

# Установка ключа электронной подписи и сертификатов

Чтобы начать работу с электронной подписью, необходимо установить в операционную систему контейнер ключа подписи, сертификат пользователя, корневой сертификат Удостоверяющего центра и список отозванных сертификатов (далее - СОС).

Контейнер ключа подписи защищен для сертифицированных носителей ключей ЭП PIN-кодом, в других случаях – паролем, известным только пользователю (лицу, формировавшему запрос на сертификат). Для органов государственной власти и местного самоуправления обязательно использование сертифицированных носителей ключей.

Сертификат с открытым ключом (для проверки подлинности вашей подписи), сертификат уполномоченного лица Удостоверяющего центра и СОС выдаются Удостоверяющим центром при получении сертификата ключа подписи.

## Установка ключа электронной подписи и личного сертификата пользователя.

1. Вставьте сертифицированный носитель ключей подписи, в примерах используется Rutoken, работа с eToken принципиально не отличается.
2. Запустите программу **ViPNet CSP**.



Рисунок: Запуск программы ViPNet CSP

3. В окне программы **ViPNet CSP** выберите раздел **Контейнеры**, затем нажмите кнопку **Установить сертификат из файла**.

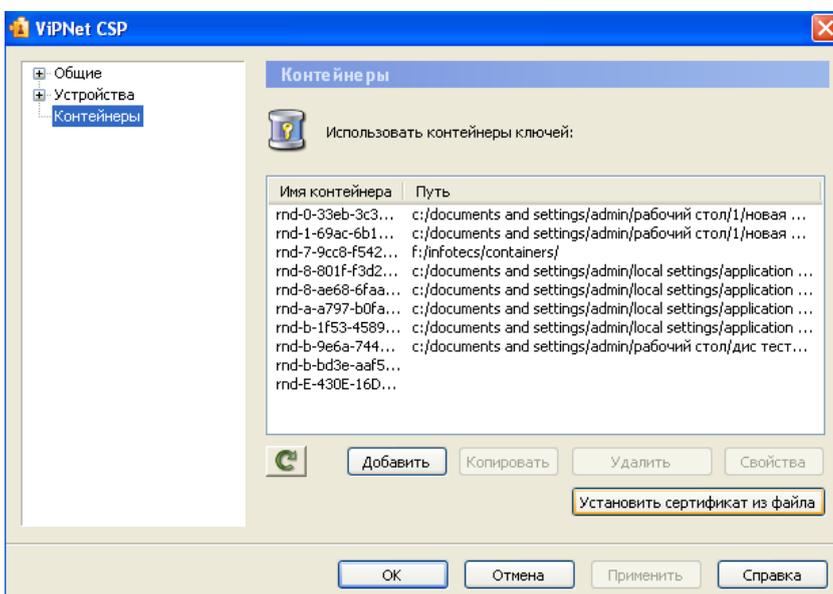


Рисунок: Панель контейнеров

4. В открывшемся окне укажите путь к сертификату и выберите сертификат пользователя

