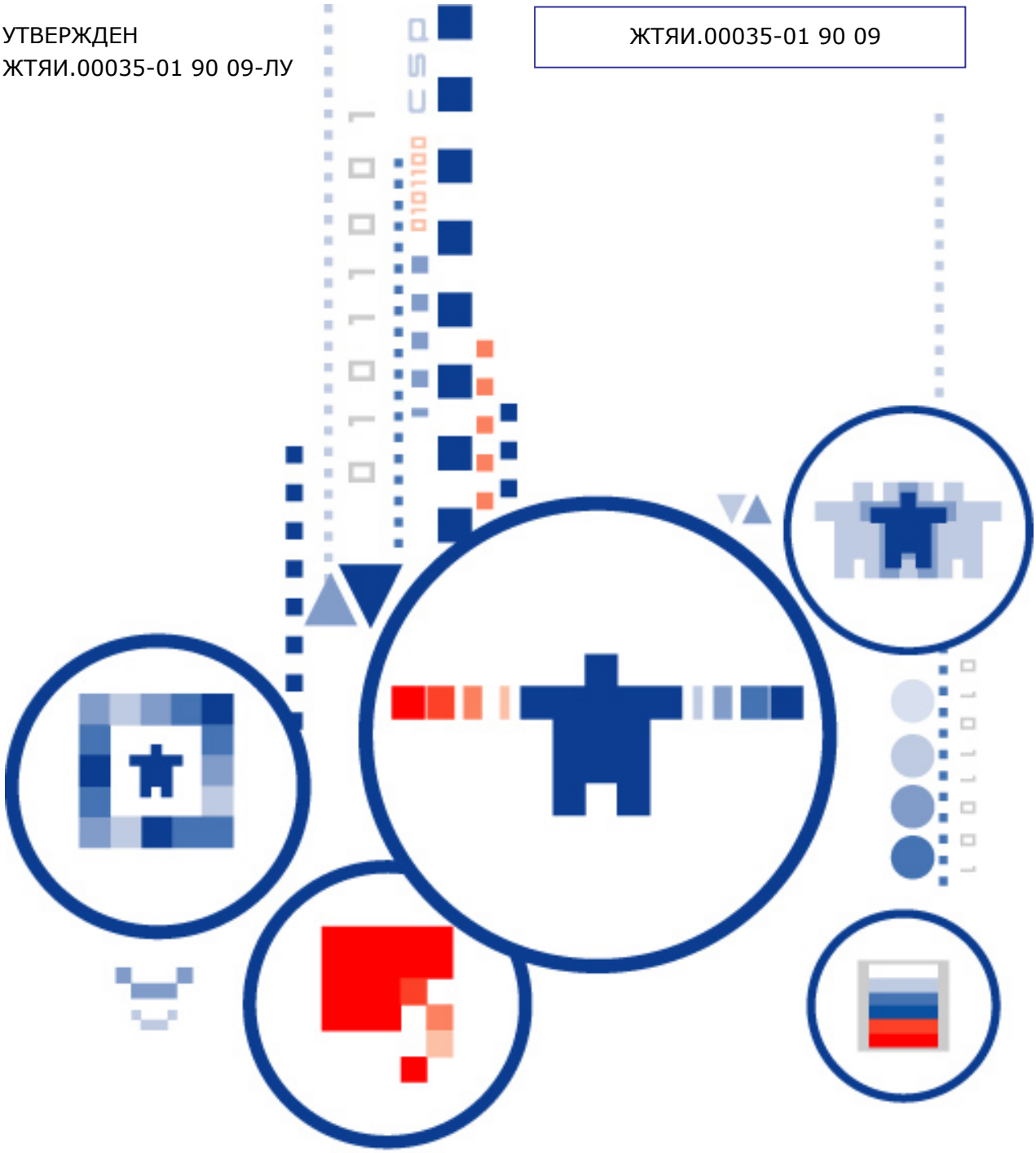
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 09-ЛУ

ЖТЯИ.00035-01 90 09



КриптоПро УЦ

программно-аппаратный комплекс
удостоверяющий центр

Руководство пользователя

АННОТАЦИЯ

Настоящий документ содержит описание эксплуатации веб-приложений Центра Регистрации программного комплекса «Удостоверяющий Центр «КриптоПро УЦ» (УЦ).

К веб-приложениям Центра Регистрации относятся:

- АРМ регистрации пользователя;
- АРМ зарегистрированного пользователя с маркерным доступом;
- АРМ зарегистрированного пользователя с ключевым доступом.

АРМы пользователя являются Web-приложениями, размещенными на Web-узле Центра регистрации.

Приложение АРМ зарегистрированного пользователя с ключевым доступом предназначено для пользователя Центра регистрации, зарегистрированного Администратором ЦР установленным порядком и имеющего как минимум один действующий сертификат. Предназначено для выполнения следующих задач:

- Генерация личных закрытых и открытых ключей и запись их на ключевой носитель;
- Управление личными пользовательскими сертификатами;
- Получения сертификата Центра сертификации УЦ;
- Получения списка отозванных сертификатов УЦ;
- Поиск и получение (импорт) сертификатов других зарегистрированных пользователей УЦ.

Приложение АРМ зарегистрированного пользователя с маркерным доступом предназначено для пользователя Центра регистрации, зарегистрированного Администратором ЦР установленным порядком, имеющего маркер временного доступа и не имеющего ни одного действующего сертификата. Предназначено для выполнения следующих задач:

- Генерация личных закрытых и открытых ключей и запись их на ключевой носитель;
- Получения сертификата Центра сертификации УЦ.

Приложение АРМ регистрации пользователя предназначено для пользователя Центра регистрации, проходящего процедуру регистрации в распределенном режиме установленным порядком, и предназначен для решения следующих задач:

- Формирование пользователем запроса на регистрацию и отправка его в Центр регистрации.

Информация о разработчике ПК «КриптоПро УЦ»:

ООО "Крипто-Про"

127 018, Москва, улица Сущевский вал, 16 строение 5

Телефон: (495) 780 4820

Факс: (495) 780 4820

http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Требования для работы с приложением

Для эксплуатации АРМ пользователя необходимо следующее программное обеспечение:

- Операционная система Microsoft Windows 98 и выше;
- Microsoft Internet Explorer 5.0 (и выше);
- Microsoft Security Bulletin MS02-048. Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q323172). August 28, 2002.
- Microsoft Security Bulletin MS02-050. Certificate Validation Flaw Could Enable Identity Spoofing (Q328145). September 09, 2002.
- Программная библиотека CAPICOM.dll версии 2.1.0.1 (http://www.microsoft.com/downloads/details.aspx?FamilyID=860ee43a-a843-462f-abb5-ff88ea5896f6&DisplayLang=en)
- Средство криптографической защиты (СКЗИ) КриптоПро CSP;
- Модуль поддержки сетевой аутентификации СКЗИ КриптоПро CSP (КриптоПро TLS).

2. Объекты управления

2.1. Сертификат открытого ключа

Сертификат — это электронный документ, который содержит открытый ключ пользователя и подписан электронной цифровой подписью его издателя, т.е. Удостоверяющего центра. Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, которая его идентифицирует.

2.2. Список отозванных сертификатов

Список отозванных сертификатов (CRL – Certificate Revocation List) – это электронный документ, который содержит перечень сертификатов, являющихся отозванными из обращения в ПАК «КриптоПро УЦ». Удостоверяющий центр поддерживает отзыв сертификатов и публикацию списков отозванных сертификатов. Абоненты могут получить эту информацию и записать ее в свое локальное хранилище, чтобы использовать для последующей проверки сертификатов.

2.3. Запрос на регистрацию

Запрос на регистрацию — сообщение, содержащее необходимую информацию для регистрации пользователя в ПАК «КриптоПро УЦ».

Формируется при регистрации пользователя, после чего передается на Центр регистрации. Обработка осуществляется администратором УЦ со своего рабочего места. Результатом обработки является формирование учетной записи пользователя в Базе Данных Центра регистрации или сообщение об ошибке.

2.4. Запрос на сертификат

Запрос на сертификат — сообщение, содержащее необходимую информацию для получения сертификата. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр регистрации Удостоверяющему Центру, где и обрабатывается. Результатом обработки является выпущенный сертификат или сообщение об ошибке.

2.5. Запрос на отзыв сертификата

Запрос на отзыв сертификата — сообщение, содержащее необходимую информацию для выполнения процедуры отзыва сертификата пользователя из обращения в системе. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр регистрации Удостоверяющему Центру, где и обрабатывается. Результатом обработки является занесение сертификата в список отозванных сертификатов или сообщение об ошибке.

2.6. Служебные ключи и сертификаты

Процесс регистрации пользователей в ПАК «КриптоПро УЦ» предусматривает централизованное изготовление служебных (закрытых) ключей и сертификатов пользователей администратором безопасности. Служебные ключи предназначены для подтверждения подлинности пользователя при формировании им рабочих закрытых ключей и передаче запроса на сертификат в Центр регистрации ПАК «КриптоПро УЦ». Часто служебные ключи и сертификаты называют «временными». Это происходит в тех случаях, когда такой ключ действует очень короткое время, а именно до получения при помощи него первого «рабочего» ключа.

2.7. Рабочие ключи и сертификаты

После процесса регистрации пользователи с использованием служебных ключей и сертификатов должны сформировать рабочие ключи и получить рабочие сертификаты. Рабочие ключи предназначены для формирования ЭЦП, выполнения операций шифрования сообщений, аутентификации пользователя при его взаимодействии с ЦР и плановой смене ключей. Запрос на сертификат от пользователя будет обработан Центром регистрации только в случае, если он подписан служебным ключом или действующим закрытым ключом пользователя.

Примечание. Разделение понятий «служебные ключи», «служебный сертификат» и соответствующих им «рабочие ключи», «рабочий сертификат» чисто условно. Наиболее частая практика регистрации новых пользователей и выдачи им первых сертификатов сводится к формированию и выдаче им временных ключей и сертификатов, действующих довольно короткое время и предназначенных лишь для того, чтобы пользователь смог с их помощью идентифицироваться в АРМ пользователя, после чего сформировать уже «рабочие» ключи и сертификат. Часто это сводится к практике централизованного изготовления ключей администратором безопасности организации и выдаче этих ключей и сертификатов пользователям на ключевых носителях. Настоящая версия Удостоверяющего центра позволяет гибко манипулировать этими понятиями, настраиваться под любые потребности конкретных организаций, эксплуатирующих УЦ. Вполне реальна ситуация, когда никаких «служебных» ключей и сертификатов не возникает. При этом сразу формируются обычные «рабочие» ключи/сертификаты, неважно, в процессе ли регистрации пользователя, или при централизованном распределении ключей. Но в целях отличия самого первого сертификата от всех последующих, полученных одним пользователем, мы в данном руководстве первоначальные ключи и сертификат будем называть «служебными» (иногда их еще называют «временными»). В результате такого сценария, после получения и установки служебного сертификата, пользователь получает статус зарегистрированного и для продолжения дальнейшей работы выполняет процедуру получения нового, рабочего сертификата самостоятельно, в АРМ пользователя.

3. Настройка рабочего места пользователя

Перед началом работы с АРМами пользователя ЦР необходимо выполнить следующие процедуры:

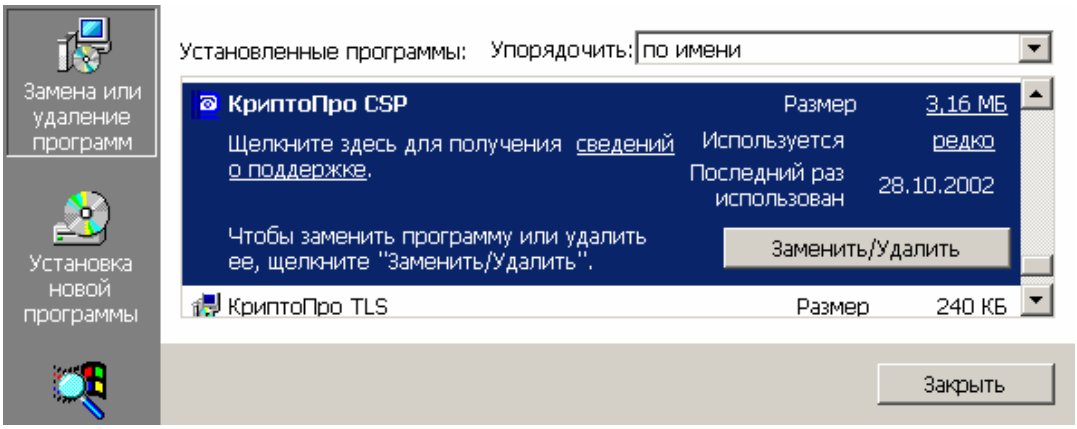
- Получить от администратора ЦР или скачать с Web сервера ЦР дистрибутивы программного обеспечения СКЗИ «КриптоПро CSP» и «КриптоПро TLS»
- Установить СКЗИ «КриптоПро CSP», «КриптоПро TLS»
- Установить сертификат ЦС
- Установить личный сертификат с ключевого носителя, полученного от администратора ЦР в случае регистрации пользователя в централизованном режиме.

Процедура получения указанных компонент регламентируется политикой конкретного Удостоверяющего Центра. В том случае, если регламентом УЦ разрешена процедура регистрации пользователя в распределенном режиме, то Удостоверяющий Центр должен предоставить пользователю все необходимые компоненты для выполнения процедур настройки рабочего места пользователя.

3.1. Установка дистрибутива ПО СКЗИ КриптоПро CSP

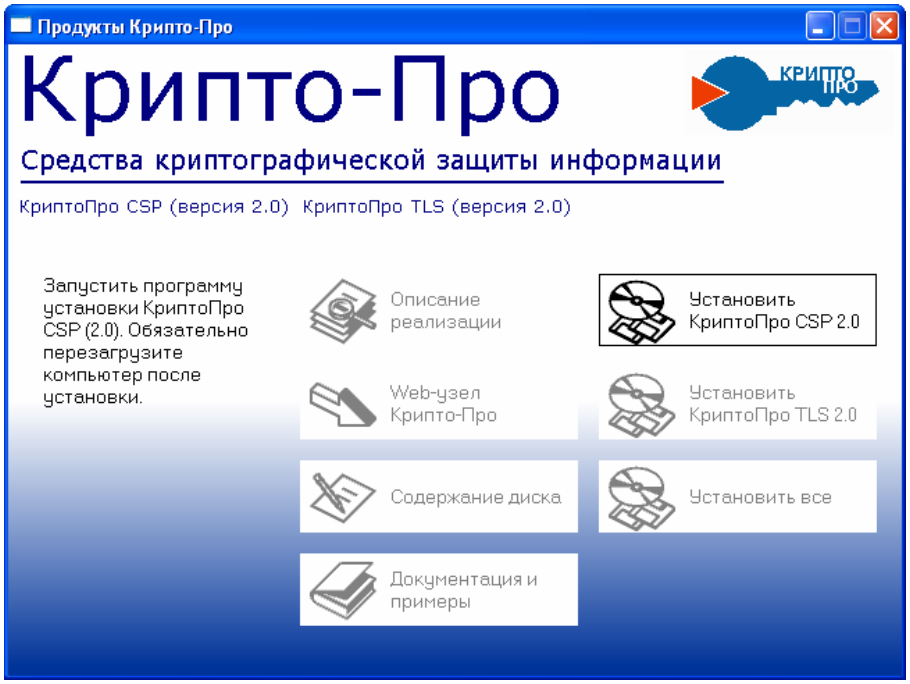
Установка дистрибутива должна производится пользователем, имеющим права администратора на локальном компьютере. Перед установкой дистрибутива КриптоПро CSP, удалите все ранее существовавшие версии устанавливаемого программного обеспечения. Если модуль криптографической поддержки не удален, новая версия не будет установлена. Для этого используйте пункты основного меню Windows **Пуск, Настройка, Панель управления, Установка и удаление программ** (см. Рисунок 1).

Рисунок 1. Окно удаления устаревших версий СКЗИ КриптоПро CSP

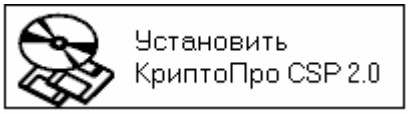


Для установки программного обеспечения вставьте компакт-диск с дистрибутивом СКЗИ в привод считывателя. Программа установки запустится автоматически (см. Рисунок 2). Если компьютер не настроен на автоматический запуск приложений с компакт-диска, запустите программу **AUTORUN.EXE** (для версии 2.0; **LAUNCH.EXE** – для версии 3.0) с компакт-диска.

Рисунок 2. Содержание диска КриптоПро CSP 2.0



Для дальнейшей установки КриптоПро CSP 2.0, выберите значок **Установить КриптоПро CSP 2.0**.

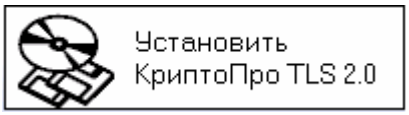


Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

3.2. Установка КриптоПро TLS

Программное обеспечение КриптоПро TLS является реализацией протокола TLS и использует криптографические функции КриптоПро CSP для обеспечения процесса аутентификации и шифрования трафика между клиентом и сервером.

Для установки программного обеспечения КриптоПро TLS с компакт-диска (см. Рисунок 2) выберите значок **Установить КриптоПро TLS 2.0**

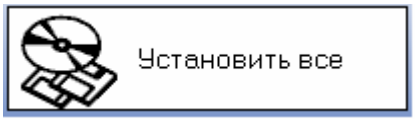


Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

3.3. Установка СКЗИ КриптоПро CSP и КриптоПро TLS

Программа установки обеспечивает дополнительный режим установки, так называемый режим **установить все**. Это режим позволяет обеспечить последовательную установку ПО СКЗИ КриптоПро CSP и КриптоПро TLS без перезагрузок компьютера после установки каждой компоненты.

Для установки программного обеспечения СКЗИ КриптоПро CSP и КриптоПро TLS с компакт-диска (см. Рисунок 2) выберите значок **Установить все**



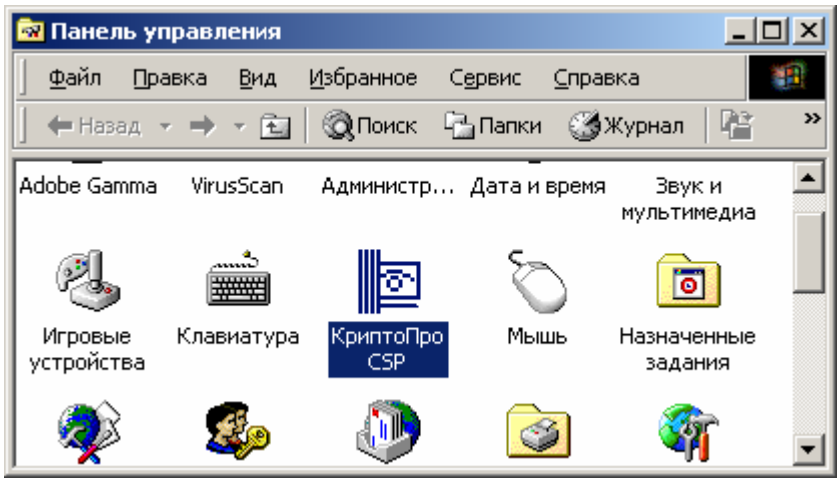
Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

Примечание: в версии 3.0 дистрибутивы КриптоПро CSP и КриптоПро TLS не разделяются и при запуске программы установки устанавливаются оба.

