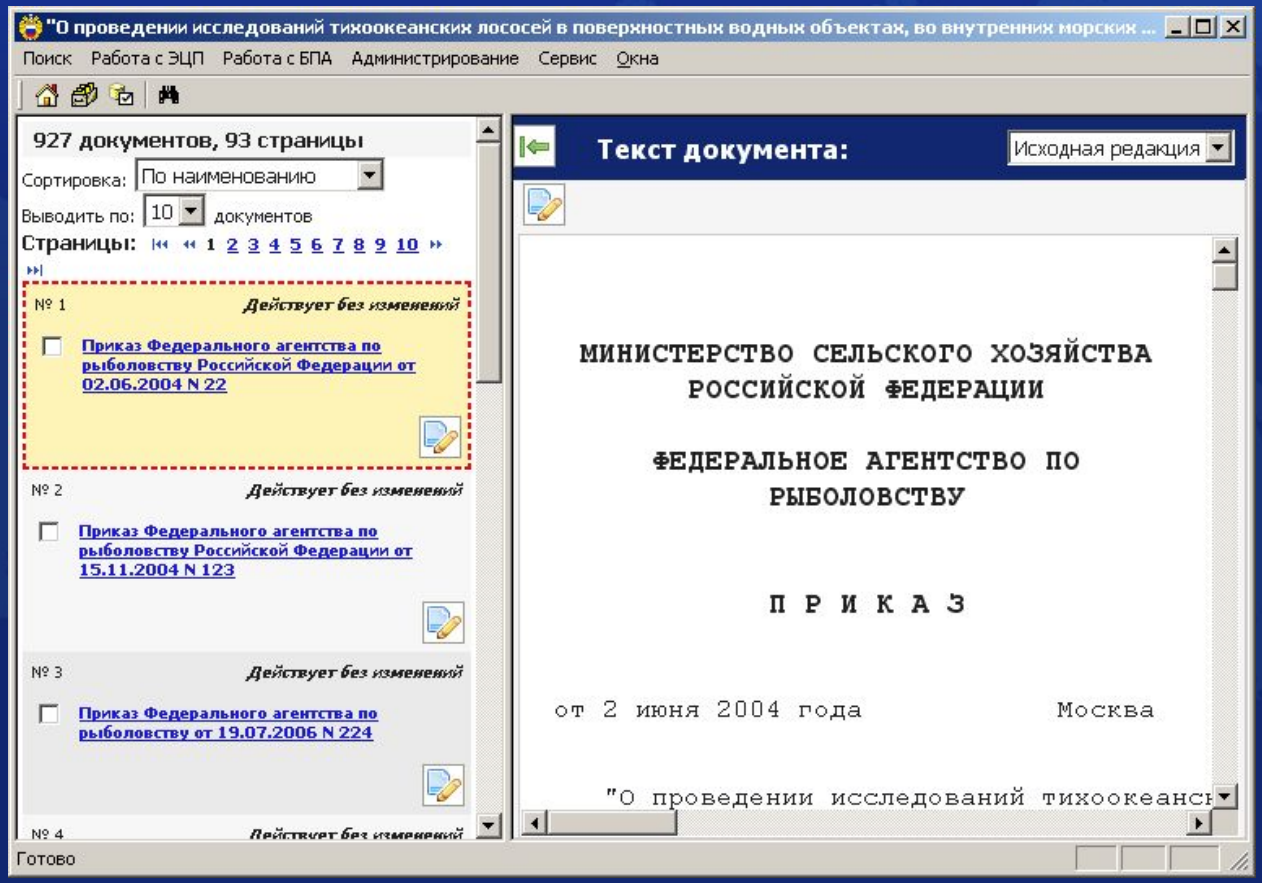
Далее действуйте аналогично действиям при добавлении сертификата в БПА, до получения положительного результата.



Система готова к работе с ЭЦП.