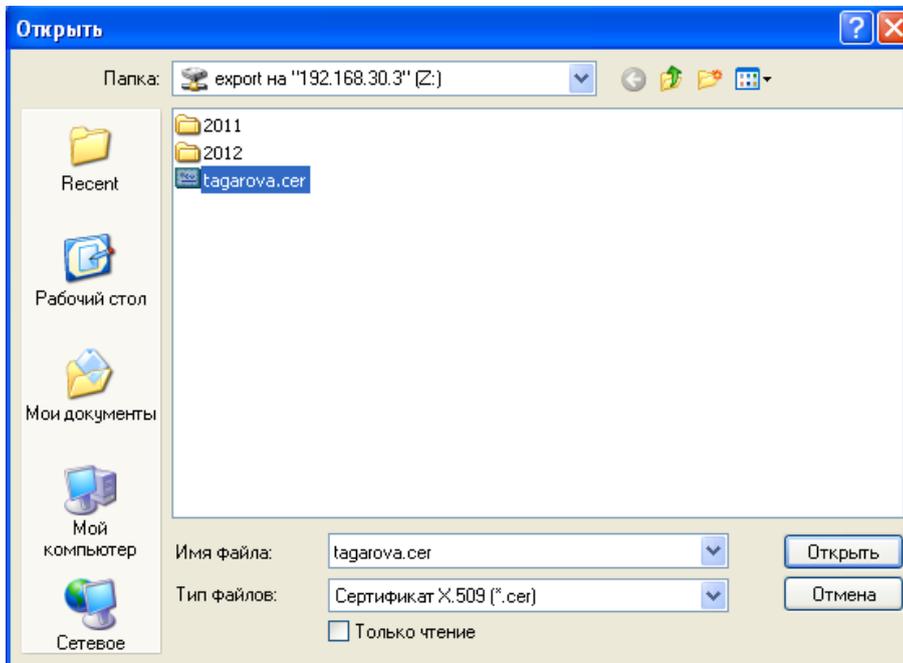


Рисунок: Выбор сертификата пользователя

5. В открывшемся окне мастера установки сертификатов нажмите **Далее**.

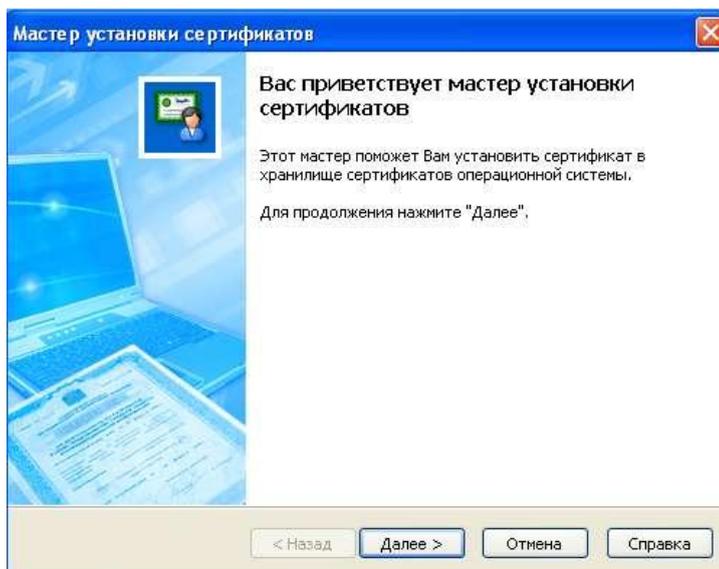


Рисунок: Окно приветствия мастера установки сертификата.

6. В открывшемся окне мастера установки сертификатов нажмите **Далее**.

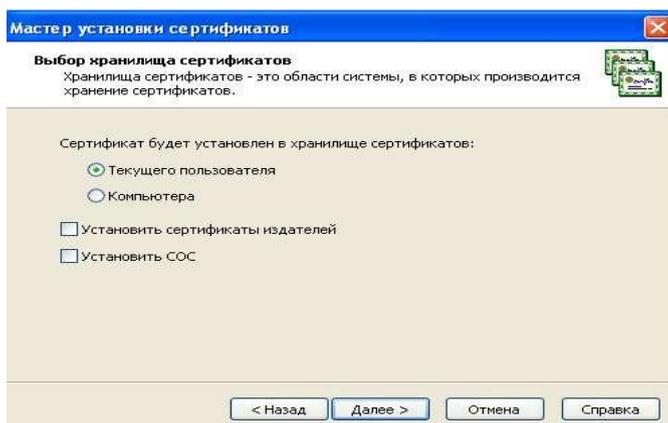


Рисунок: Окно мастера установки сертификата.

7. В открывшемся окне мастера установки отметьте **Указать контейнер с закрытым ключом**, затем нажмите **Далее**.