3.4. Изменение набора устройств хранения ключевой информации

Программа установки по умолчанию устанавливает все модули, обеспечивающие работу с различными поддерживаемыми устройствами хранения ключевой информации, но при этом настройки КриптоПро CSP допускают использовать в качестве ключевого носителя только дискету 3,5". Если для работы с КриптоПро CSP необходимы дополнительные типы устройств работы с ключевыми носителями, выберите режим изменения их состава.

Рисунок 3. Панель управления



Для этого откройте панель управления компьютером, используя пункты меню **Пуск, Настройка, Панель управления** и в окне панели управления (см. Рисунок 3) выберите значок **КриптоПро CSP**. В панели настройки СКЗИ КриптоПро CSP (см. Рисунок 4) выберите закладку **Оборудование** и, нажав кнопку **Настроить считыватели/Configure carriers**, добавьте (или удалите) из списка те устройства, которые будут использованы в качестве считывателей ключевой информации (см. Рисунок 5).

Рисунок 4. Вкладка Оборудование окна свойств приложения КриптоПро CSP

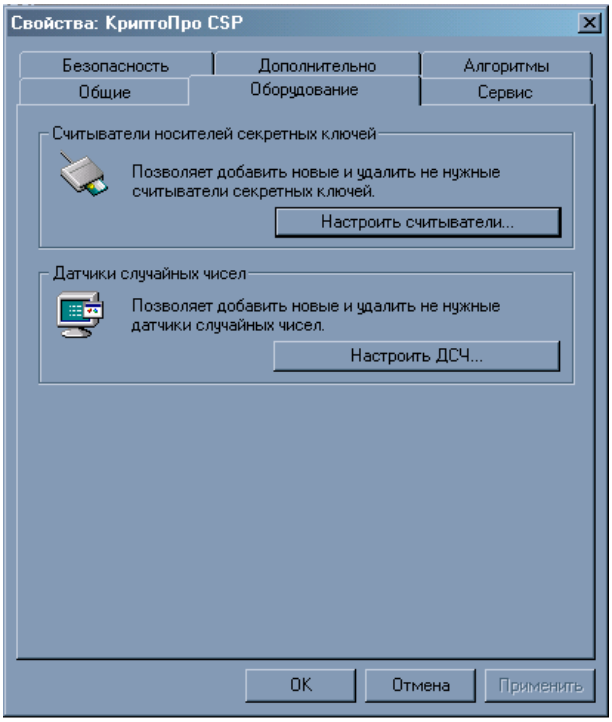
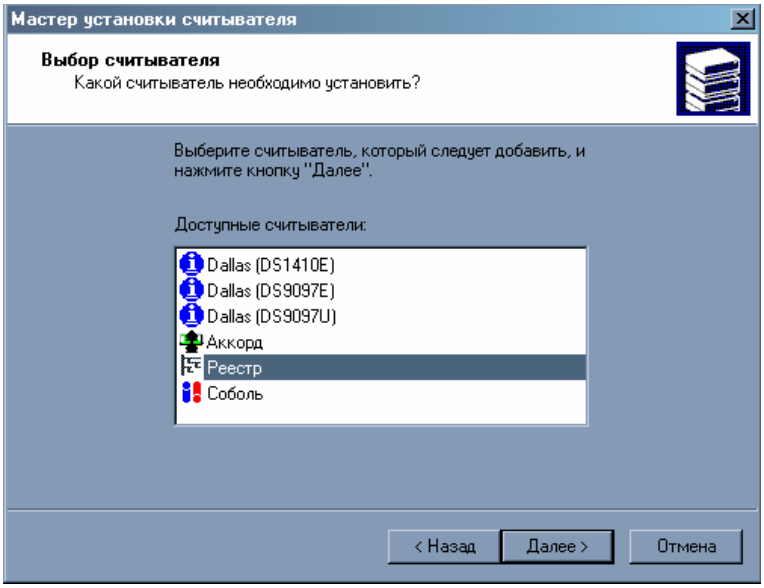


Рисунок 5. Окно выбора устройства хранения ключей Мастера установки считывателя



- В состав дистрибутива СКЗИ КриптоПро CSP не входят драйвера и другие модули третьих производителей, обеспечивающие взаимодействие КриптоПро CSP с аппаратной частью. Для их установки нужно воспользоваться программой установки, поставляемой производителями таких устройств, либо получить их с сервера разработчика по адресу http://www.cryptopro.ru/cryptopro/products/csp/readers.htm. Например, если КриптоПро CSP уже установлено, и нужно использовать новые устройства, необходимо установить поддерживающие драйвера и другие модули от производителей этих устройств.

3.5. Лицензия и регистрация ПО СКЗИ

Программное обеспечение КриптоПро CSP распространяется с ограниченным использованием по времени – 30 дней. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер и код активации с Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (Дилера).

Для этого откройте панель управления компьютером, используя пункты меню **Пуск, Настройка**, **Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. В панели настройки СКЗИ КриптоПро CSP (см. Рисунок 6) выберите пункт **Ввод лицензии** и введите **серийный номер** и **ключ активации** с бланка **Лицензии** (см. Рисунок 7).

Рисунок 6. Вкладка общие окно свойств приложения КриптоПро CSP

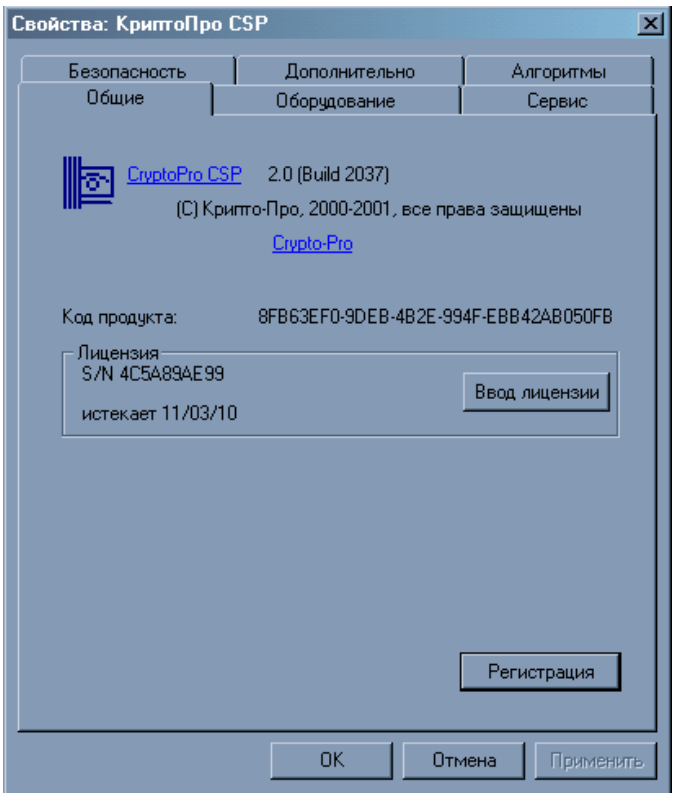
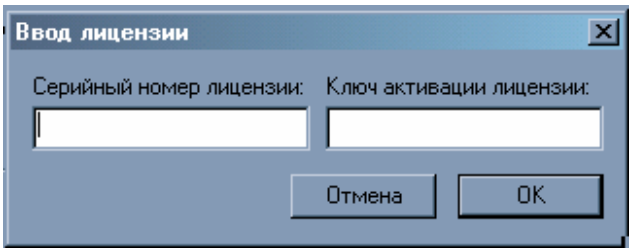


Рисунок 7. Ввод данных лицензии



После завершения программы установки рекомендуется зарегистрировать установленное программное обеспечение КриптоПро CSP у организации-разработчика. Для этого откройте панель управления компьютером, используя пункты меню **Пуск, Настройка, Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**.

В панели настройки СКЗИ КриптоПро CSP (см. Рисунок 6) выберите пункт **Регистрация**, и выполните регистрацию.

3.6. Настройка КриптоПро CSP

КриптоПро CSP может функционировать и хранить ключевую информацию в двух режимах:

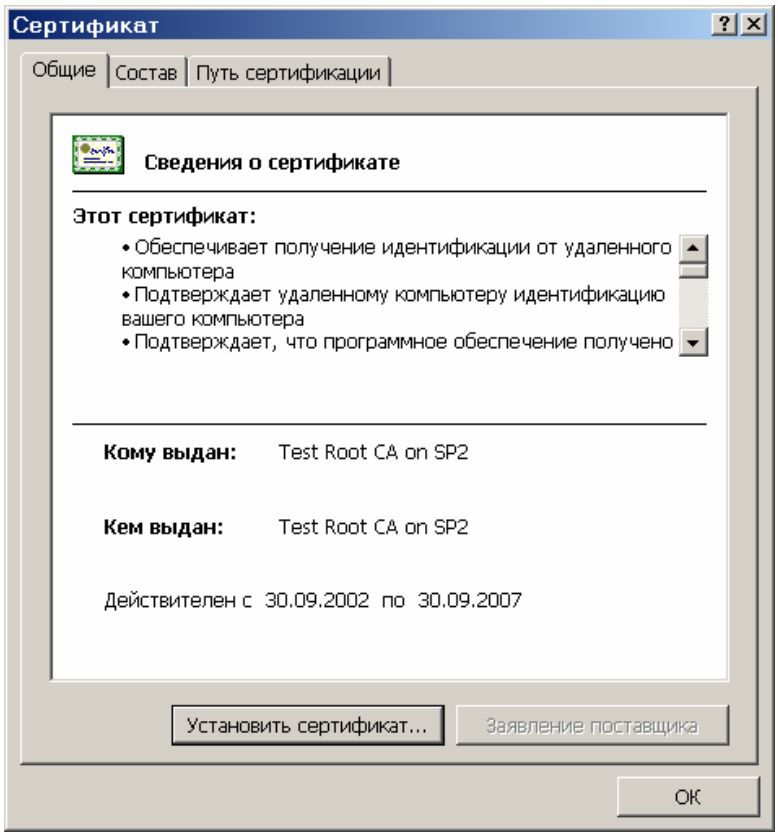
- В памяти приложения.
- В "Службе хранения ключей", которая реализована в виде системного сервиса.

Функционирование КриптоПро CSP в "Службе хранения ключей" обеспечивает дополнительную защиту ключевой информации от других приложений, выполняющихся на компьютере, но может незначительно снизить производительность. Для изменения режима функционирования СКЗИ откройте панель настроек КриптоПро CSP, как описано в предыдущем пункте, и выберите необходимый режим.

3.7. Установка Сертификата Центра сертификации

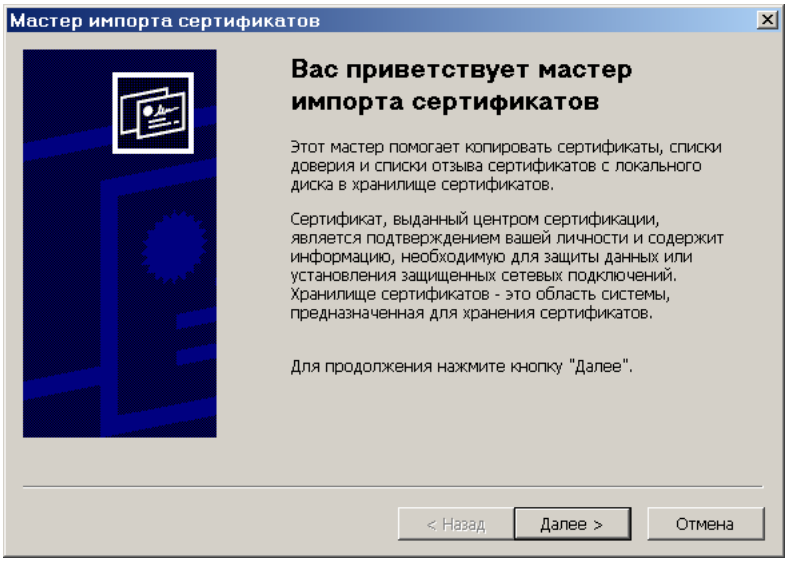
- Для установки сертификата ЦС необходимо открыть файл, содержащий сертификат ЦС, с использованием Проводника ОС MS Windows.

Рисунок 8. Окно просмотра сертификата Центра Сертификации



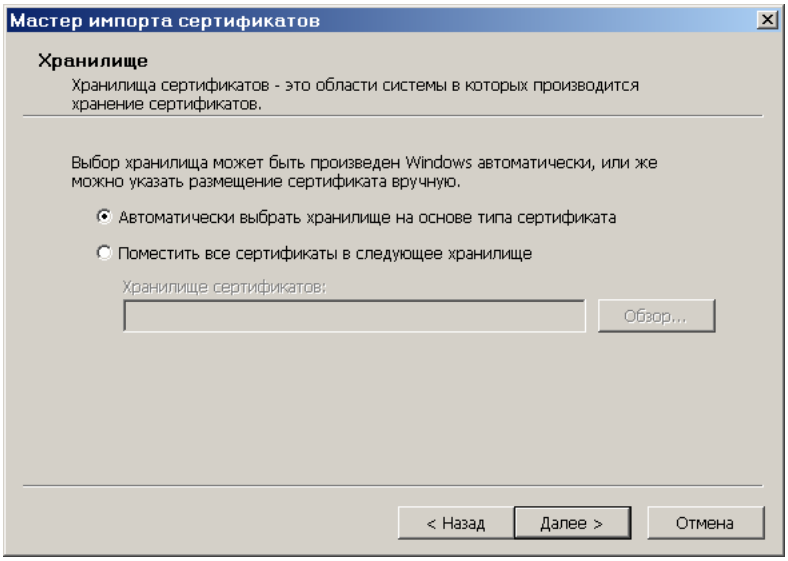
- Нажать кнопку **Установить сертификат** и с помощью Мастера импорта сертификатов (см. Рисунок 9) произвести установку сертификата в Хранилище сертификатов компьютера.

Рисунок 9. Окно Мастера импорта сертификатов



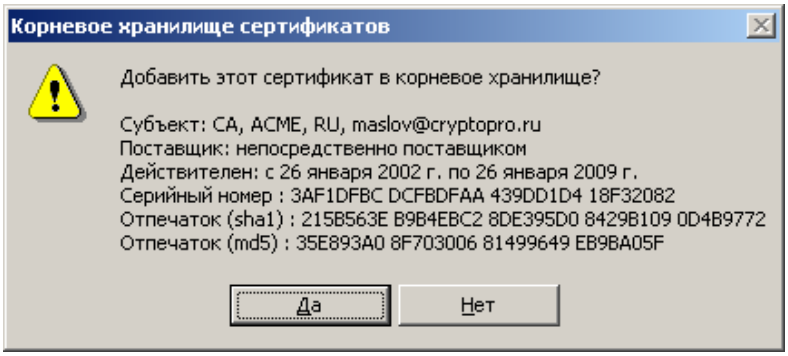
- В процессе работы Мастера, в качестве хранилища сертификатов выбрать опцию автоматического определения хранилища на основе типа сертификата (см. Рисунок 10).

Рисунок 10. Окно выбора хранилища сертификатов Мастера импорта сертификатов



- При появлении сообщения (см. Рисунок 11) о добавлении сертификата в корневое хранилище нажать кнопку **Да**. Появление данного сообщения свидетельствует об успешной установке сертификата Центра Сертификации. Отсутствие сообщения свидетельствует о том, что данный сертификат ранее был уже установлен на данный компьютер или он не является корневым сертификатом Центра Сертификации.

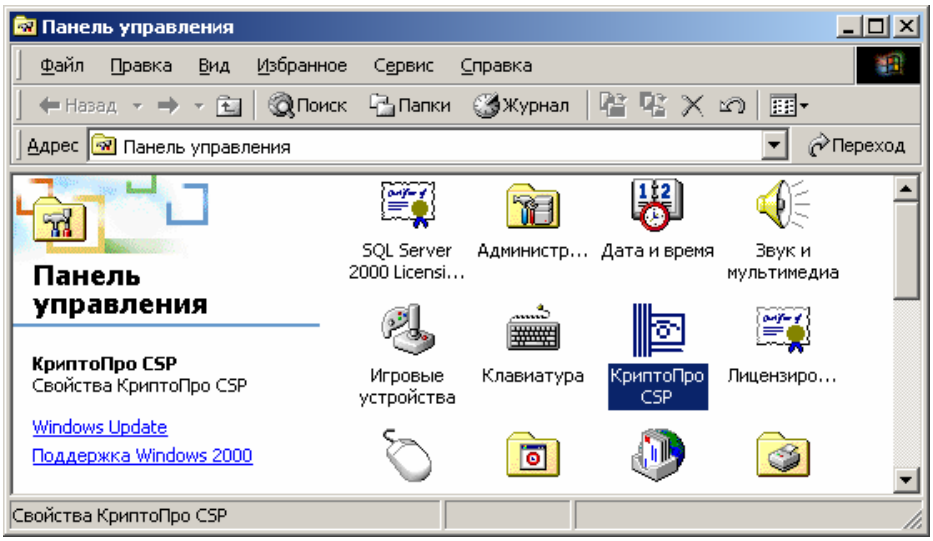
Рисунок 11. Окно сообщения о добавлении сертификата в корневое хранилище



3.8. Установка личного служебного сертификата пользователя, выданного администратором ЦР

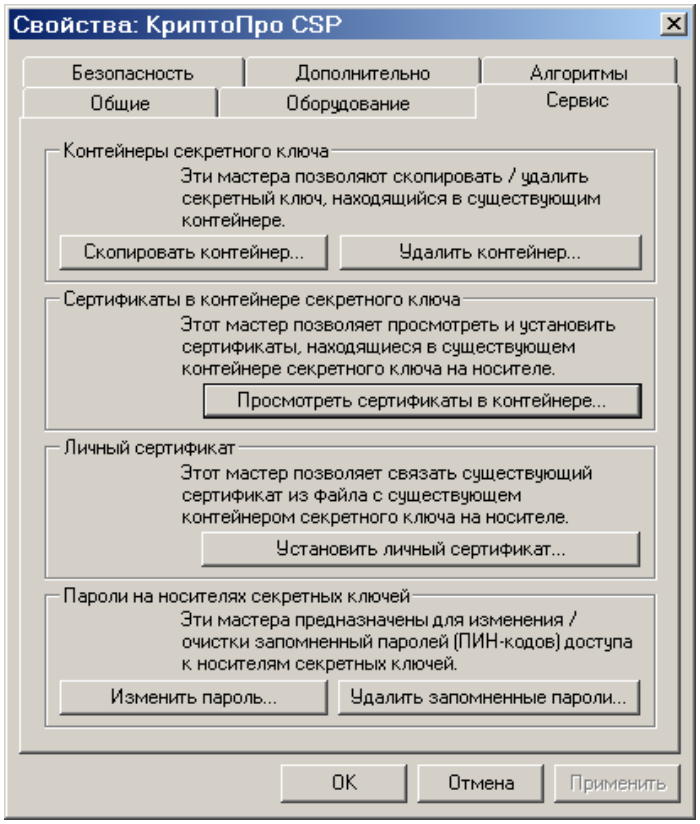
- Для установки личного сертификата с ключевого носителя необходимо воспользоваться интерфейсом СКЗИ «КриптоПро CSP», доступного из Панели управления (см. Рисунок 12).