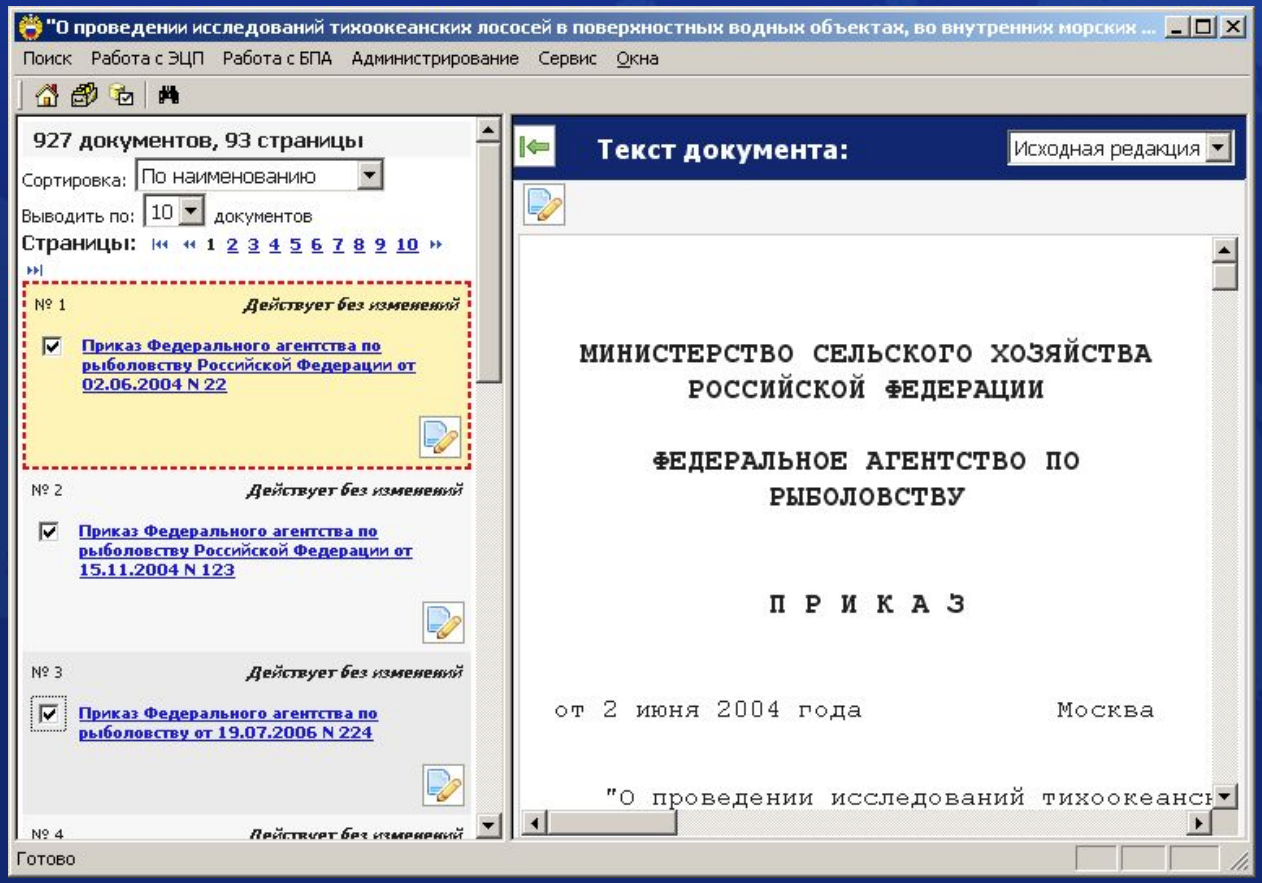
В заключение, рассмотрим пример со списком документов, на которые необходимо поставить ЭЦП.