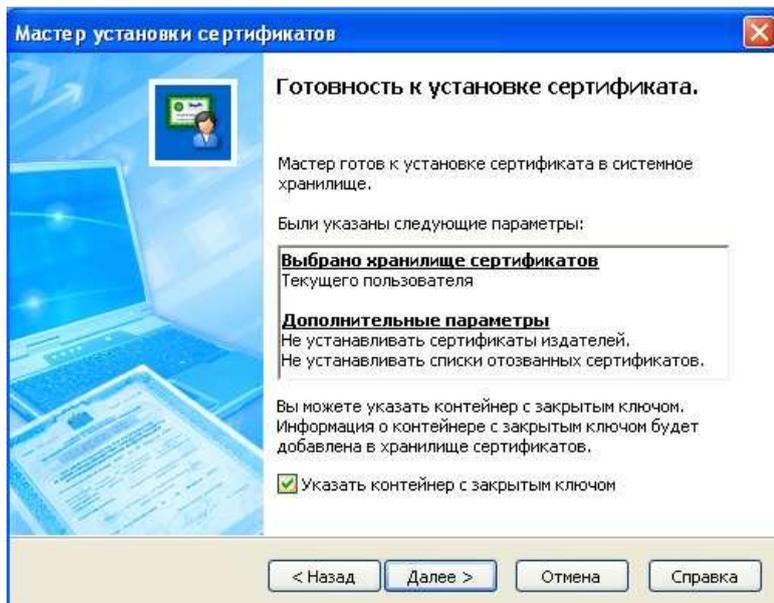


Рисунок: Окно мастера установки сертификата.

8. В открывшемся окне выбора контейнера установите переключатель **Выберите устройство** – для сертифицированных носителей или **Папка на диске** – во всех остальных случаях, как показано на рисунке и введите PIN-код носителя, затем нажмите кнопку **ОК**.

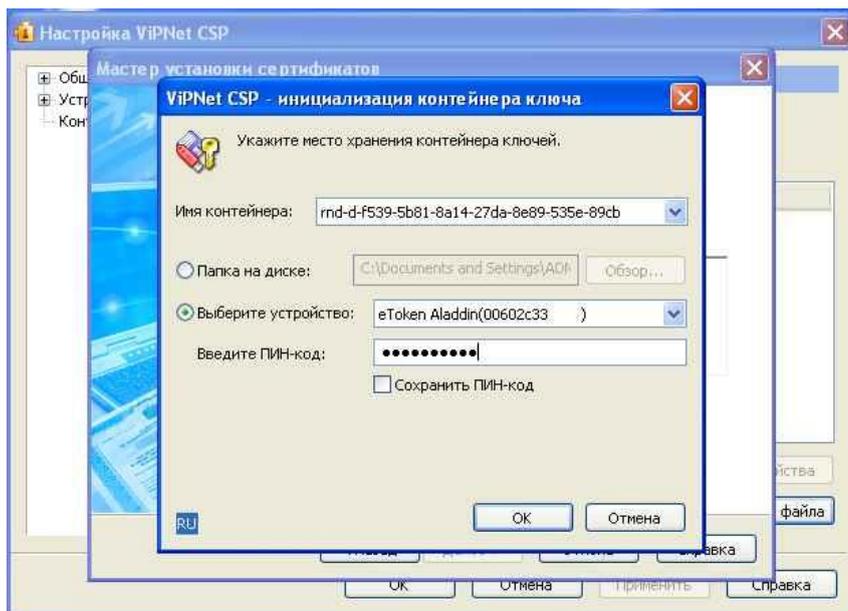


Рисунок: Окно выбора контейнера закрытого ключа.

9. Если появится запрос о сохранении сертификата в контейнере, ответьте **Да**.