Рисунок 12. Окно панели управления



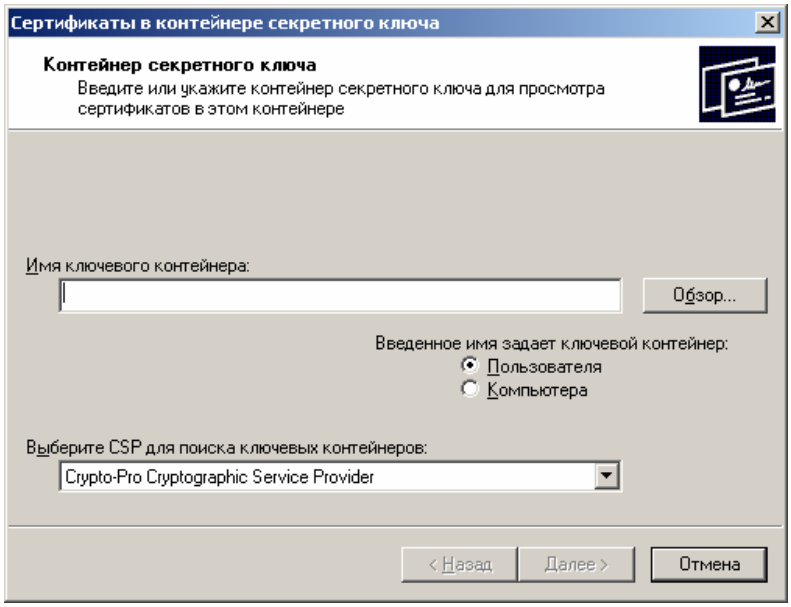
- Запустите приложение КриптоПро CSP из Панели и установите сертификат с ключевого носителя. Для этого выполните следующие процедуры:
  - На вкладке **Сервис** окна свойств приложения КриптоПро CSP (см. Рисунок 13) нажмите кнопку **Просмотреть сертификаты в контейнере**

Рисунок 13. Вкладка Сервис окна свойств приложения КриптоПро CSP



- В открывшемся окне нажмите кнопку **Обзор** для выбора ключевого контейнера (см. Рисунок 14)

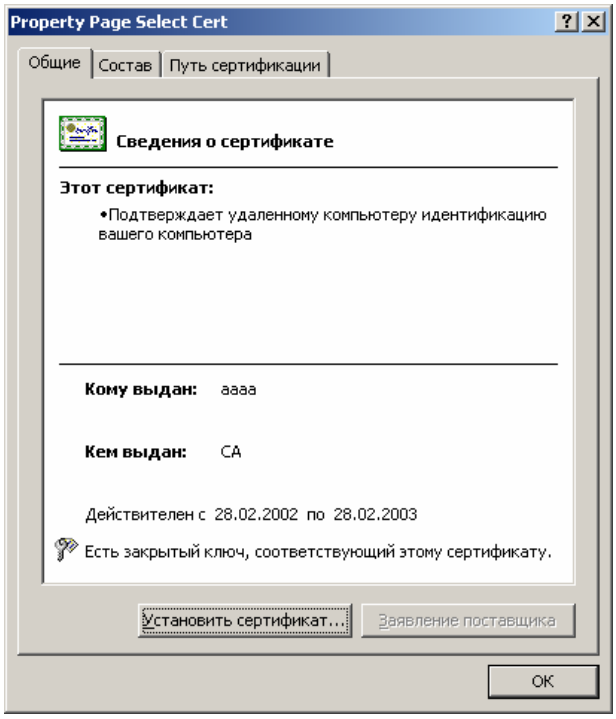
Рисунок 14. Окно выбора контейнера для установки сертификата



- В появившемся списке ключевых контейнеров установите курсор на соответствующий контейнер и нажмите кнопку **OK**.
- Для продолжения работы нажмите кнопку **Далее**
- В появившемся окне будет отражена информация из сертификата, расположенного в ключевом контейнере. Убедитесь в соответствии данной информации Вашим персональным данным. В случае, если данные совпадают, нажмите кнопку **Свойства**. Если данные не совпадают (выбран не тот ключевой контейнер), повторите процедуру выбора имени ключевого контейнера.

- После нажатия кнопки **Свойства** на экране отображается окно с полной информацией о сертификате (см. Рисунок 15).

Рисунок 15. Окно свойств сертификата из ключевого контейнера



- Продолжая процедуру установки сертификата, нажмите кнопку **Установить сертификат**
- В соответствии с работой Мастера импорта сертификатов, произведите установку данного сертификата в хранилище на рабочее место (компьютер).
- При работе Мастера рекомендуется выбирать предлагаемые им значения по умолчанию, т.е. нажимать кнопки **Далее** и **Готово**
- Появление сообщения об успешном импорте сертификата и возврата к окну с информацией о сертификате (предыдущий рисунок), нажмите кнопку **ОК**
- После этого на окне **Сертификат для просмотра** и далее последовательно нажимайте кнопки **Отмена**.

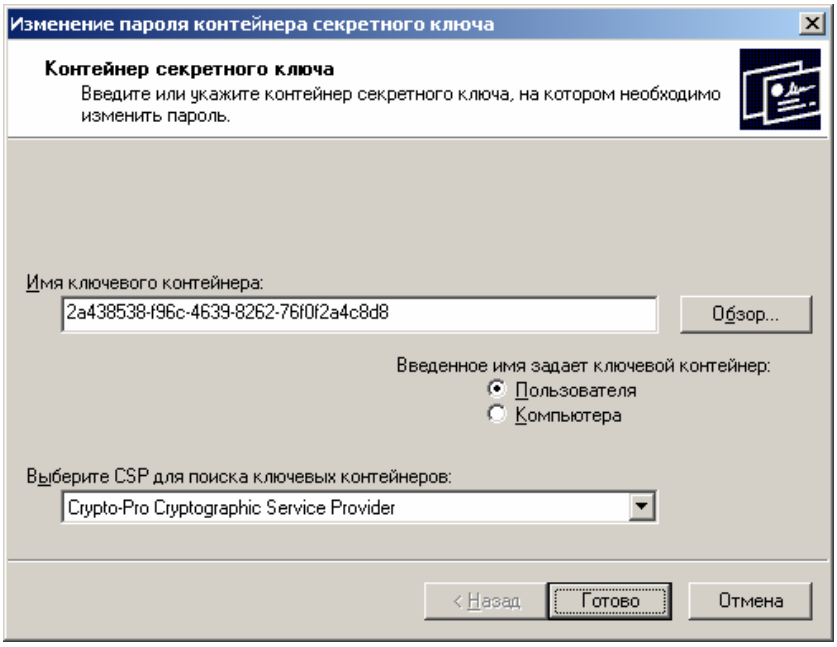
3.9. Дополнительные настройки КриптоПро CSP

В процессе работы с ключами (генерация ключей, использование в процедурах формирования подписи, аутентификации и шифрования), имеется возможность установки на ключевой контейнер дополнительного средства защиты ключевого контейнера, так называемого пароля (PIN-кода).

В процессе эксплуатации ключей, расположенных в ключевом контейнере, возможна смена данного пароля. Регламент смены пароля определяется пользователем самостоятельно. Процедура смены пароля выполняется следующим образом:

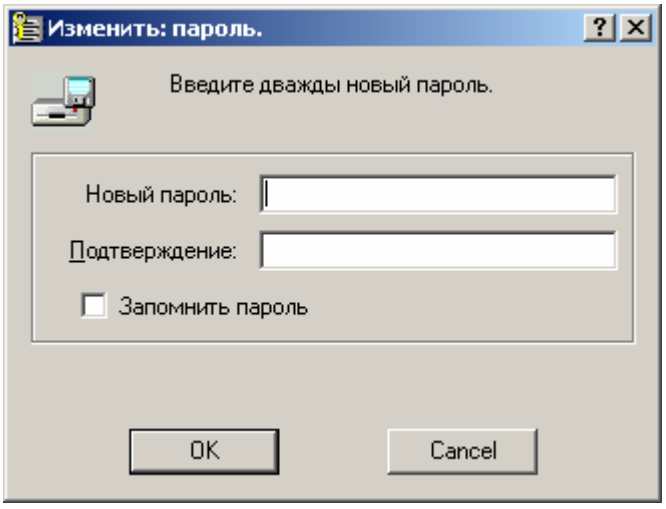
- Из Панели управления запустить приложение КриптоПро CSP
- Открыть вкладку **Сервис** (см. Рисунок 13) и нажать кнопку **Изменить пароль**
- Аналогично тому, как описано в пункте установки личного сертификата из ключевого контейнера, выберите необходимый ключевой контейнер и нажмите кнопку **Готово**. (см. Рисунок 16).

Рисунок 16. Окно изменения пароля ключевого контейнера



- В появившемся окне введите существующий пароль на ключевой контейнер
- В случае если Вы забыли свой пароль, обратитесь к Администратору системы за инструкцией по дальнейшим действиям
- В случае успешного ввода пароля, в появившемся окне (см. Рисунок 17) введите дважды новый пароль и нажмите кнопку **ОК**

Рисунок 17. Окно ввода пароля на ключевой контейнер



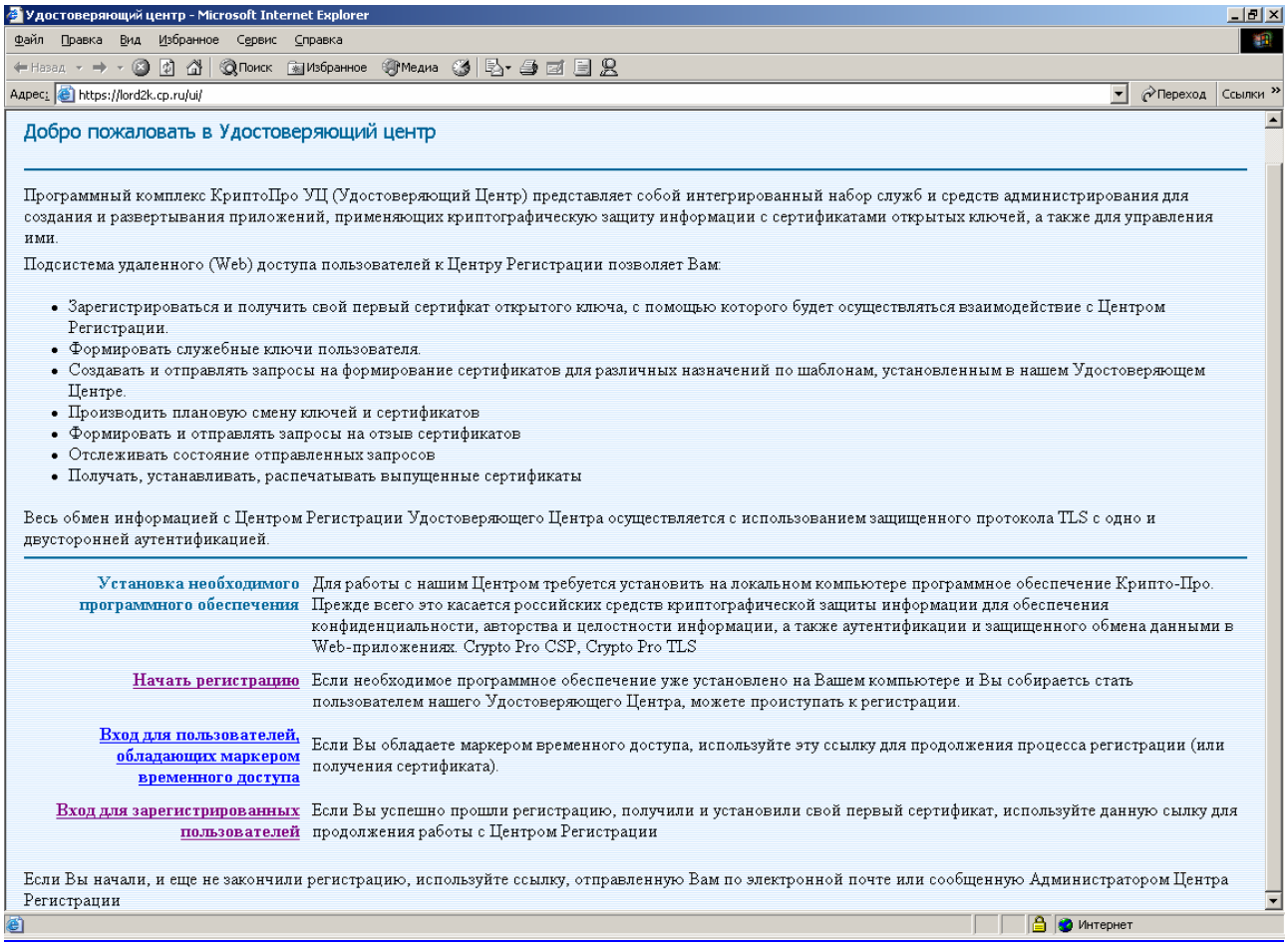
- После закрытия окна с вводом пароля, повторно запустите приложение КриптоПро CSP из Панели управления (см. Рисунок 12) и нажмите кнопку **Отмена**

4. АРМ зарегистрированного пользователя с ключевым доступом

4.1. Запуск АРМ зарегистрированного пользователя с ключевым доступом

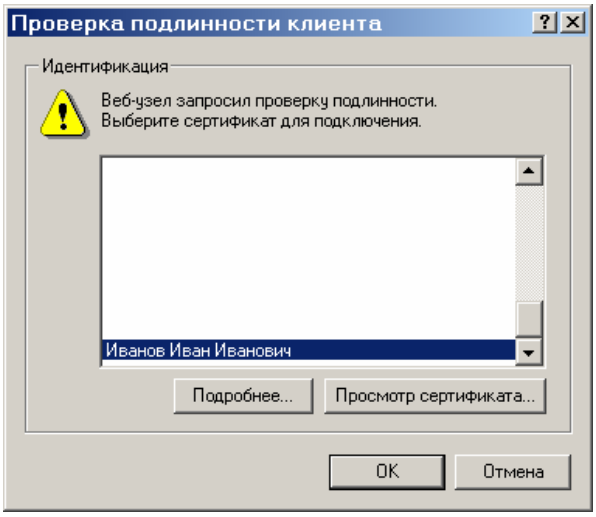
Для запуска и работы с АРМ пользователя необходимо открыть окно браузера MS IE и перейти по адресу https://имя_сервера_ЦР/UI/User/User.ASP, где имя_сервера_ЦР – имя Web-узла Центра регистрации, или воспользоваться стартовой страничкой Web-приложений Центра регистрации (см. Рисунок 18), где выбрать режим **Вход для зарегистрированных пользователей**.

Рисунок 18. Стартовая страница Web-приложений Центра Регистрации



Для аутентификации пользователя на ЦР и получения доступа к АРМ пользователя необходимо в процессе запуска выбрать сертификат пользователя, по которому будет выполняться процедура аутентификации. Данный выбор происходит в окне проверки подлинности клиента приложения MS IE (см. Рисунок 19).

Рисунок 19. Окно выбора сертификата для проверки подлинности клиента

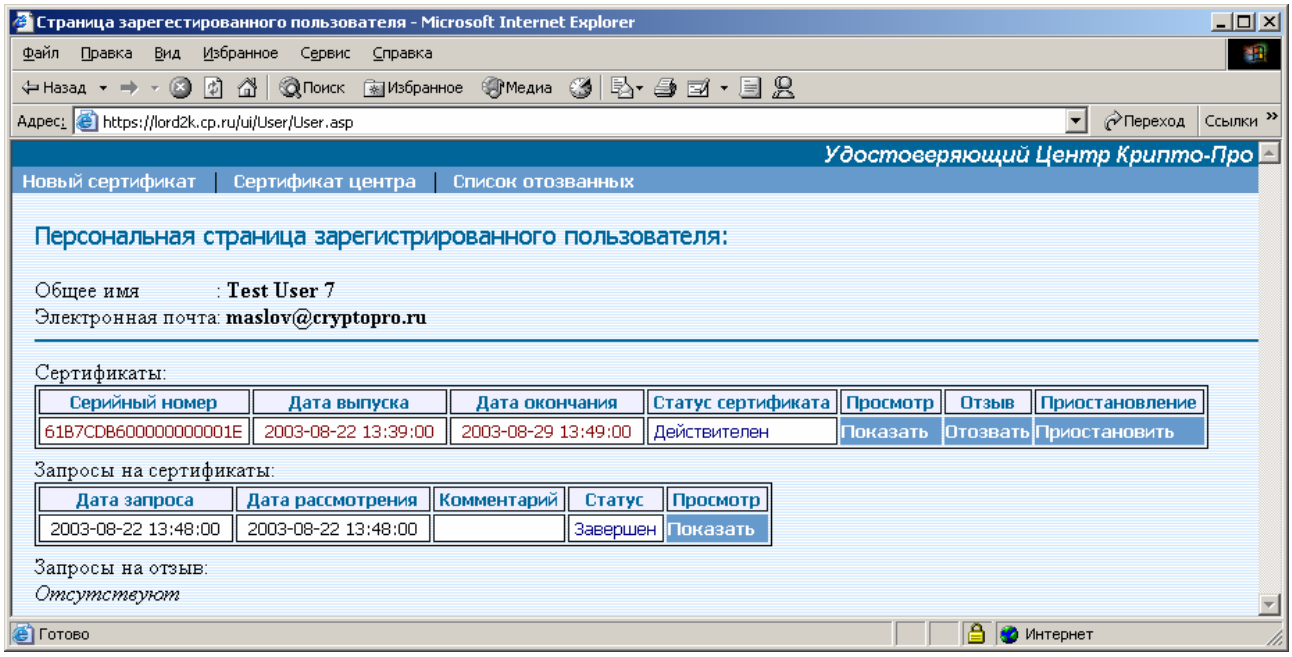


В данном окне отображается список сертификатов пользователя, установленных в хранилище сертификатов текущего пользователя локального компьютера. Необходимо установить курсор на нужном сертификате и нажать кнопку **ОК**. Для просмотра информации о сертификате воспользуйтесь кнопкой **Просмотр сертификата**.

4.2. Работа в АРМ зарегистрированного пользователя с ключевым доступом

Основное окно Web-приложения Центра Регистрации АРМ зарегистрированного пользователя с ключевым доступом имеет следующий вид (см. Рисунок 20):

Рисунок 20. Окно АРМа зарегистрированного пользователя



В верхней части окна расположена область основных режимов работы пользователя, которая содержит три кнопки:

1. **Новый сертификат** – режим работы по созданию новых ключей и запроса на сертификат пользователя

2. **Сертификат центра** – получение и установка на локальном компьютере сертификата Центра сертификации
3. **Список отозванных** – получение списка отозванных сертификатов данного Центра сертификации

Ниже области режимов работы расположена информация о текущем пользователе, сформированная во время его регистрации

Далее в виде таблиц идет информация о выпущенных сертификатах, запросах на сертификаты, запросах на отзыв сертификатов.

Таблица со списком сертификатов пользователя имеет следующие колонки:

- **Серийный номер** – серийный номер сертификата, соответствующего текущей строке таблицы
- **Дата выпуска** – Дата/время выпуска сертификата. С этого момента сертификат считается действительным и может использоваться по назначению, указанному в сертификате.
- **Дата окончания** - Дата/время окончания действия сертификата. После указанной даты сертификат считается недействительным и не может использоваться по назначению.
- **Статус сертификата** – текущее состояние сертификата. Может принимать следующие значения: **Действителен**, **Запрошен к отзыву**, **Отозван**.
- **Просмотр** – содержит ссылку (кнопку), по нажатию которой можно вывести содержимое сертификата в отдельное окно для просмотра и/или печати на бумажный носитель.
- **Отзыв** - содержит ссылку (кнопку), по нажатию которой можно перейти к режиму работы по формированию запроса на отзыв соответствующего (расположенного в текущей строке таблицы) сертификата. Если же данный сертификат уже отозван, то ссылка не показывается.
- **Приостановление** - содержит ссылку (кнопку), по нажатию которой можно перейти к режиму работы по формированию запроса на приостановление действия соответствующего (расположенного в текущей строке таблицы) сертификата. Если же данный сертификат уже отозван, то ссылка не показывается.