1) Пусть сформирован следующий список документов:



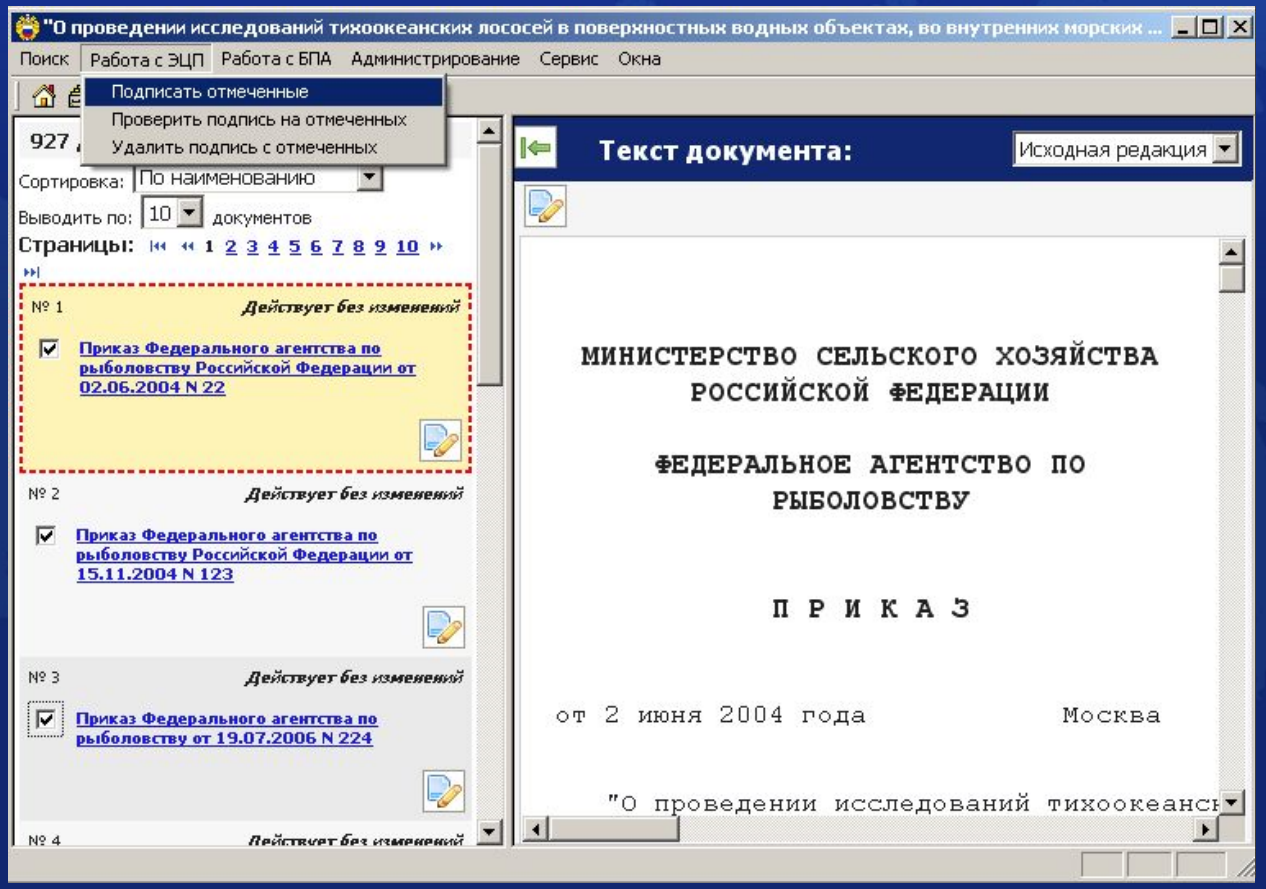
В заключение, рассмотрим пример со списком документов, на которые необходимо поставить ЭЦП.

2) Щелчком мыши выделим в этом списке первые три документа:



В заключение, рассмотрим пример со списком документов, на которые необходимо поставить ЭЦП.

3) В меню **Работа с ЭЦП** щелчком мыши по команде **Подписать отмеченные** эти три документа будут подписаны ЭЦП.



Проверить это можно, открыв указанный список документов в подсистеме Доступа.