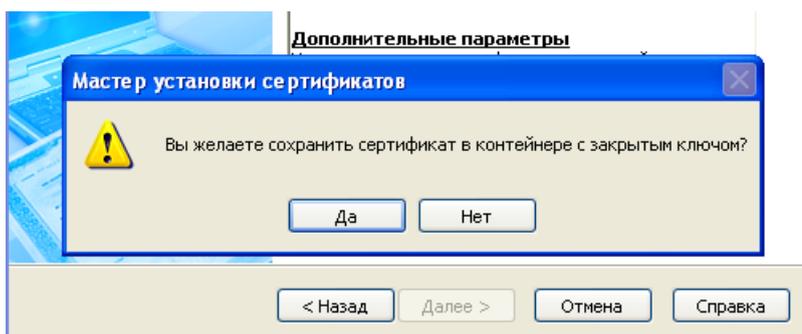


Рисунок: Окно сохранения сертификата в контейнере закрытого ключа. Дождитесь завершения работы мастера, после чего программу VIPNet CSP можно завершить.

# Установка корневого сертификата Удостоверяющего центра и СОС

Имена файлов сертификатов и СОС:

- ChitaCA\_20xx.crt – корневой сертификат Удостоверяющего центра, где xx- год выпуска сертификата;
- revokedCerts.crl - СОС;

Эти файлы пользователь получает из Удостоверяющего центра в папках вида 20xx, где XX – год выпуска корневого сертификата и соответствующего ему списка отозванных сертификатов, поскольку срок действия ключа подписи составляет 1 год, то достаточно иметь папки за текущий и предыдущий год.

Установка сертификатов и СОС выполняется средствами операционной системы.

## Установка корневого сертификата Удостоверяющего центра:

1. Откройте папку с файлом сертификата и щелкните правой кнопкой мыши по значку сертификата.

2. В контекстном меню выберите пункт **Установить сертификат**.

**Примечание:** отсутствие вкладки **Установить сертификат** свидетельствует о том, что вы используете несертифицированную копию операционной системы Windows, из которой вырезаны средства работы с сертификатами, в этом случае следует установить сертифицированную версию Windows.

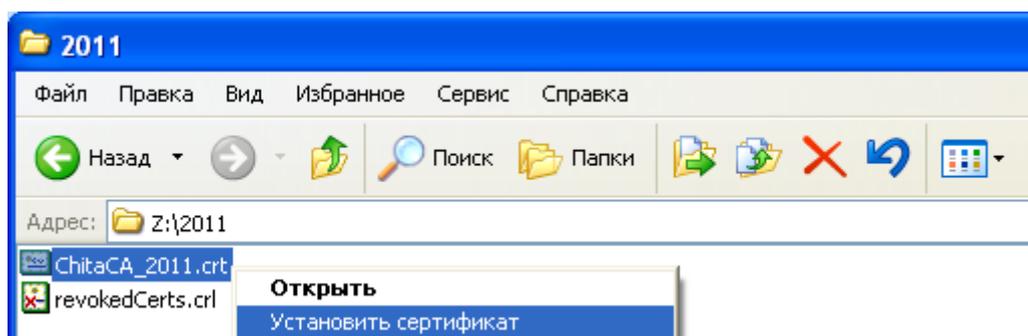


Рисунок: Установка сертификата

3. В окне приветствия мастера импорта сертификатов нажмите **Далее**.