Информация о сертификате открытого ключа, который в данный момент используется для установления защищенного TLS соединения с Web сервером Центра регистрации, показывается красным цветом.

Таблица со списком запросов на сертификаты имеет следующие колонки:

- **Дата запроса** – дата/время формирования запроса на сертификат
- **Дата рассмотрения** – Дата/время принятия или отклонения запроса администратором центра регистрации.
- **Комментарий** – дополнительная информация, указанная пользователем или администратором ЦР при формировании запроса на сертификат.
- **Статус** – Текущее состояние запроса на сертификат. Может принимать значения:
  - **Обработка** – запрос находится в стадии рассмотрения
  - **Отклонен** – запрос отклонен администратором ЦР
  - **Завершен** – запрос обработан, выпущенный сертификат получен и установлен пользователем
  - **Установить** – промежуточное состояние, требующее от пользователя установить выпущенный по данному запросу сертификат. В этом случае наименование состояния выполнено в виде ссылки/кнопки, по

клику на которой запускается процесс установки сертификата на локальной машине.

- **Просмотр** – содержит ссылку (кнопку), по нажатию которой можно вывести содержимое запроса на сертификат в отдельное окно для просмотра и/или печати на бумажный носитель.

Для каждой строки данной таблицы со статусом **Завершен** должна присутствовать строка в таблице сертификатов.

Таблица со списком запросов на отзыв сертификатов имеет следующие колонки:

- **Номер сертификата** – Серийный номер отзываемого/отозванного сертификата
- **Дата запроса** – дата/время формирования запроса на отзыв сертификата.
- **Дата отзыва** – Дата время рассмотрения запроса на отзыв сертификата администратором ЦР. В случае положительного решения – с данного момента сертификат считается недействительным и должен попасть в очередной список отозванных сертификатов.
- **Причина –** Причина, по которой пользователь/администратор отозвал сертификат.
- **Статус запроса –** текущее состояние запроса на отзыв сертификата. Может принимать следующие значения:
  - **Обработка –** запрос находится в стадии рассмотрения
  - **Удовлетворен –** запрос принят, сертификат отозван
  - **Отклонен –** запрос отклонен администратором

Если запрос на отзыв имеет статус **Удовлетворен**, то соответствующий сертификат в таблице сертификатов имеет статус **Отозван**.

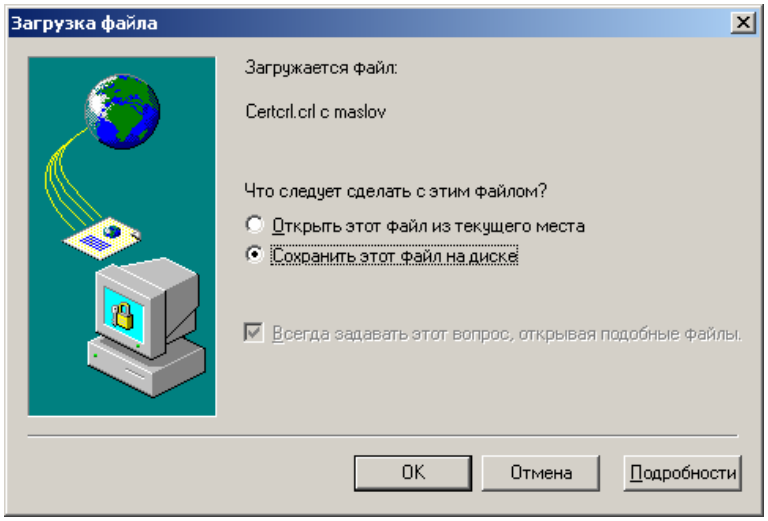
Если пользователь ни разу не формировал запрос на отзыв сертификатов, то таблица со списком запросов на отзыв сертификата не показывается.

4.2.1. Получение списка отозванных сертификатов

Для получения и установки списка отозванных сертификатов необходимо выполнить следующие действия:

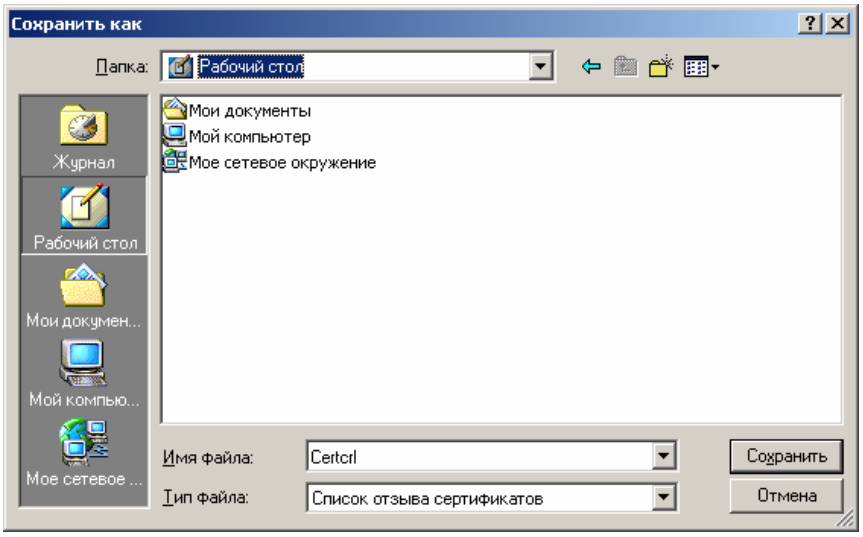
- В окне АРМ пользователя нажать ссылку **Список отозванных**. В результате этого действия происходит загрузка файла, содержащего список отозванных сертификатов с Центра Регистрации УЦ.
- В окне **Загрузка файла** (см. Рисунок 21) выберите пункт **Сохранить этот файл на диске**

Рисунок 21. Окно загрузки файла со списком отозванных сертификатов



- В окне определения имени и расположения сохраняемого файла выберите в качестве места размещения рабочий стол компьютера (см. Рисунок 22).

Рисунок 22. Окно сохранения файла со списком отозванных сертификатов



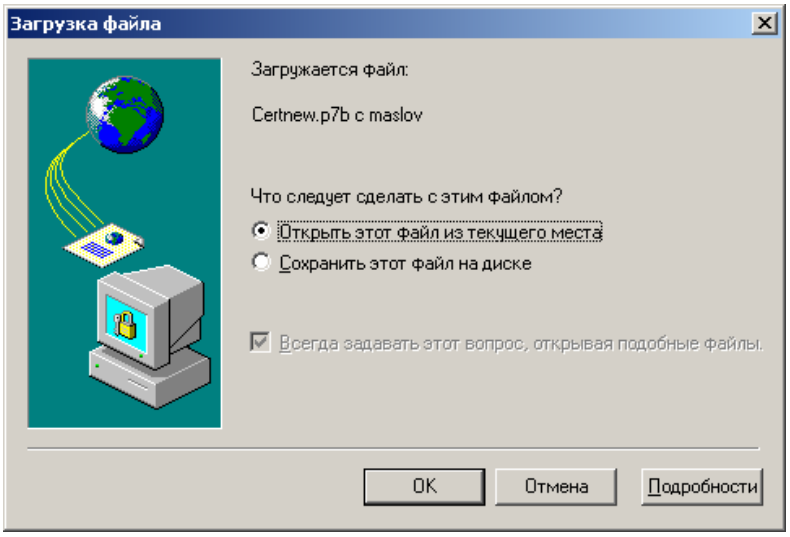
- После этого перейдите на рабочий стол компьютера, выберите иконку данного файла, нажмите правую кнопку мышки и из появившегося списка пунктов меню выберите пункт **Установить список отзыва (CRL)**
- Далее в соответствии с Мастером импорта сертификатов (см. Рисунок 9), установите список отозванных сертификатов. При этом следует выбирать автоматическое определение хранилища, в соответствии с типом сертификата

4.2.2. Получение сертификата Центра Сертификации

Для получения и установки сертификата ЦС необходимо выполнить следующие действия:

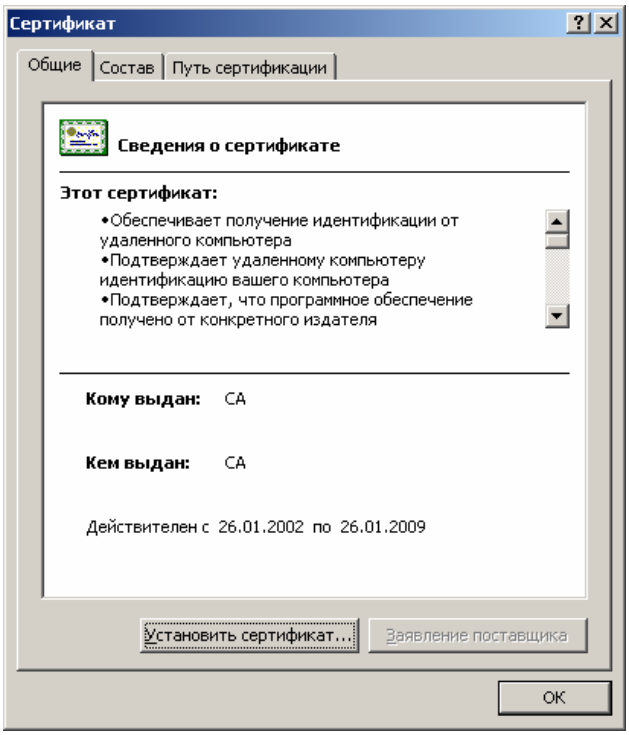
- В окне АРМ пользователя нажать ссылку **Сертификат центра**. В результате этого действия происходит загрузка файла, содержащего сертификат ЦС.
- В окне **Загрузка файла** выберите пункт **Открыть этот файл из текущего места** (см. Рисунок 23)

Рисунок 23. Окно загрузки файла с сертификатом ЦС



- В появившемся окне с информацией о сертификате (см. Рисунок 24) нажмите кнопку **Установить сертификат**

Рисунок 24. Окно свойств сертификата ЦС



- Далее следуйте указаниям Мастера импорта сертификатов

4.2.3. Получение нового сертификата

Получение нового (рабочего) сертификата осуществляется в соответствии с регламентом работы, определенном Центром регистрации (плановая смена ключей и сертификатов), или в случае внеплановой смены ключей и сертификатов (отзыв ранее действующего сертификата).

Получение нового сертификата выполняется на основании запроса на сертификат, получаемого ЦР от пользователя в электронном виде. Данный запрос формируется с использованием АРМ пользователя по ссылке **Новый сертификат**. В процессе формирования запроса производится генерация ключей и запись их на ключевой носитель.

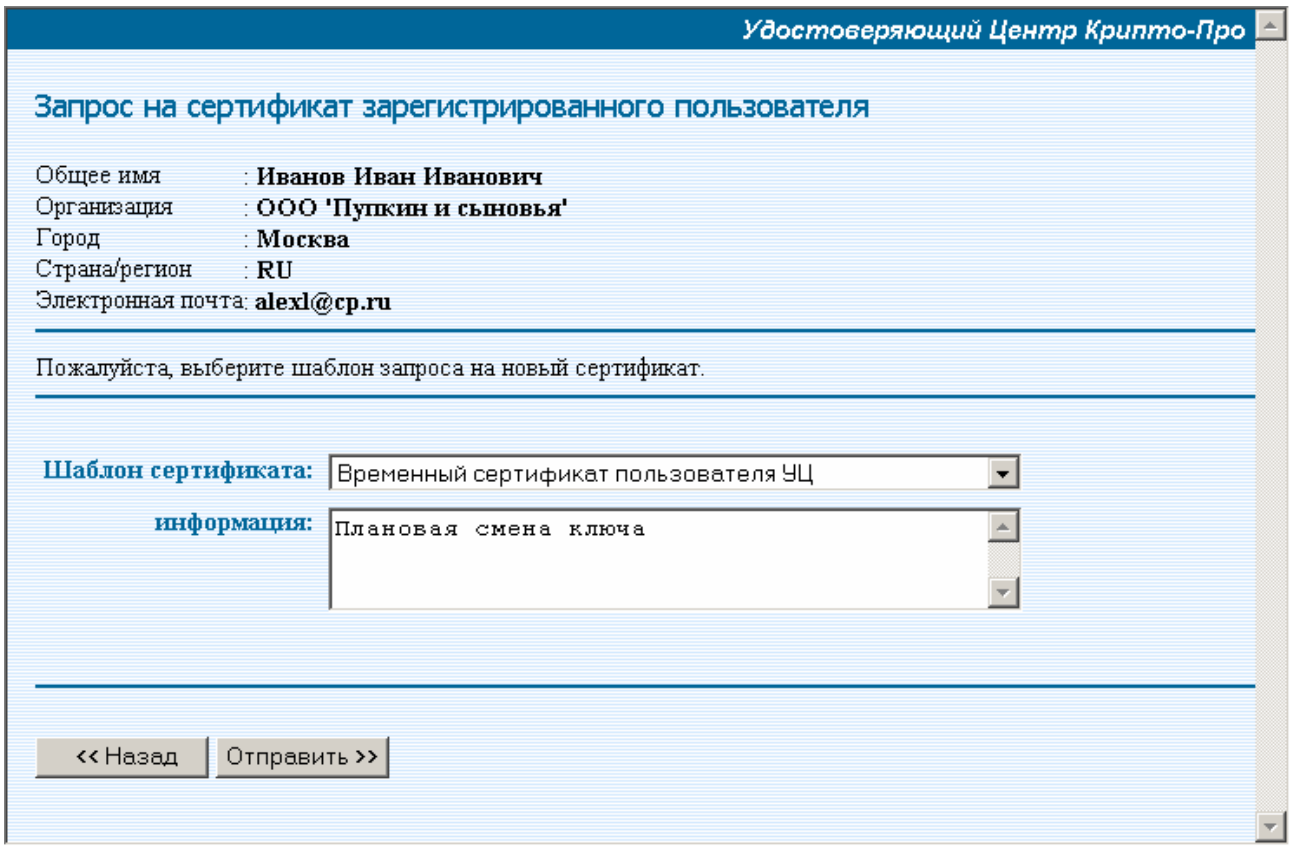
После получения запроса на новый сертификат от пользователя, Центр регистрации передает данный запрос на Центр сертификации, где происходит формирование сертификата. Выпущенный сертификат устанавливается пользователем в хранилище сертификатов своего рабочего места (на компьютер). Установка сертификата также происходит с помощью программного обеспечения АРМ пользователя. В процессе установки сертификата также автоматически производится запись данного сертификата на ключевой носитель. В дальнейшем, данный сертификат может быть повторно установлен на рабочее место пользователя (в случае потери сертификата, например, в результате сбоя компьютера или операционной системы) или на другое рабочее место (в случае миграции пользователя). В этом случае установка сертификата с ключевого носителя производится с использованием интерфейса СКЗИ «КриптоПро CSP» в порядке, аналогичном порядку, определенному в соответствующем пункте раздела Установка личного служебного сертификата пользователя, выданного администратором ЦР.

Процедура получения нового сертификата:

4.2.4. Формирование запроса на сертификат

- Нажмите ссылку «Новый сертификат». Рабочее окно АРМ пользователя примет следующий вид (см. Рисунок 25):

Рисунок 25. Окно формирования запроса на новый сертификат

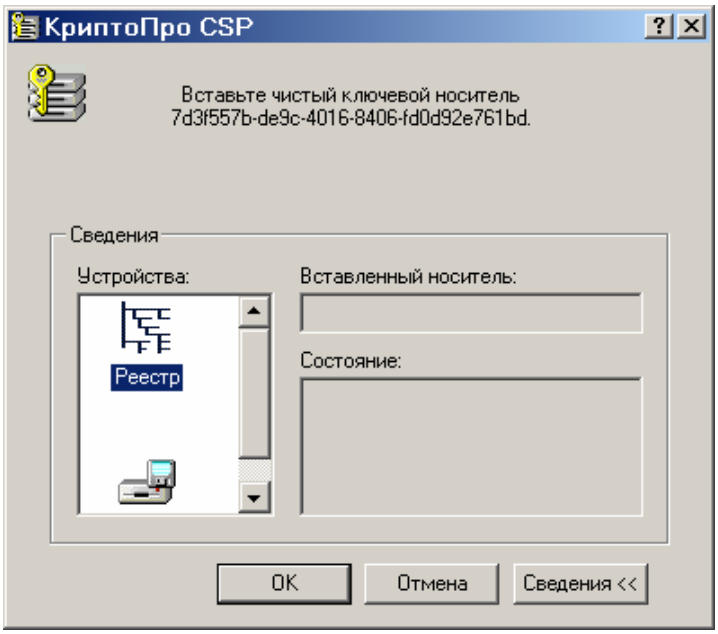


- В списке доступных шаблонов сертификатов выберите требуемый шаблон, определенный регламентом работы пользователя с УЦ.
- В поле дополнительной информации можете ввести небольшой комментарий, который увидит администратор Центра Регистрации.
- Нажмите кнопку **Отправить** для продолжения формирования запроса на сертификат. Нажмите кнопку **Назад** для отказа от режима формирования запроса на сертификат и возврата в главное окно АРМ пользователя.

Примечание. Шаблоны сертификатов настраиваются и формируются администратором ЦР в соответствии регламентирующими документами организации – УЦ. Пользователю необходимо выбрать нужный шаблон из представленного списка.

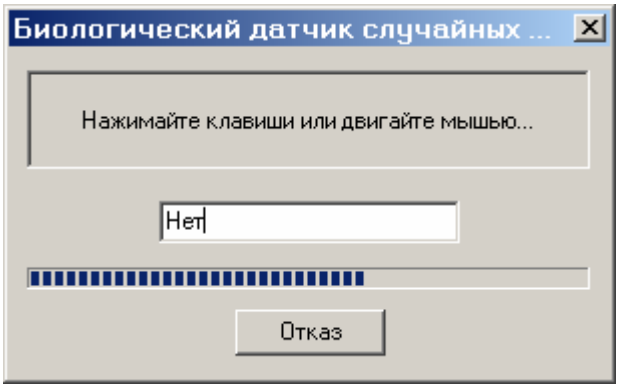
- После нажатия кнопки **Отправить** система перейдет к процедуре формирования новых ключей.
- Выберите необходимый тип ключевого носителя из списка подключенных в СКЗИ КриптоПро CSP (см. Рисунок 26).

Рисунок 26. Окно выбора ключевого носителя для генерации ключей



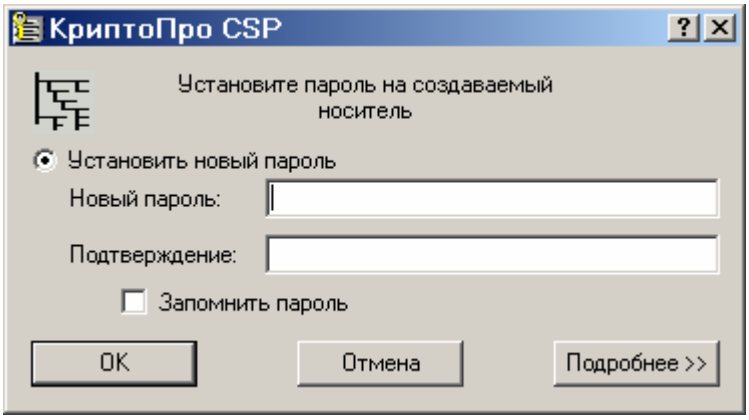
- проинициализируйте генератор случайных чисел (путем нажатия клавиш на клавиатуре или движением указателя мышки в окне инициализации) (см. Рисунок 27).

Рисунок 27. Окно инициализации датчика случайных чисел



- при необходимости установите пароль (ПИН-код) на создаваемый ключевой контейнер (см. Рисунок 28)

Рисунок 28. Окно задания пароля на создаваемый ключевой контейнер

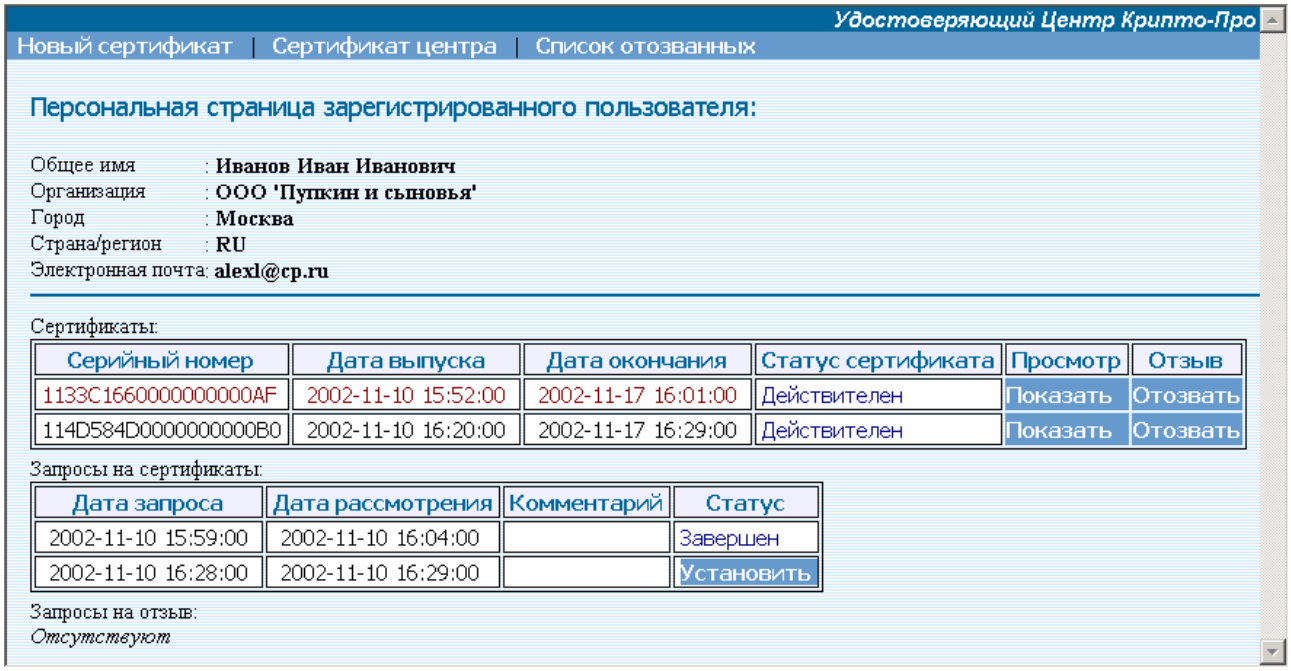


- В результате успешного выполнения вышеперечисленных действий сформированный запрос будет отправлен в ЦР на рассмотрение, а в таблице запросов на сертификат появится новая строка со статусом запроса **Обработка**.
- После успешного принятия данного запроса уполномоченным лицом в ЦР, статус запроса изменится и появится возможность установить новый сертификат в хранилище сертификатов на локальном компьютере.

4.2.5. Установка сертификата

О завершении обработки запроса на сертификат и наличии возможности установить выпущенный сертификат, свидетельствует установление статуса запроса на сертификат в состояние **Установить** (см. Рисунок 29). Продолжительность обработки запроса зависит от регламента работы Центра регистрации.

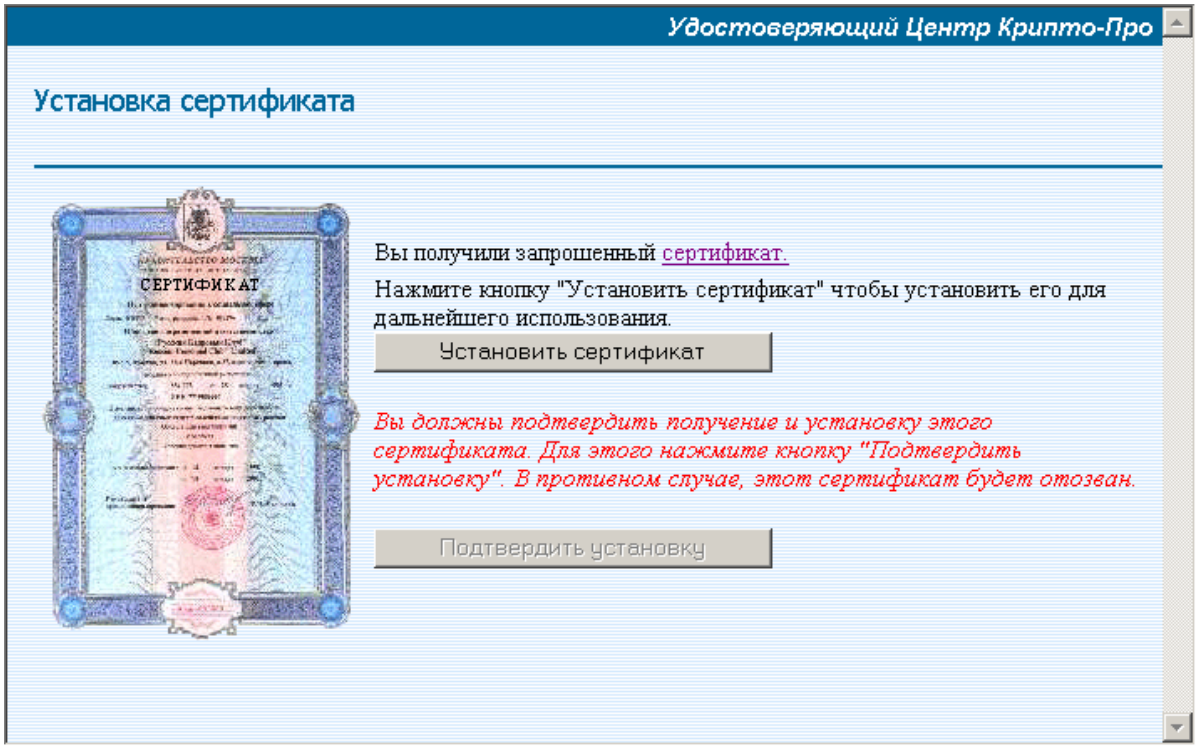
Рисунок 29. Окно АРМ пользователя со статусом Установить запроса на сертификат



В случае установления статуса запроса на сертификат в состояние возможности установления сертификата в хранилище сертификатов рабочего места пользователя, выполните следующие действия:

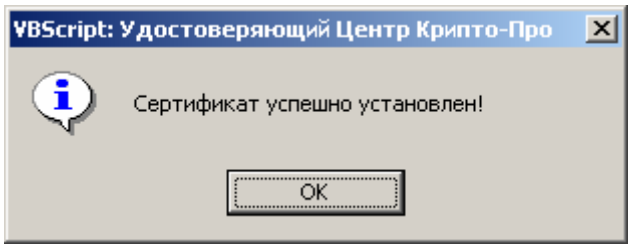
- Нажмите ссылку **Установить** в соответствующей строке таблицы запросов на сертификат. При этом рабочая область АРМ пользователя примет следующий вид (см. Рисунок 30):

Рисунок 30. Окно установки запрошенного сертификата



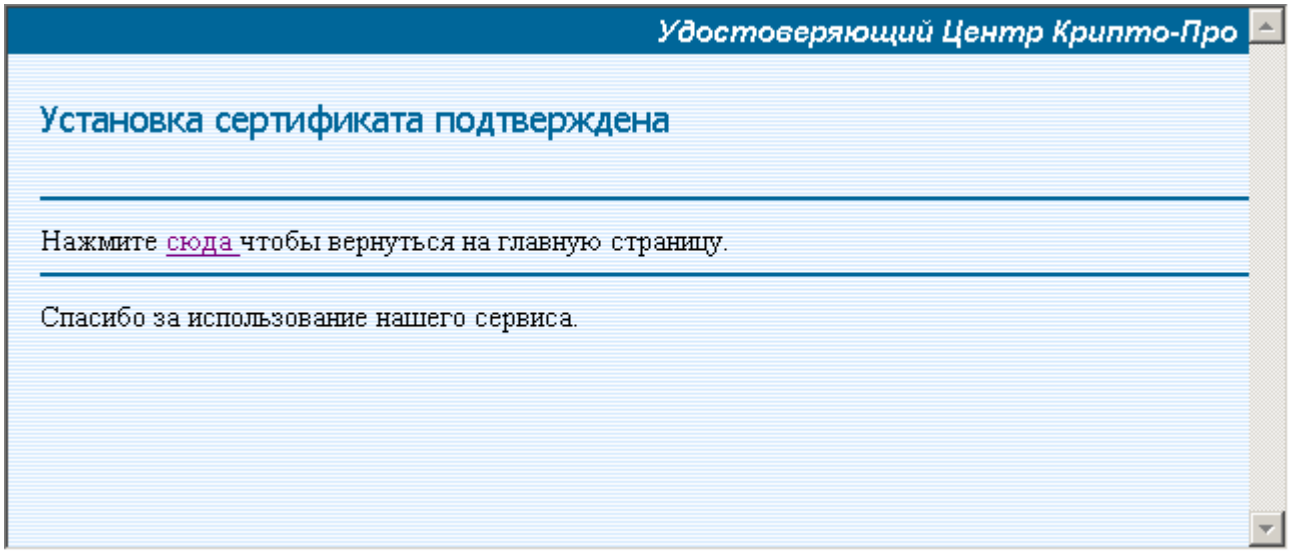
- В появившейся форме убедитесь в соответствии полученного сертификата отправленному запросу. Для этого нажмите на ссылку **сертификат** данного окна. В случае несоответствия данных обратитесь к Администратору.
- Для продолжения установки сертификата нажмите кнопку **Установить сертификат**

Рисунок 31. Информационное окно об успешной установке сертификата



- Появление сообщения (см. Рисунок 31) свидетельствует об успешной установке данного сертификата в хранилище сертификатов.
- Для подтверждения факта установки и сообщения об этом на ЦР нажмите кнопку **Подтвердить установку**. В случае не подтверждения установки сертификат будет занесен в список отозванных сертификатов.
- После подтверждения установки запрошенного сертификата, пользователю будет отображено соответствующее окно (см. Рисунок 32), из которого он может вернуться в основное окно АРМ пользователя.

Рисунок 32. Окно завершения установки запрошенного сертификата

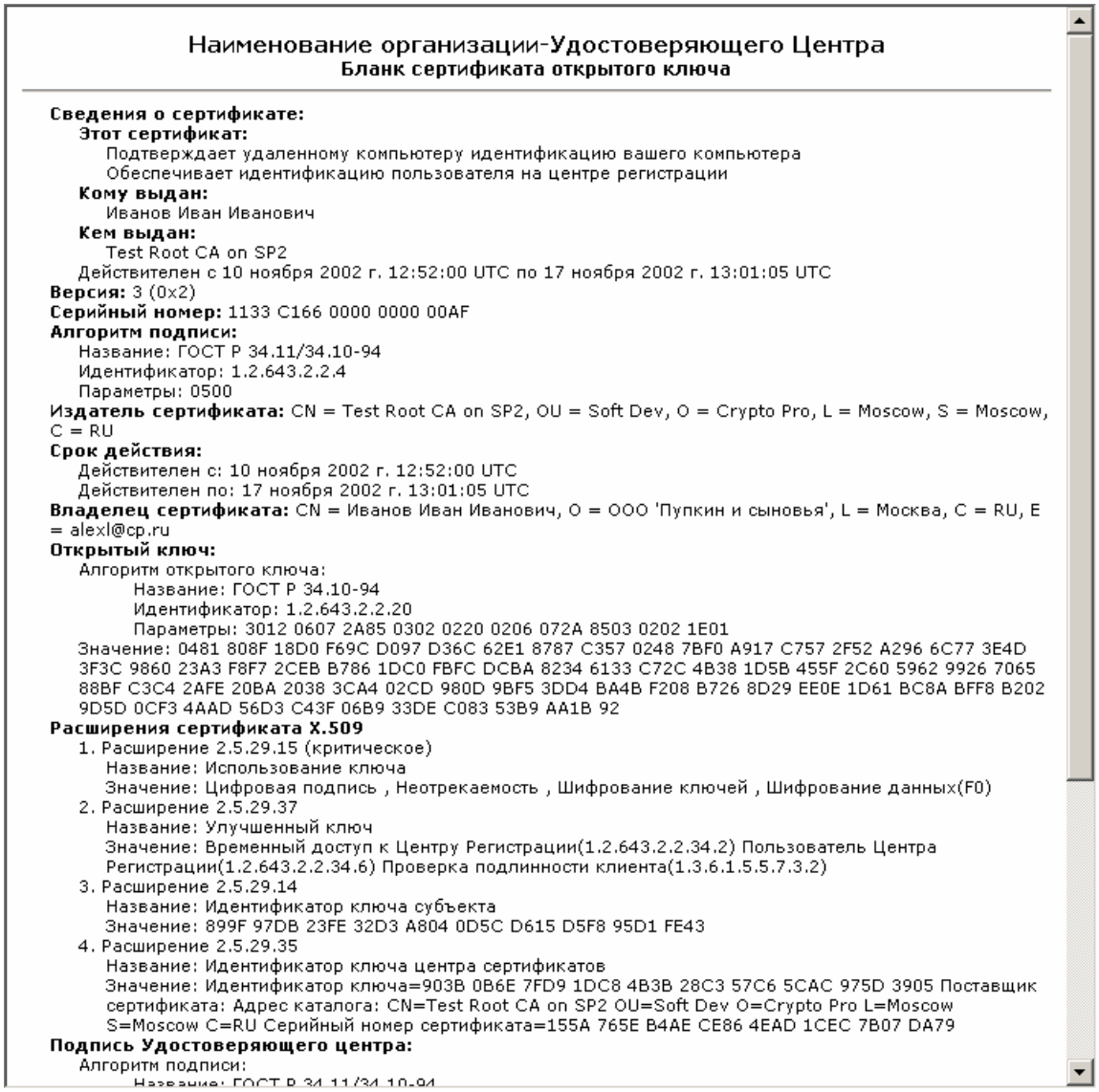


4.2.6. Печать сертификата

Формирование печатной формы и вывод ее на бумажный носитель выполняется пользователем в порядке и в сроки, определенные регламентирующими документами УЦ.

Для печати сертификата необходимо в окне АРМ пользователя в соответствующей строке таблицы сертификатов нажать ссылку **Показать**. В результате в новом окне браузера MS IE (см. Рисунок 33) будет сформирована печатная форма сертификата пользователя.

Рисунок 33. Окно с бланком сертификата



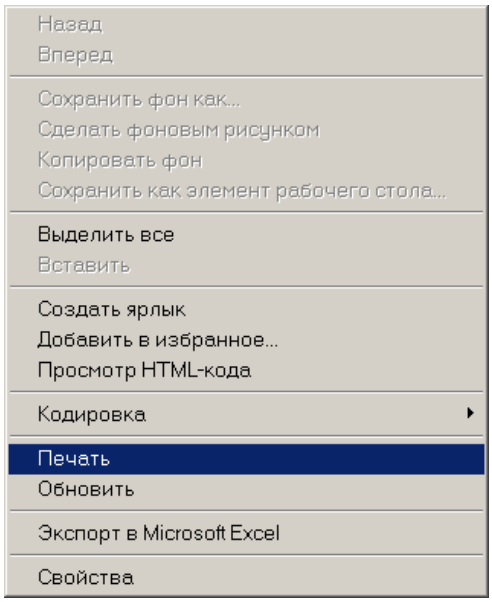
Наименование организации-Удостоверяющего Центра

Бланк сертификата открытого ключа

Сведения о сертификате:
Этот сертификат:
Подтверждает удаленному компьютеру идентификацию вашего компьютера
Обеспечивает идентификацию пользователя на центре регистрации
Кому выдан:
Иванов Иван Иванович
Кем выдан:
Test Root CA on SP2
Действителен с 10 ноября 2002 г. 12:52:00 UTC по 17 ноября 2002 г. 13:01:05 UTC
Версия: 3 (0x2)
Серийный номер: 1133 C166 0000 0000 00AF
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-94
Идентификатор: 1.2.643.2.2.4
Параметры: 0500
Издатель сертификата: CN = Test Root CA on SP2, OU = Soft Dev, O = Crypto Pro, L = Moscow, S = Moscow, C = RU
Срок действия:
Действителен с: 10 ноября 2002 г. 12:52:00 UTC
Действителен по: 17 ноября 2002 г. 13:01:05 UTC
Владелец сертификата: CN = Иванов Иван Иванович, O = ООО 'Пупкин и сыновья', L = Москва, C = RU, E = alexl@cp.ru
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-94
Идентификатор: 1.2.643.2.2.20
Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01
Значение: 0481 808F 18D0 F69C D097 D36C 62E1 8787 C357 0248 7BF0 A917 C757 2F52 A296 6C77 3E4D 3F3C 9860 23A3 F8F7 2CEB B786 1DC0 FBFC DCBA 8234 6133 C72C 4B38 1D5B 455F 2C60 5962 9926 7065 88BF C3C4 2AFE 20BA 2038 3CA4 02CD 980D 9BF5 3DD4 BA4B F208 B726 8D29 EE0E 1D61 BC8A BFF8 B202 9D5D 0CF3 4AAD 56D3 C43F 06B9 33DE C083 53B9 AA1B 92
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Временный доступ к Центру Регистрации(1.2.643.2.2.34.2) Пользователь Центра Регистрации(1.2.643.2.2.34.6) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: 899F 97DB 23FE 32D3 A804 0D5C D615 D5F8 95D1 FE43
4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=903B 0B6E 7FD9 1DC8 4B3B 28C3 57C6 5CAC 975D 3905 Поставщик сертификата: Адрес каталога: CN=Test Root CA on SP2 OU=Soft Dev O=Crypto Pro L=Moscow S=Moscow C=RU Серийный номер сертификата=155A 765E B4AE CE86 4EAD 1CEC 7B07 DA79
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-94

Для вывода бланка сертификата на печать откройте данное окно, установите указатель мыши в произвольном месте окна на тексте бланка и нажмите правую кнопку мыши. В появившемся меню (см. Рисунок 34) выберите пункт «Печать» (Print).

Рисунок 34. Окно меню с пунктом печати сертификата



4.2.7. Приостановление действия сертификата

Приостановление действия сертификата, т.е. помещение его в список отозванных сертификатов на определенный срок, выполняется Центром сертификации на основании запроса на приостановление действия сертификата, полученного от пользователя, с подтверждением данного запроса на Центре регистрации.