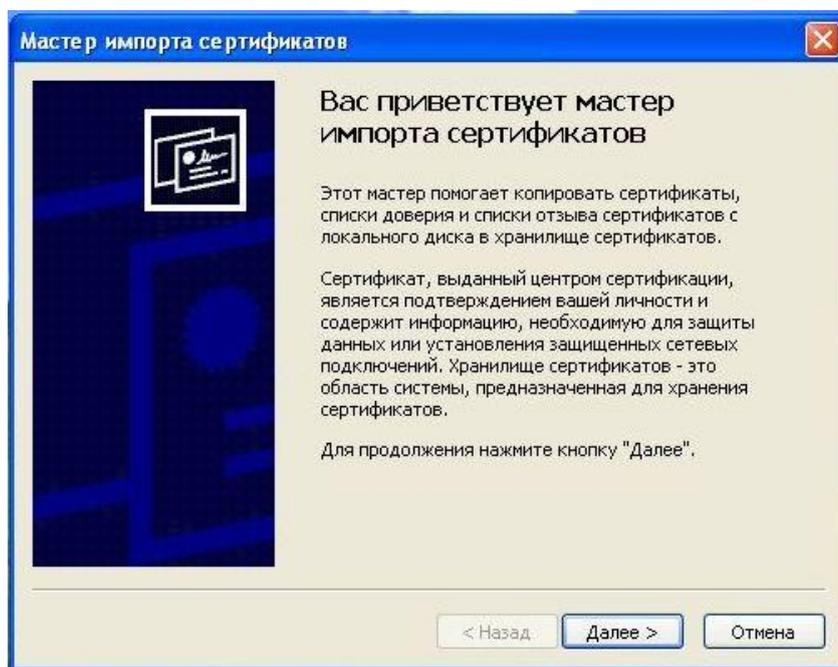


Рисунок: Окно приветствия мастера импорта сертификатов

4. На странице **Хранилище сертификатов** выберите **Поместить все сертификаты в следующее хранилище** и нажмите **Далее**.

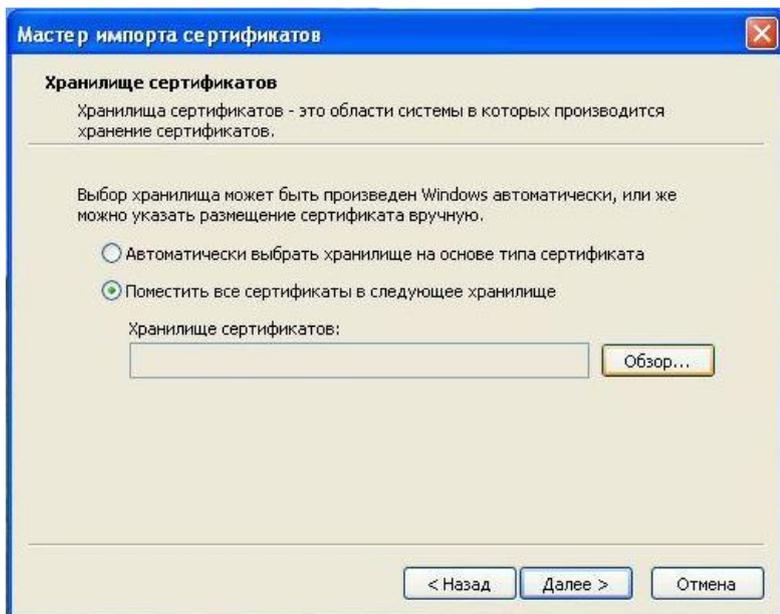


Рисунок: Выбор хранилища для сертификата Удостоверяющего центра

5. На странице **Выбора хранилища сертификатов** выберите **Доверенные корневые центры сертификации** и нажмите **ОК**.