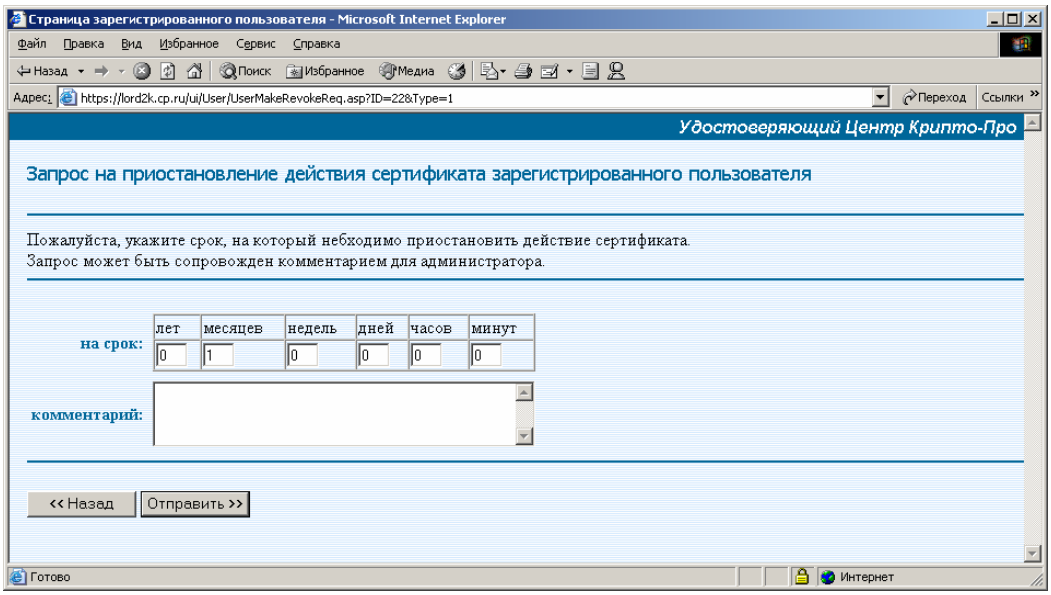
Данный запрос формируется пользователем с использованием АРМ пользователя и посылается на Центр регистрации в электронном виде.

Приостановленным может быть любой сертификат пользователя.

Для создания запроса на приостановление действия сертификата необходимо выполнить следующие действия:

- В таблице сертификатов нажать ссылку **Приостановить** соответствующей строки. Рабочая область АРМ пользователя примет следующий вид (см. Рисунок 35):

Рисунок 35. Окно формирования запроса на приостановление действия сертификата



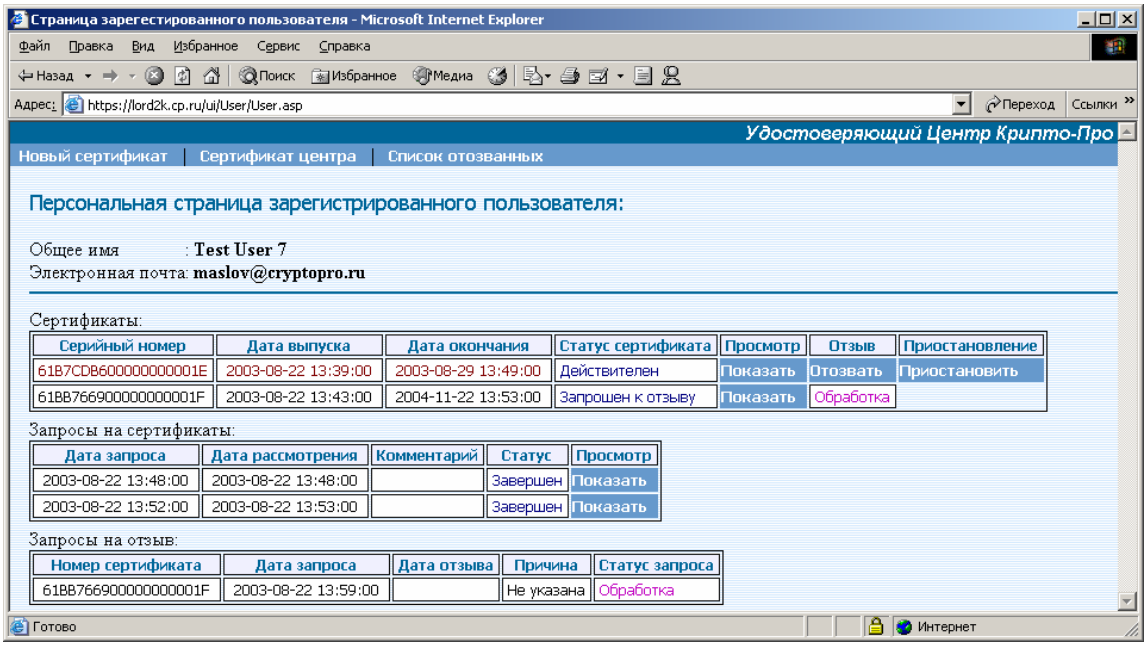
В данном окне задайте срок, на который требуется приостановить сертификат открытого ключа и нажмите кнопку **Отправить**.

Запрос на приостановление действия сертификата поступает на Центр Регистрации в форме запроса на отзыв и становится в очередь на обработку администратором Центра Регистрации.

В период обработки запрос на приостановление действия сертификата находится в окне АРМа в списке запросов на отзыв в состоянии **Обработка** (см. Рисунок 36).

Статус отзыва сертификата в списке сертификатов, отображаемых на АРМе, находится в состоянии **Обработка** (см. Рисунок 36).

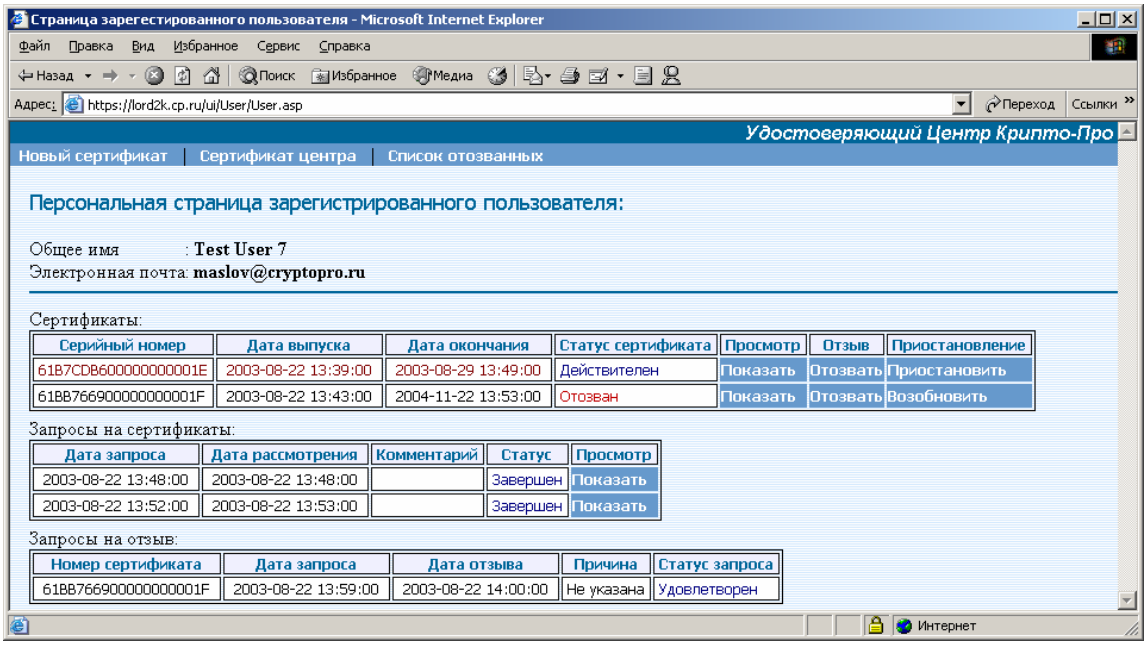
Рисунок 36. Окно отображения состояния обработки запроса на приостановление действия сертификата



По окончании обработки, запрос на приостановление действия сертификата переходит в состояние **Завершен** (см. Рисунок 37).

Статус сертификата в списке сертификатов, отображаемых на АРМе, переходит в состояние **Отозван** (см. Рисунок 37).

Рисунок 37. Окно отображения завершение обработки запроса на приостановление действия сертификата



4.2.8. Возобновление действия сертификата

Возобновление действия сертификата, т.е. удаление его из списка отозванных сертификатов, выполняется Центром сертификации на основании запроса на возобновление действия сертификата, полученного от пользователя, с подтверждением данного запроса на Центре регистрации.

Данный запрос формируется пользователем с использованием АРМ пользователя и посылается на Центр регистрации в электронном виде.

Возобновить действие можно только для сертификата, ранее приостановленного по запросу.

Для создания запроса на возобновление действия сертификата необходимо нажать ссылку **Возобновить** соответствующей строки (см. Рисунок 37):

4.2.9. Отзыв сертификата

Отзыв сертификата, т.е. помещение его в список отозванных сертификатов, выполняется Центром сертификации на основании запроса на отзыв сертификата, полученного от пользователя, с подтверждением данного запроса на Центре регистрации.

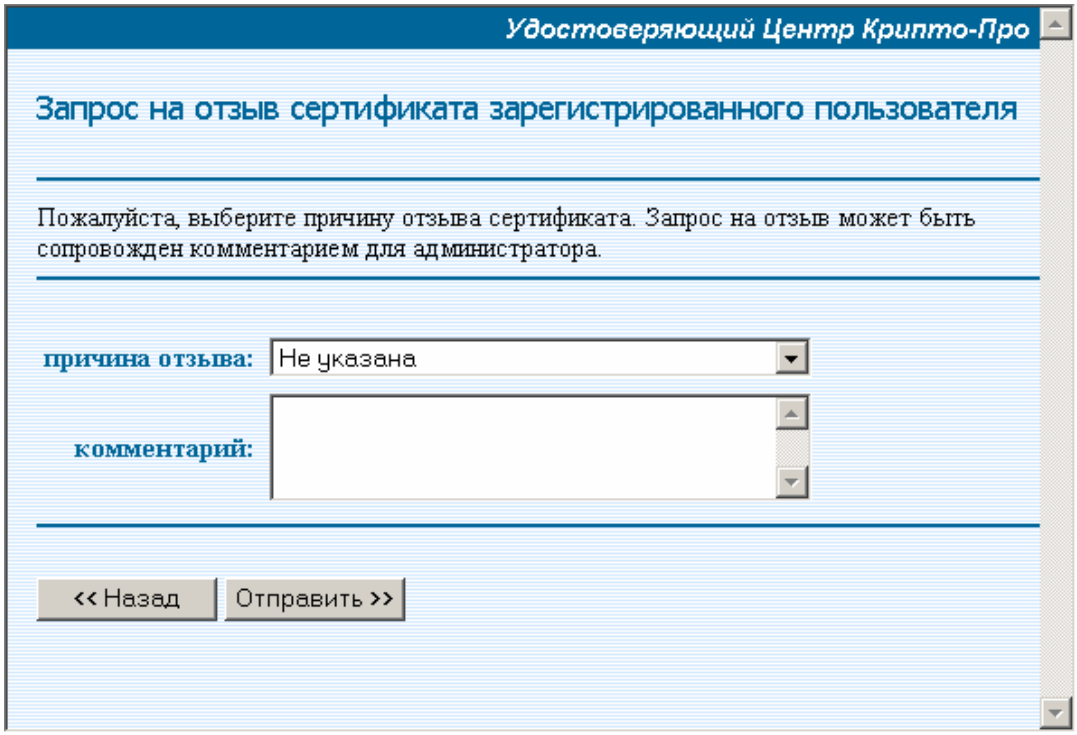
Данный запрос формируется пользователем с использованием АРМ пользователя и посылается на Центр регистрации в электронном виде.

Отозванным может быть любой сертификат пользователя, за исключением того, на котором выполнена аутентификация пользователя в текущем окне АРМ. Для отзыва данного сертификата необходимо установить соединение с Центром регистрации на другом действующем сертификате. В случае если у пользователя имеется только один действующий сертификат, необходимо сформировать запрос на новый сертификат, получить и установить его. После этого закрыть окно АРМ и установить новое соединение с Центром регистрации, используя новый полученный сертификат. После этого старый сертификат доступен для отзыва.

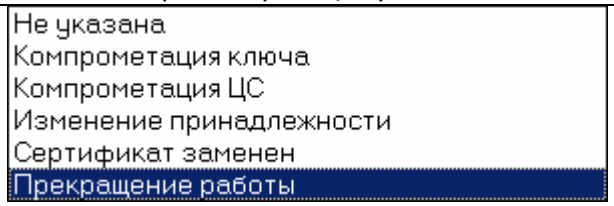
Для создания запроса на отзыв сертификата необходимо выполнить следующие действия:

- В таблице сертификатов нажать ссылку **Отозвать** соответствующей строки. Рабочая область АРМ пользователя примет следующий вид (см. Рисунок 38):

Рисунок 38. Окно формирования запроса на отзыв сертификата



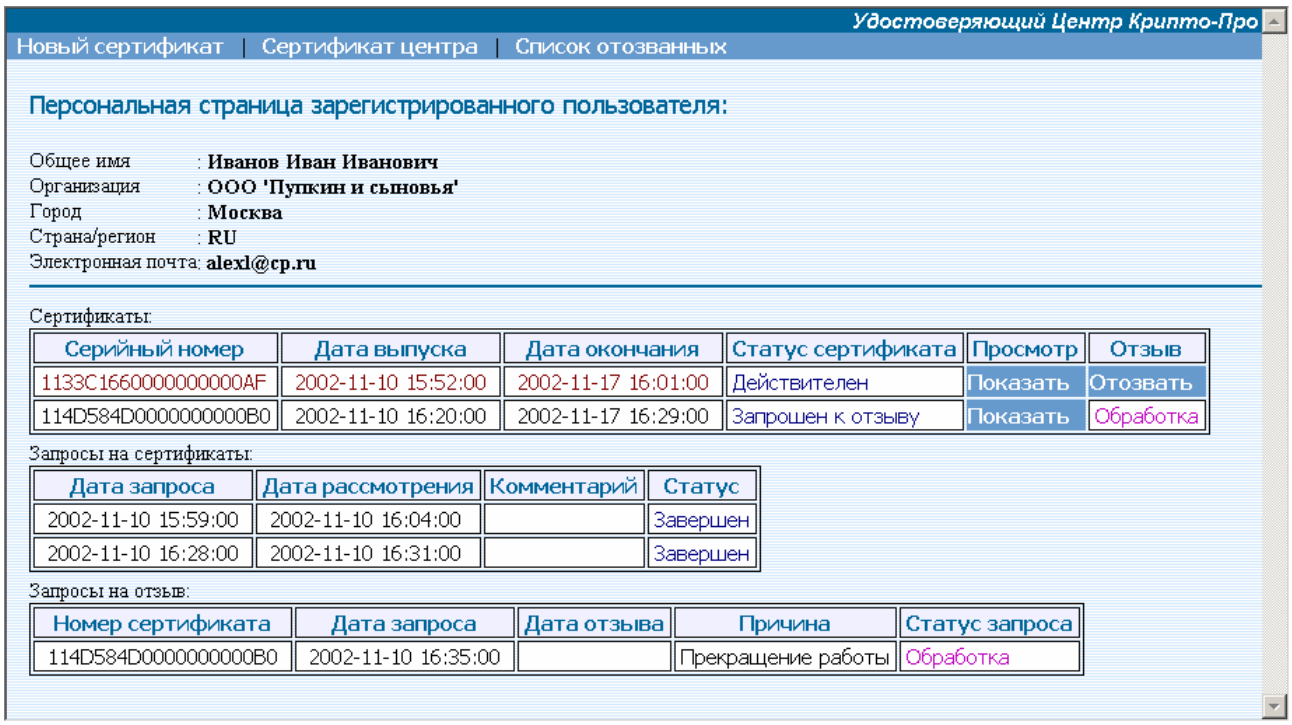
- В появившейся форме укажите причину отзыва сертификата и, при необходимости, комментарии для Администратора. Причину отзыва можно выбрать из предложенного списка:



- Нажмите кнопку **Отправить** для отправки запроса на отзыв в Центр регистрации или кнопку **Назад** для отмены данного режима работы и возврата в основное окно АРМ пользователя.

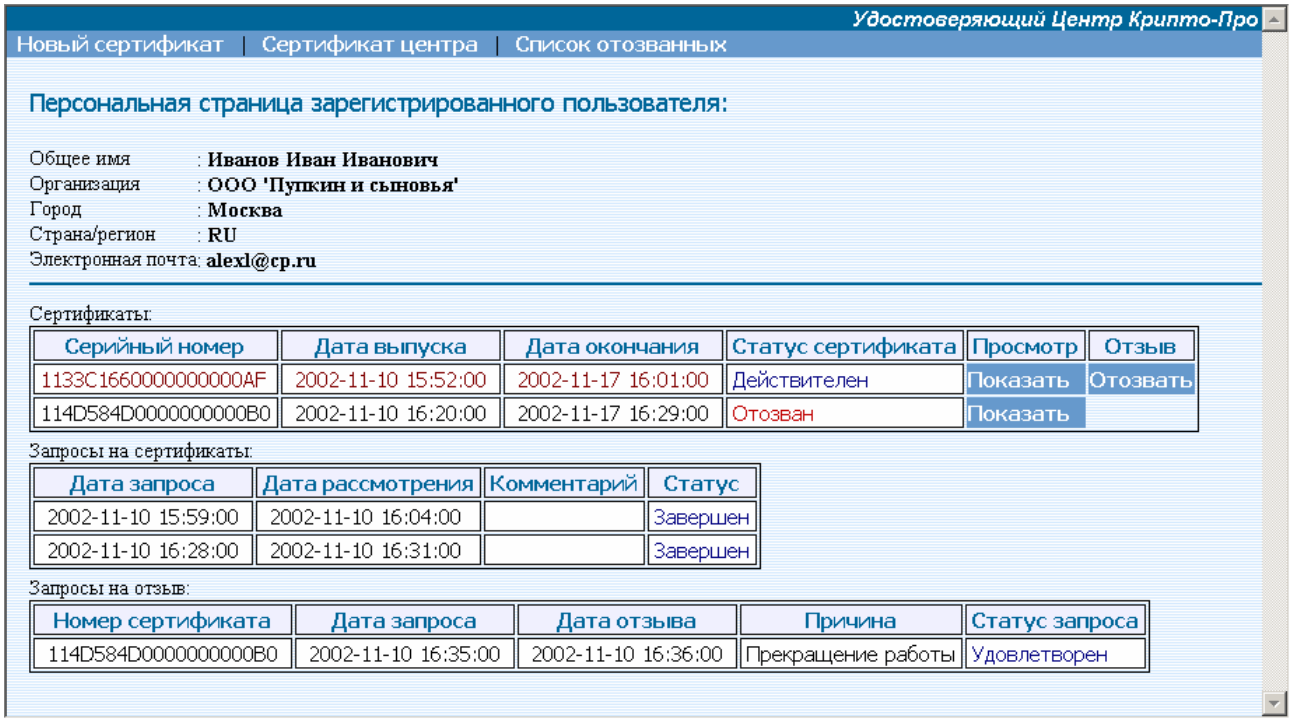
В результате выполнения этих действий будет сформирован запрос на отзыв сертификата. В основном окне АРМ пользователя в таблице запросов на отзыв сертификатов появится соответствующая строка со статусом **Обработка**. В таблице сертификатов отзываемый сертификат примет статус **Запрошен к отзыву** (см. Рисунок 39).

Рисунок 39. Окно АРМ пользователя со статусом "Запрошен к отзыву" сертификата открытого ключа



Продолжительность обработки запроса на отзыв сертификата зависит от регламента работы Центра регистрации. После подтверждения уполномоченным лицом ЦР запроса на отзыв его состояние изменится на **Удовлетворен**, а состояние соответствующего сертификата изменится на **Отозван** (см. Рисунок 40):

Рисунок 40. Окно АРМ пользователя со статусом "Отозван" сертификат открытого ключа



В том случае, если запрос на отзыв будет отклонен, состояние запроса изменится на **Отклонен**.

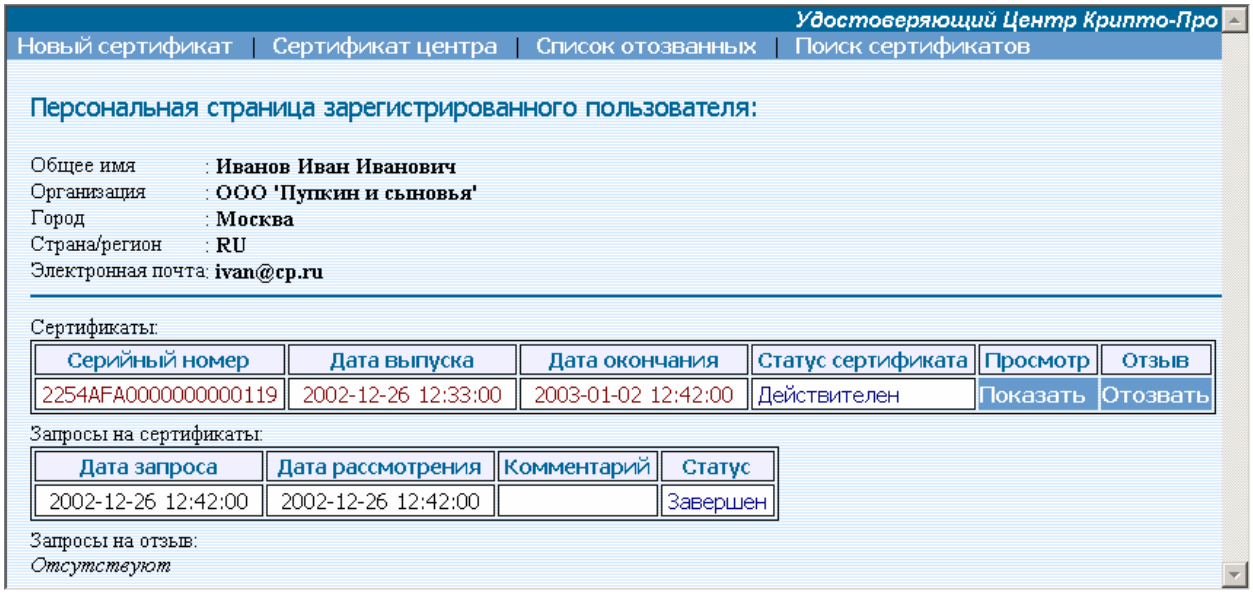
4.2.10. Поиск и импорт сертификатов открытых ключей других зарегистрированных пользователей Центра Регистрации

Политикой Центра Регистрации Удостоверяющего Центра может быть разрешен доступ владельцев сертификатов к общему реестру сертификатов. Обычно это необходимо в тех случаях, когда пользователи – участники информационной системы – общаются между собой с использованием средств криптографической защиты и электронной цифровой подписи. При этом используются ключи и сертификаты, выданные в Удостоверяющем центре.

Для подобного общения (переписка с использованием E-Mail, обмен зашифрованными и подписанными ЭЦП файлами, электронная цифровая подпись содержимого Web страниц) абонентам необходимо иметь у себя сертификаты других пользователей информационной системы. Данный режим Центра регистрации позволяет зарегистрированным пользователям осуществлять удаленный поиск требуемых сертификатов в Реестре Центра Регистрации, импортировать найденные сертификаты себе на локальный компьютер в виде файлов или в специально предназначенное для этого в операционной системе Windows хранилище. В дальнейшем это позволит осуществлять проверку электронной цифровой подписи других абонентов информационной системы и шифрование информации в их адрес.

Если политикой Центра регистрации данный режим разрешен, то основной экран интерфейса зарегистрированного пользователя будет выглядеть следующим образом (см. Рисунок 41).

Рисунок 41. Окно АРМ пользователя с пунктом меню "Поиск сертификатов"

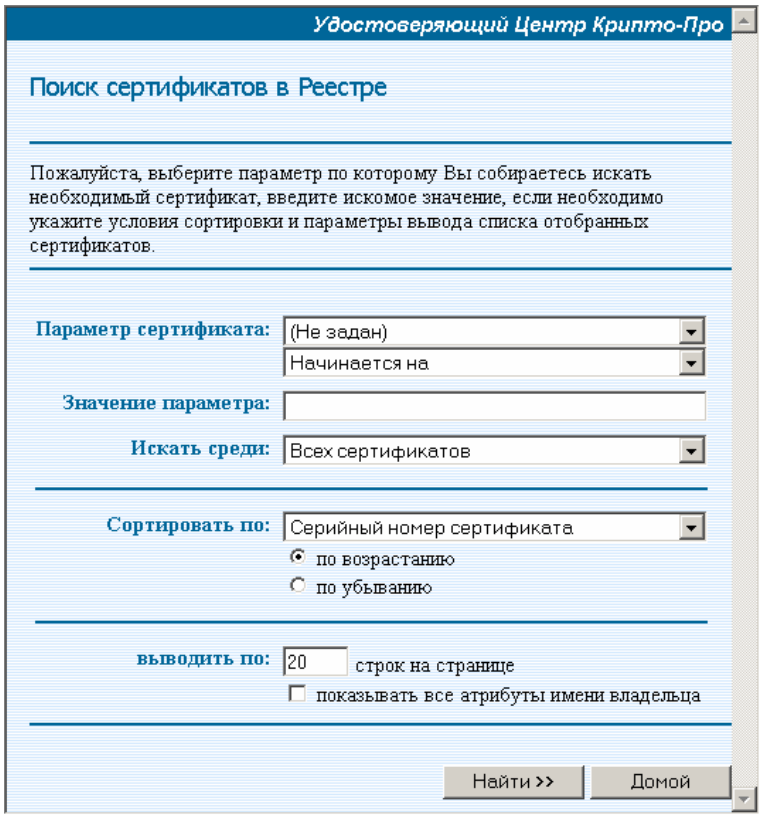


В верхней части экрана в строке меню появился новый пункт **Поиск сертификатов**.

Кликнув на нем указателем мыши, Вы выйдете на экран формирования запроса на поиск сертификатов (см. Рисунок 42).

4.2.11. Формирование запроса на поиск сертификатов

Рисунок 42. Окно определения параметров поиска сертификатов



Данный экран имеет три основные секции для ввода информации.

В первой секции указываются условия, по которым следует отобрать сертификаты из реестра.

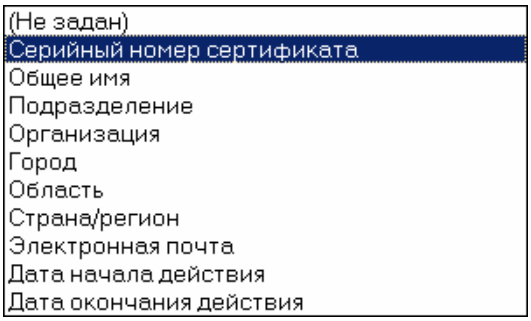
Во второй секции указываются условия сортировки отобранных в результате поиска сертификатов.

В третьей – параметры отображения списка найденных сертификатов.

Поиск сертификатов в данной версии может осуществляться только по одному выбранному условию, не считая статуса сертификатов, среди которых искать (среди всех, действующих, отозванных, просроченных…).

Необходимо отметить, что если **не выбирать** параметр сертификата, по которому осуществлять поиск, то в результате будут отобраны все сертификаты из базы данных Центра Регистрации.

Для ввода условия запроса выберите из раскрывающегося списка с комментарием «Параметр сертификата» требуемый параметр.



Состав параметров в каждом конкретном Центре Регистрации может варьироваться, в зависимости от «Политики Имен» Центра Регистрации, присутствующих в сертификатах. Всегда присутствуют следующие параметры: «Серийный номер сертификата», «Дата начала действия» сертификата, «Дата окончания действия» сертификата, остальные параметры формируются динамически, в зависимости от указанной политики Центра Регистрации.

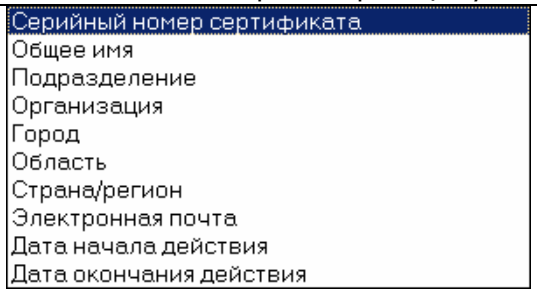
После выбора параметра, по которому искать, введите в поле «Значение параметра» значение, которое искать.

Далее укажите «точность» поиска. Для этого выберите из списка условие – каким образом осуществлять поиск введенного значения: «Начинается на …» или «содержит…». Условие «Начинается на» означает, что будут отобраны все сертификаты, у которых указанный Вами параметр начинается на значение, введенное Вами в поле «Значение параметра». Условие «Содержит» означает, что будут отобраны все сертификаты, у которых в любом месте указанного Вами параметра содержится введенная Вами в поле «Значение параметра» подстрока.

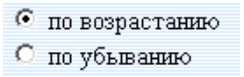
Дополнительно, Вы можете указать подмножество сертификатов, среди которых осуществлять поиск, выраженное статусом сертификатов «Искать среди:»

Выберите из списка нужное подмножество. По умолчанию, поиск осуществляется среди всего множества сертификатов, находящихся в реестре Центра Регистрации.

После ввода условий поиска, Вы можете указать условия сортировки отобранного списка сертификатов. Для этого в секции сортировки выберите из списка с комментарием «Сортировать по» параметр сертификата, по которому сортировать результирующий набор:



Можно указать направление сортировки – по возрастанию или по убыванию значений, выбранного параметра сертификата. Для этого установите «переключатель»



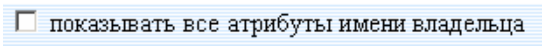
в нужное положение.

В секции параметров отображения найденного списка можно указать количество отображаемых сертификатов результирующего списка на одной странице. Ввиду того, что списки могут быть довольно большими, разумно разбивать их на отдельные страницы (чтобы не ждать загрузки всего списка). Особенно актуально это при работе в Интернет с медленными каналами связи.

В поле «выводить по:» XXX «строк на странице» Вы можете указать значение от 1 до 999. Каждая страница будет содержать не более указанного количества сертификатов. Естественно, если в результате поиска будет отобрано меньше сертификатов, чем указано в данном параметре, или если на последней странице содержится не кратное данному числу количество сертификатов, то страница будет содержать меньше указанного числа строк сертификатов.

По умолчанию список сертификатов будет выдаваться в виде таблицы с ограниченным числом колонок: «Серийный номер сертификата», «Имя владельца», «Дата выпуска» сертификата, «Дата окончания» действия сертификата, «Статус» сертификата. Но вы можете указать, чтобы результирующий список содержал расширенный набор колонок, куда вошли бы все параметры Имени владельца сертификата (Адрес, Организация, Должность, город, Адрес электронной почты и др.). Состав таких параметров устанавливается «Политикой Имен» конкретного Центра Регистрации.

Для получения развернутого списка поставьте «галку» на элементе



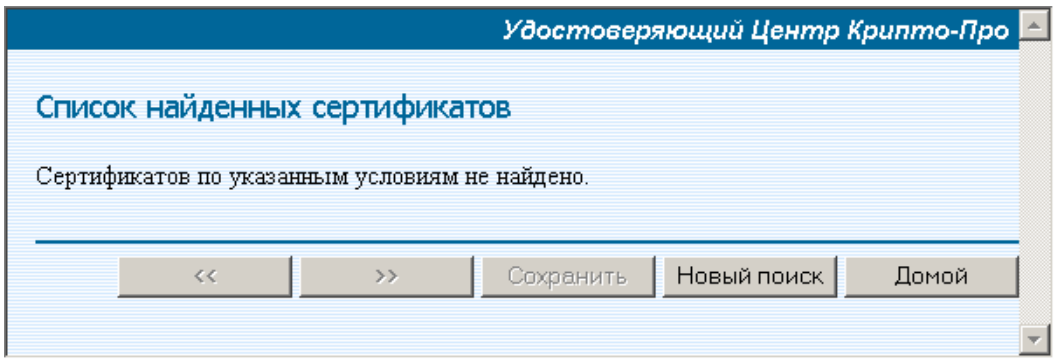
Введя все необходимые условия, нажмите кнопку «Найти >>» для запуска механизма поиска и получения списка найденных сертификатов.

Нажатие на кнопку «Домой» вернет Вас на домашнюю страницу зарегистрированного пользователя.

4.2.12. Работа со списком отобранных сертификатов

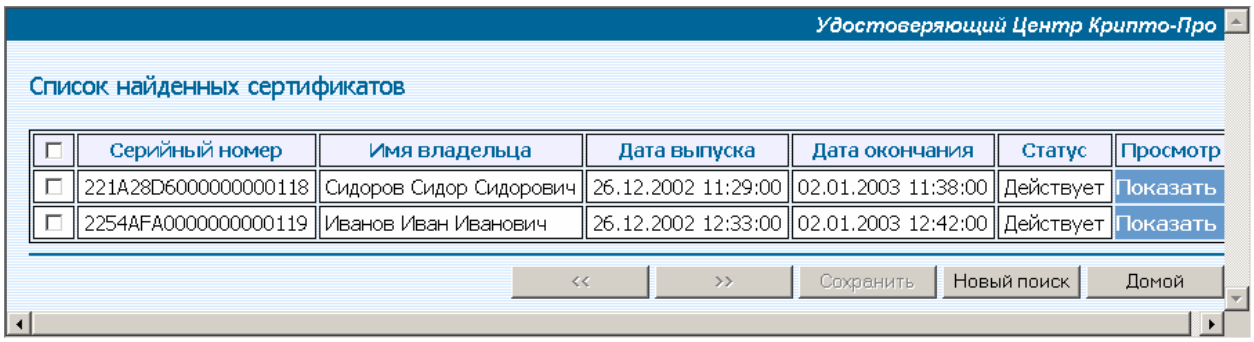
Если в результат поиска не дал положительного результата на экран будет выведено следующее сообщение (см. Рисунок 43).

Рисунок 43. Окно сообщения об отсутствии сертификатов, удовлетворяющих условиям поиска



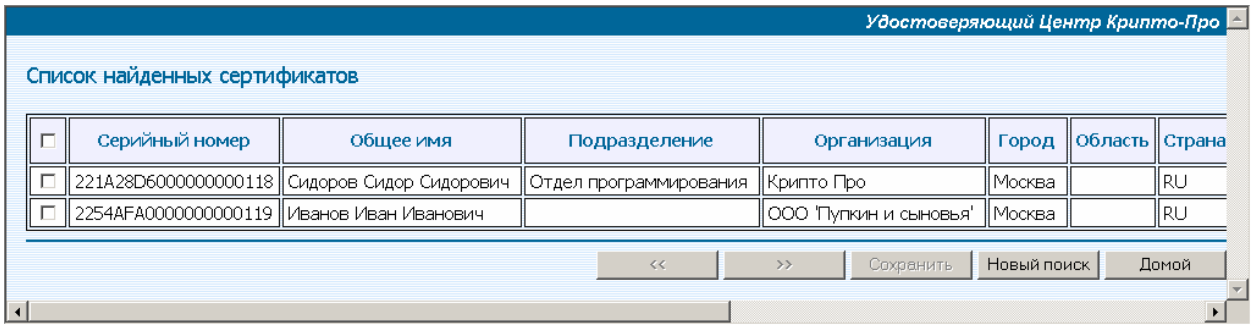
Если же будет найден хоть один сертификат, удовлетворяющий заданным условиям, будет отображена страница со списком найденных сертификатов (см. Рисунок 44):

Рисунок 44. Окно сообщения со списком сертификатов, удовлетворяющих условиям поиска



В развернутом виде (если указано – показывать все атрибуты имени владельца) окно будет выглядеть следующим образом (см. Рисунок 45):

Рисунок 45. Окно сообщения со списком сертификатов, удовлетворяющих условиям поиска, и полным перечнем атрибутов имени владельцев



Примечание. На рисунке показана только левая часть списка. Воспользовавшись прокруткой можно увидеть все остальные колонки списка.

В общем случае, типовой экран со списком найденных сертификатов включает две секции:

1. собственно, список сертификатов
2. панель кнопок с режимами работы

На предыдущих рисунках видно, что в зависимости от указанных параметров отображения, список может содержать типовой и расширенный набор колонок.

В самой левой колонке любого списка находится колонка, позволяющая отметить требуемые сертификаты для исполнения с ними некоторых групповых операций. Элемент управления, находящийся в этой колонке в заголовке таблицы, позволяет отметить/разметить сразу все расположенные в списке сертификаты.

В самой правой колонке списка - «Просмотр» - для каждой строки содержится ссылка, по клику на которой можно просмотреть отдельный сертификат, импортировать его в локальное хранилище сертификатов для дальнейшего использования или сохранить в файле на диске.

Кнопки позволяют осуществлять следующие режимы работы:

<< - перейти к предыдущей странице списка (просмотреть предыдущие NNN отобранных сертификатов, где NNN – указанное Вами количество строк на странице). При этом если Вы просматриваете первую страницу, данная кнопка будет недоступна.

>> - перейти к следующей странице списка (просмотреть следующие NNN отобранных сертификатов, где NNN – указанное Вами количество строк на странице). При этом если Вы просматриваете последнюю (или единственную) страницу, данная кнопка будет недоступна.

Сохранить - сохранить отмеченные в списке сертификаты на своем компьютере в виде файла специального формата PKCS#7, либо импортировать их в специальное хранилище сертификатов операционной системы Windows для дальнейших криптографических операций. При этом если в списке не отмечен ни один сертификат, то данная кнопка будет недоступна.

Новый поиск - вернуться на страницу формирования условий запроса.

Домой - вернуться на домашнюю страницу зарегистрированного пользователя.

4.2.13. Сохранение сертификатов других пользователей на локальном компьютере

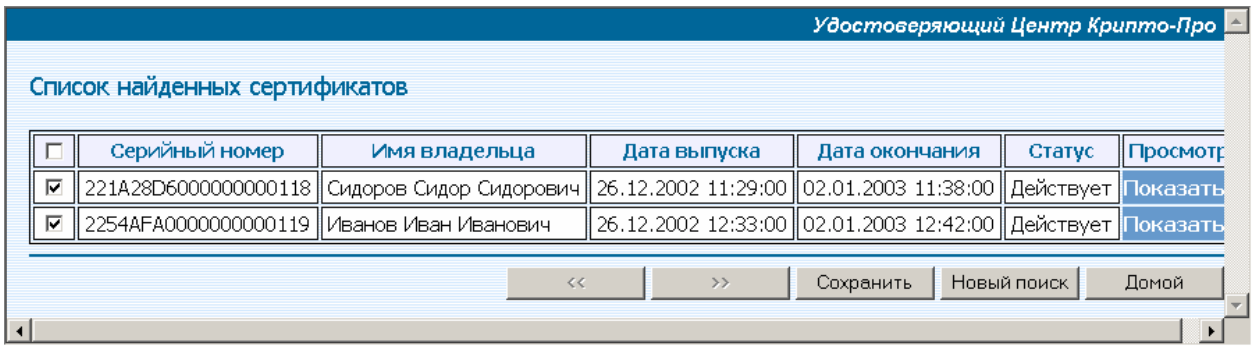
Для общения между собой пользователей – участников информационной системы электронного документооборота - с использованием средств криптографической защиты и электронной цифровой подписи (переписка с использованием E-Mail, обмен зашифрованными и подписанными ЭЦП файлами, подпись содержимого Web страниц) необходимо, чтобы у каждого такого пользователя на локальном компьютере имелись открытые ключи других пользователей. Данные ключи в системах с открытым распределением ключей оформляются в виде сертификатов широко распространенного открытого стандарта X509. Версии операционной системы Windows имеют встроенную поддержку, обеспечивающую полноценную работу с данными сертификатами.