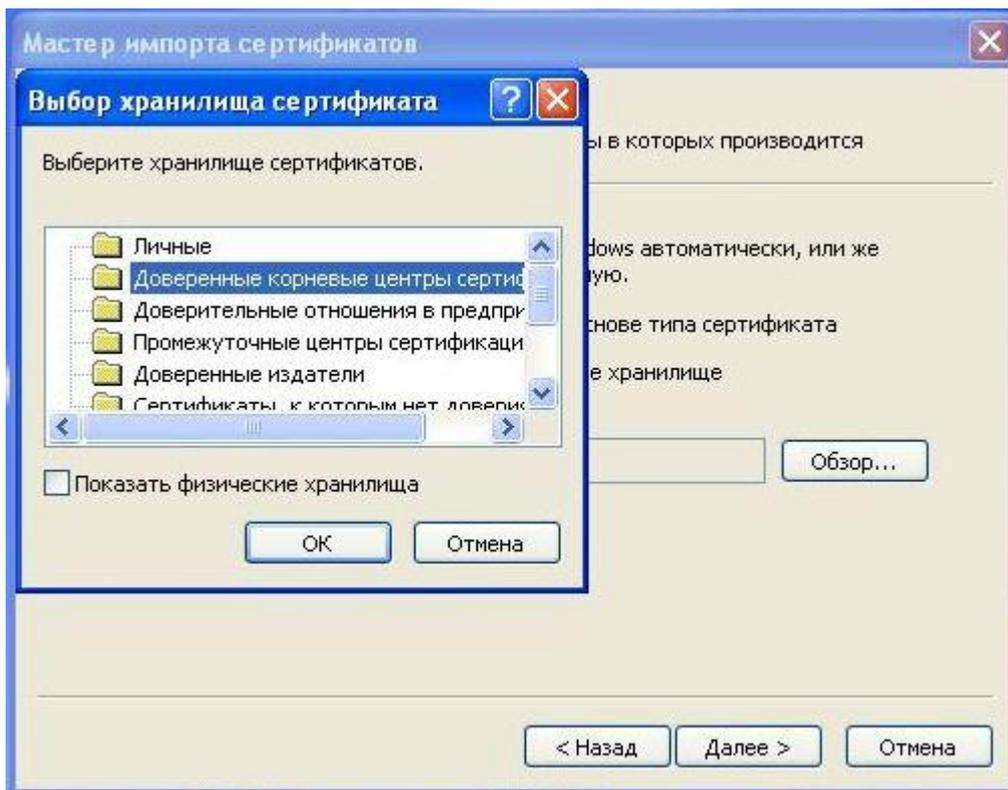


Рисунок: Выбор хранилища для сертификата Удостоверяющего центра

6. В окне **Мастер импорта сертификатов** нажмите **Далее**.

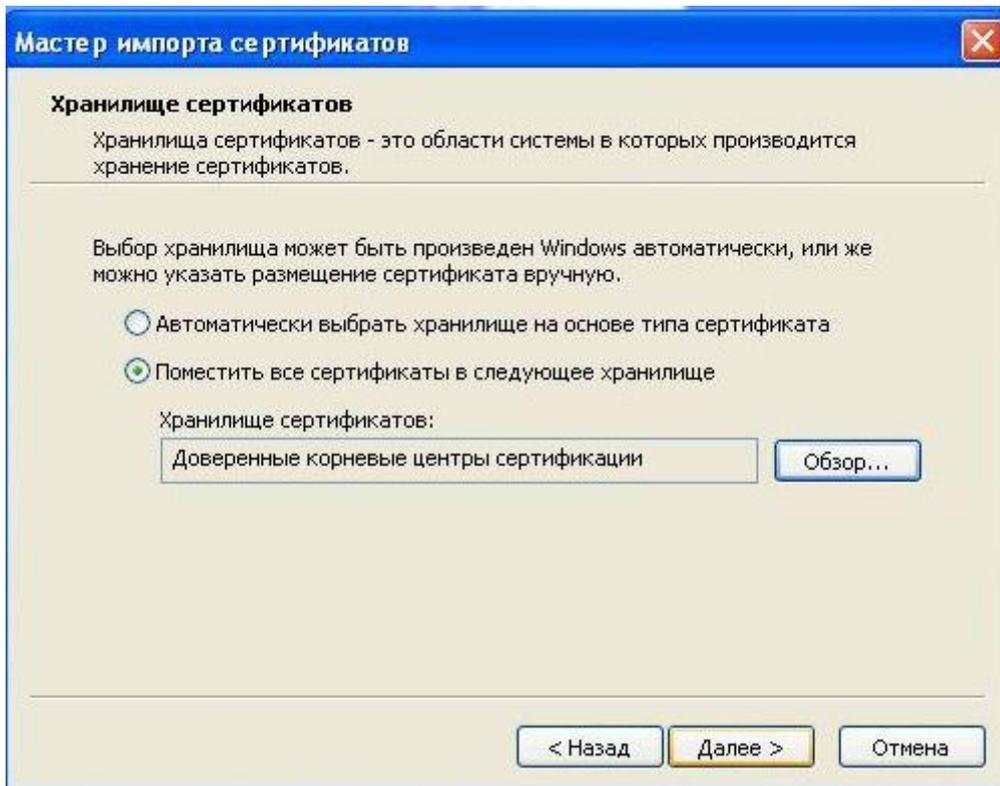


Рисунок: Окно мастера импорта сертификатов

7. На следующей странице нажмите **Готово**.

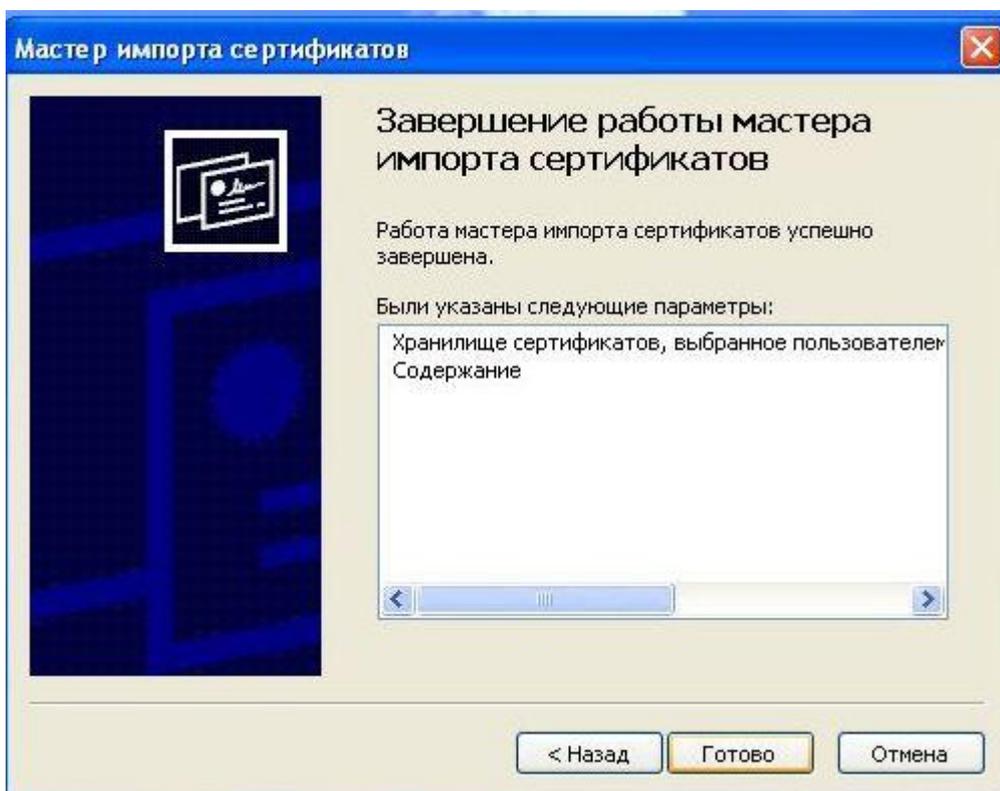


Рисунок: Окно завершения работы мастера импорта сертификатов

8. Ответьте **Да** на предупреждение системы безопасности.

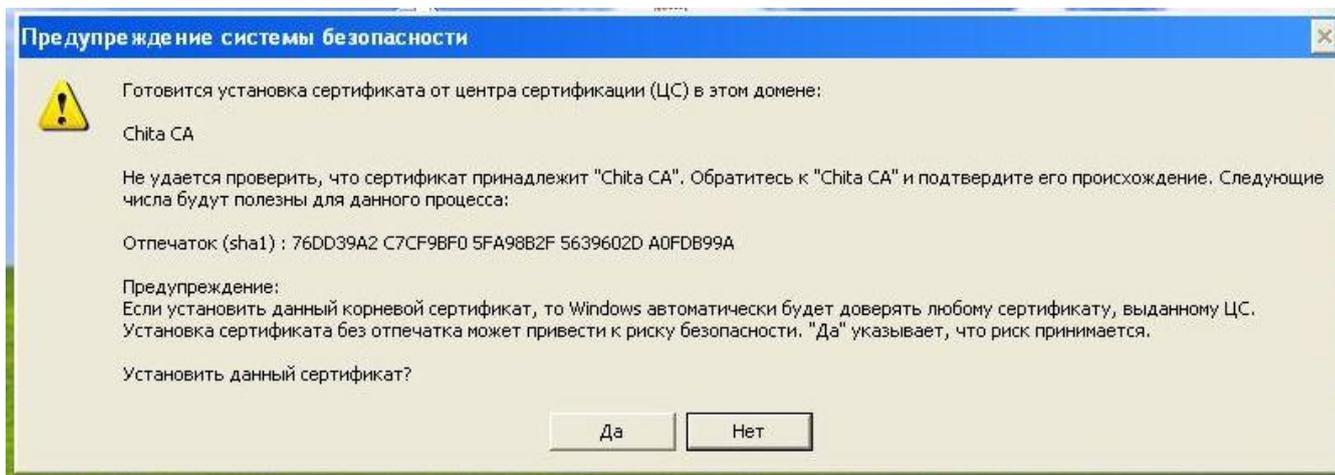


Рисунок: Окно предупреждения системы безопасности

9. В окне **Мастер импорта сертификатов** появится сообщение об успешном импорте сертификата. Нажмите **ОК**, установка завершена.

## Установка СОС:

1. Откройте папку с файлом СОС и щелкните правой кнопкой мыши по значку списка.
2. В контекстном меню выберите пункт **Установить список отзыва (CRL)**.

**Примечание:** отсутствие вкладки **Установить список отзыва (CRL)** свидетельствует о том, что вы используете несертифицированную копию операционной системы Windows, из которой вырезаны средства работы с сертификатами, в этом случае следует установить сертифицированную версию Windows.

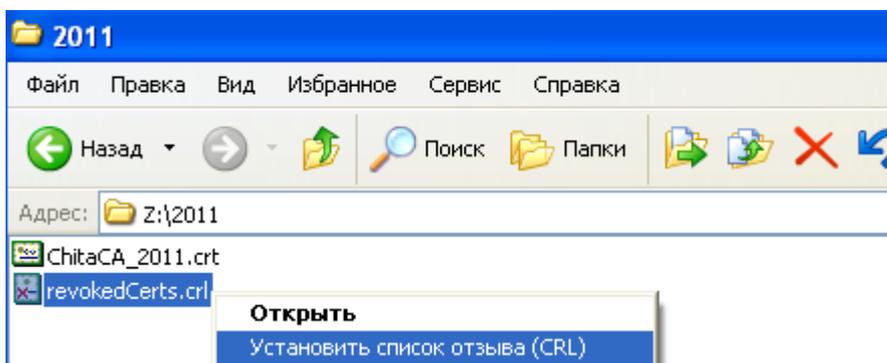


Рисунок: Установка СОС

3. Далее на все предложения мастера установки нажимайте кнопку **Далее**, в конце работы нажмите кнопку **Готово**, дождитесь окончания работы мастера и сообщения об успешном завершении работы.