Web интерфейс зарегистрированного пользователя Центра Регистрации позволяет осуществлять удаленный поиск требуемых сертификатов в Реестре Центра Регистрации, импортировать найденные сертификаты себе на локальный компьютер в виде файлов или в специально предназначенное для этого в операционной системе Windows хранилище.

4.2.13.1. Сохранение группы сертификатов

Для импорта сертификатов воспользуйтесь режимом поиска, описанным в предыдущих главах. Получив список требуемых сертификатов, отметьте в нем (см. Рисунок 46) строки таблицы с сертификатами, которые Вы хотели бы иметь у себя на компьютере (для проверки ЭЦП пользователей-владельцев данных сертификатов или для шифрования сообщений в их адрес).

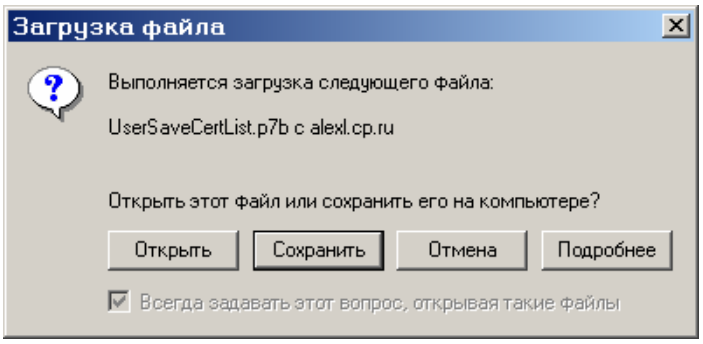
Рисунок 46. Окно с отмеченными сертификатами для сохранения в списке найденных



Если хоть одна строка списка помечена, то кнопка **Сохранить** станет доступна.

Нажмите кнопку **Сохранить**. При этом стандартный режим браузера MS IE предложит либо сохранить полученную от сервера информацию в файле на диске, либо открыть сообщение при помощи встроенных в операционную систему программ (см. Рисунок 47).

Рисунок 47. Окно загрузки файла с выбранными сертфиикатами

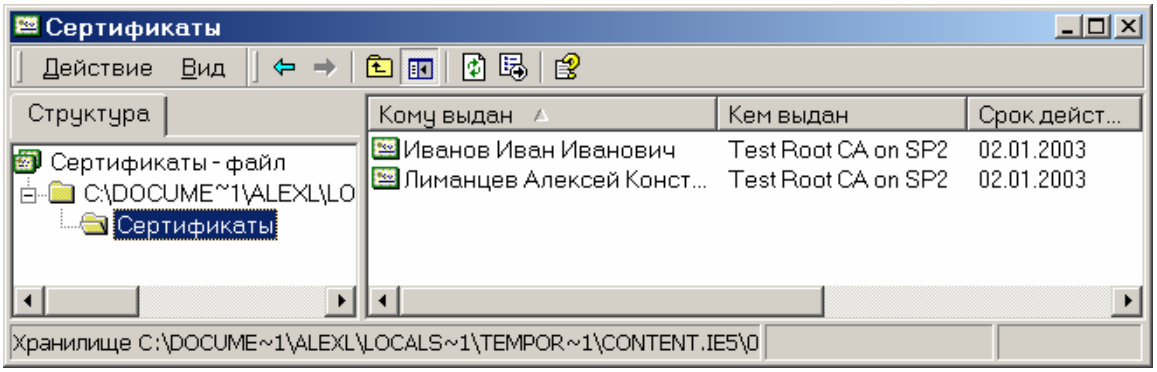


Если Вы не собираетесь сразу импортировать сертификаты в специальное хранилище ОС Windows, нажмите кнопку **Сохранить**(«Save»). В этом случае Вам будет предложено выбрать место в файловой директории, куда следует сохранить полученный файл.

Если вы собираетесь сразу импортировать сертификаты (или в Windows 2000 просмотреть список сертификатов, содержащихся в файле) нажмите кнопку **Открыть** («Open»).

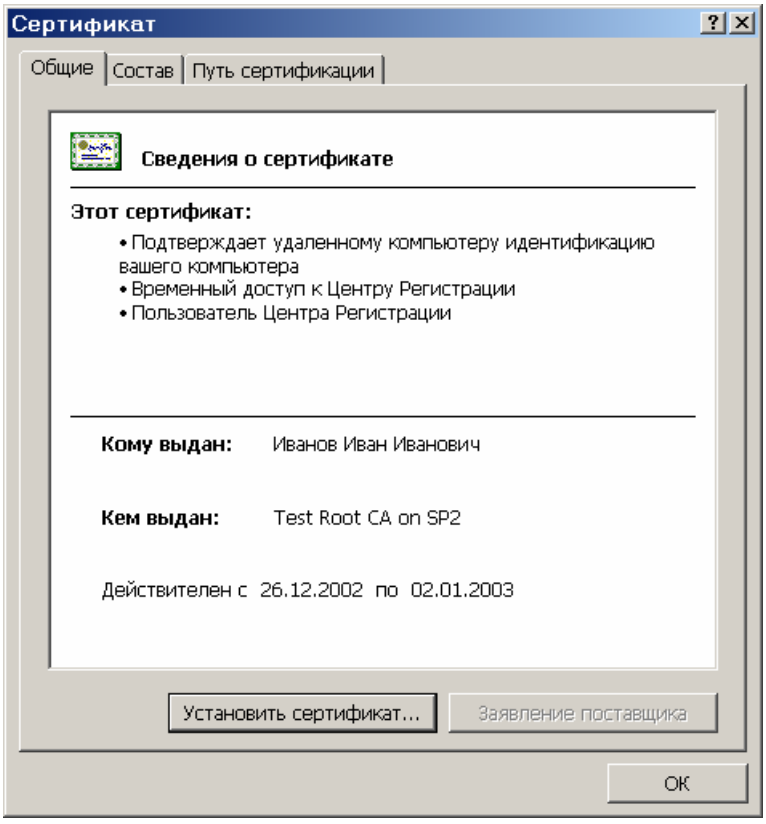
Необходимо отметить, что при нажатии кнопки **Открыть**, разные версии операционной системы ведут себя по разному. Windows 98 при этом сразу запускает мастер импорта сертификатов, содержащихся в файле, а Windows 2000 открывает данный файл для просмотра в следующем виде (см. Рисунок 48):

Рисунок 48. Окно просмотра загруженных сертификатов в MS Windows 2000



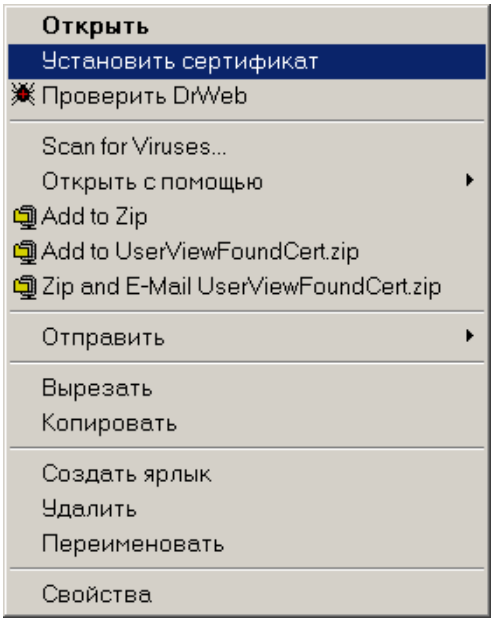
Используя данное окно, можно просмотреть каждый сертификат, содержащийся в полученном файле (кликнув на нем дважды мышкой) и в стандартном окне просмотра сертификата выбрать кнопку **Установить сертификат** («Import certificate»), для импорта сертификата в хранилище (см. Рисунок 49).

Рисунок 49. Окно свойств найденного сертификата



Для импорта сразу всех сертификатов в ОС Windows 2000 лучше сначала сохранить полученный файл на диске, а потом, кликнув на нем правой кнопкой мыши, из раскрывшегося меню выбрать пункт **Установить сертификат** (см. Рисунок 50).

Рисунок 50. Окно меню для установки нескольких сертификатов в MS Windows 2000



При этом запустится мастер установки (импорта) сертификатов в хранилище сертификатов пользователей. В ОС Windows 98 такой мастер запускается сразу, если Вы выберете режим «Открыть» при загрузке файла с выбранными сертификатами (см. Рисунок 9).

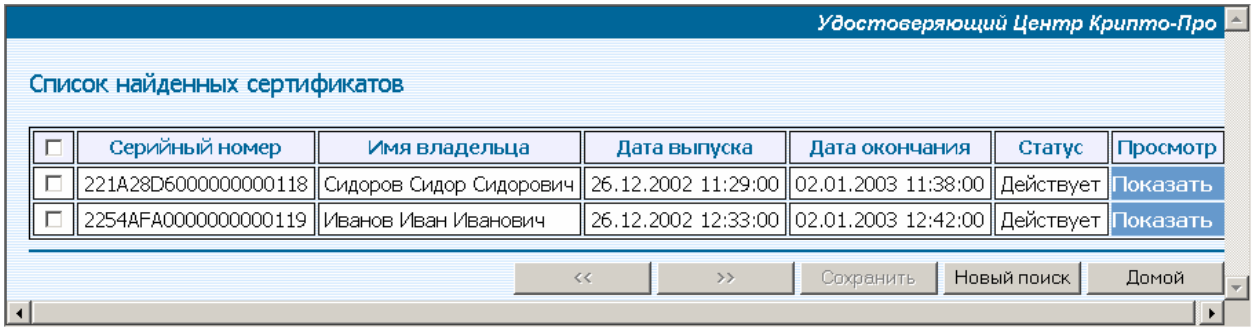
Далее следуйте указаниям Мастера импорта сертификатов, выбирая предлагаемые значения по умолчанию.

Примечание. Политикой безопасности Центра Регистрации может быть запрещен режим импорта чужих сертификатов. При этом загруженный с Центра Регистрации файл будет содержать только сертификаты, которые разрешены Вам для импорта политикой безопасности.

4.2.13.2. Сохранение отдельного сертификата

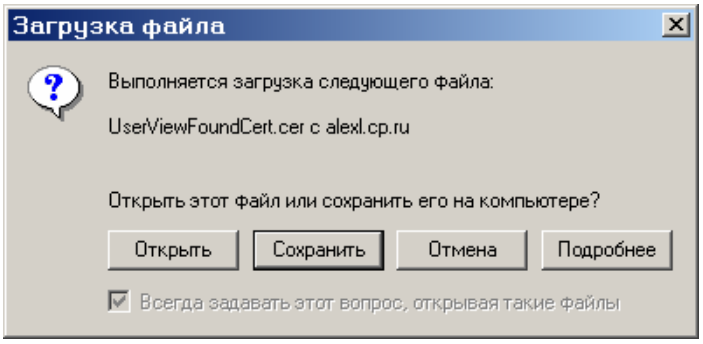
Для импорта отдельного сертификата на странице со списком отобранных в результате поиска сертификатов в правой колонке списка кликните мышкой на ссылке **Показать** в соответствующей строке списка (см. Рисунок 51):

Рисунок 51. Окно со списком найденных сертификатов для использования ссылки Показать



При этом стандартный режим браузера MS IE предложит вам либо сохранить сертификат (файл с расширением .cer) в файле на диске, либо открыть его при помощи встроенного в операционную систему режима просмотра сертификатов (см. Рисунок 52).

Рисунок 52. Окно загрузки файла с выбранным сертификатом



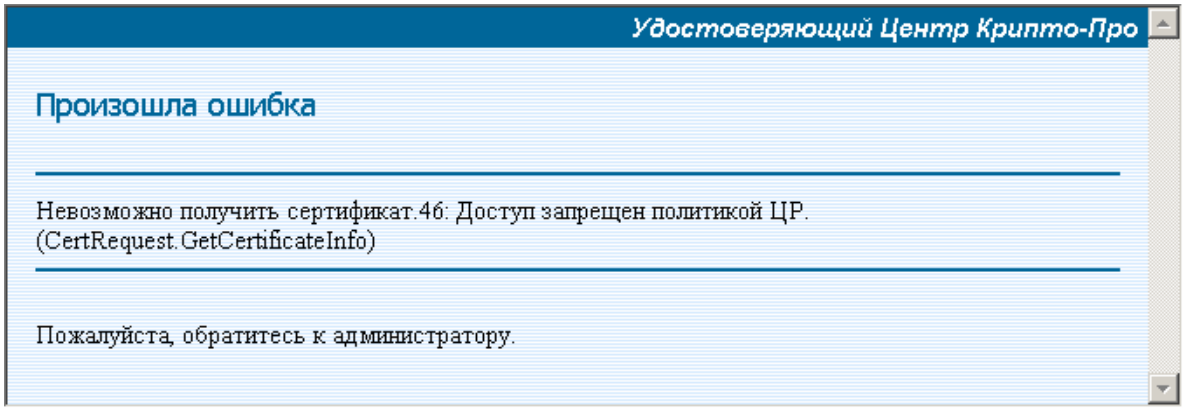
Если Вы не собираетесь просматривать или сразу импортировать полученные сертификаты в специальное хранилище ОС Windows нажмите кнопку **Сохранить** («Save»). В этом случае Вам будет предложено выбрать место в файловой директории, куда следует сохранить полученный сертификат.

Если же вы выберете режим **Открыть** («Open»), то загруженный с сервера сертификат будет отображен в стандартном окне просмотра сертификатов (см. Рисунок 49).

Для импорта сертификата в специальное хранилище операционной системы в данном окне нажмите кнопку «Установить сертификат». При этом будет запущен Мастер импорта сертификатов, описанный в предыдущей главе.

Примечание. Политикой безопасности Центра Регистрации может быть запрещен режим импорта чужих сертификатов. При этом при использовании данного режима работы (при клике на ссылке **Показать**) может быть выдано следующее сообщение (см. Рисунок 53):

Рисунок 53. Окно с сообщением о запрещении импорта сертификатов других пользователей



5. АРМ регистрации пользователей

Режим распределенной регистрации поддерживается Центром Регистрации в зависимости от его политики, определенной регламентом УЦ.

Под регистрацией пользователя в распределенном режиме понимается предоставление потенциальному пользователю возможности со своего рабочего места ввода персональных учетных данных, получения служебных ключей и служебного сертификата.

Регистрация пользователя в распределенном режиме выполняется в несколько этапов:

- Установка программного обеспечения СКЗИ «КриптоПро CSP», «КриптоПро TLS» и сертификата Центра сертификации
- Формирование запроса на регистрацию
- Формирование служебных ключей и запроса на служебный сертификат
- Получение и установка служебного сертификата

5.1. Запуск АРМ регистрации пользователей

Для запуска и работы с АРМ регистрации пользователей необходимо открыть окно браузера MS IE и перейти по адресу https://имя-Web-сервера-ЦР/ui/Register/RegGetSubject.asp, где имя_сервера_ЦР – имя Web-узла Центра регистрации, или воспользоваться стартовой страничкой Web-приложений Центра регистрации (см. Рисунок 18), где выбрать режим **Начать регистрацию**.

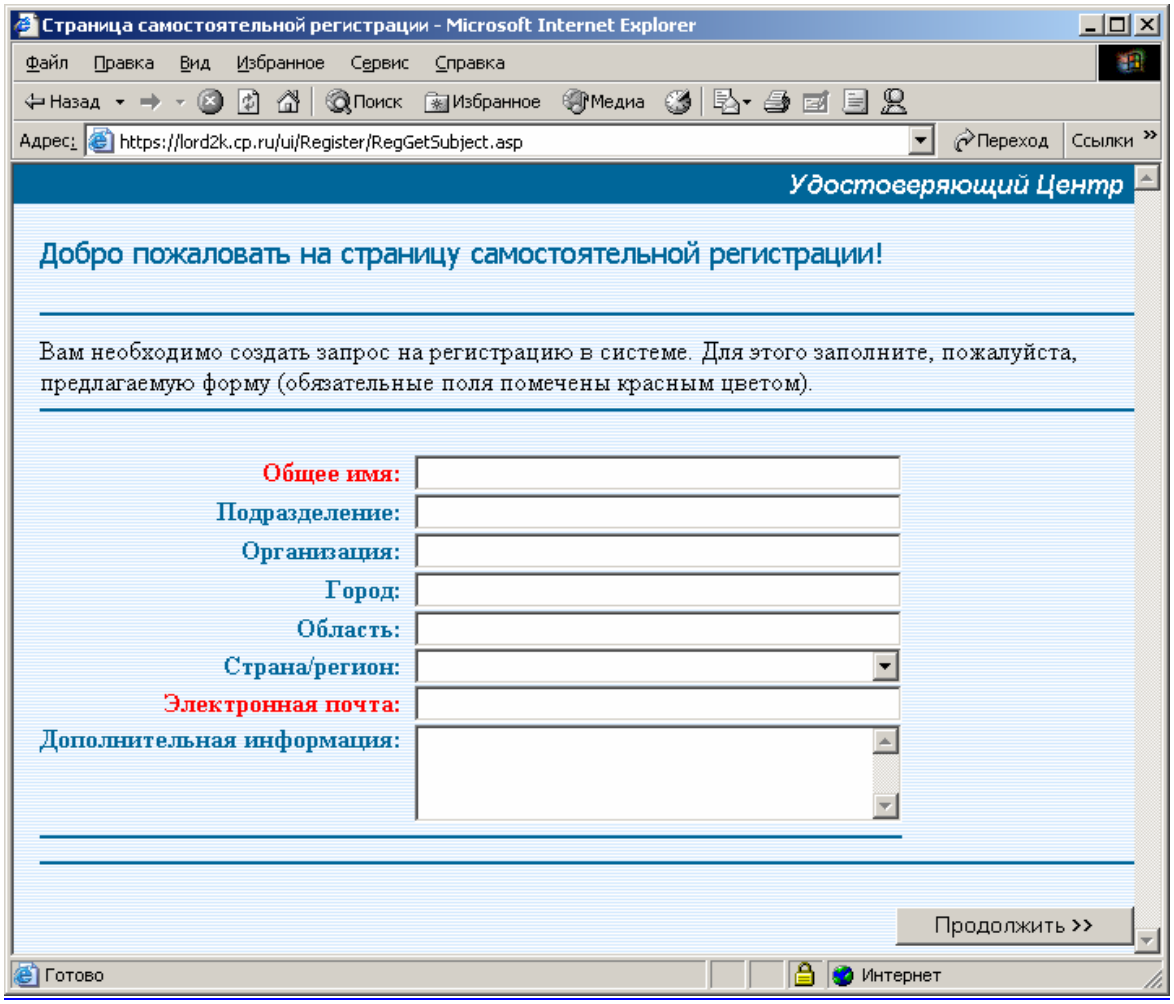
Процесс регистрации происходит в защищенном режиме с использованием протокола TLS, поэтому обращаем внимание, что в поле **адрес** необходимо вводить именно https (не http).

5.2. Процедура регистрации пользователей

5.2.1. Формирование и отправка запроса на регистрацию

Первой экранной формой окна браузера MS IE отображается экранная форма ввода значений атрибутов имени регистрируемого пользователя (см. Рисунок 54) для формирования запроса на регистрацию.

Рисунок 54. Окно ввода информации по атрибутам имени регистрируемого пользователя



Данная экранная форма формируется динамически, в соответствии с политикой имен Центра Регистрации, вследствие этого, набор атрибутов имени может изменяться и не соответствовать приведенному на рисунке выше.

Обязательные для заполнения поля отображаются красным цветом букв их наименований (наименования параметров также настраиваются в Центре Регистрации).

После ввода полей экранной формы необходимо нажать кнопку **Продолжить**.

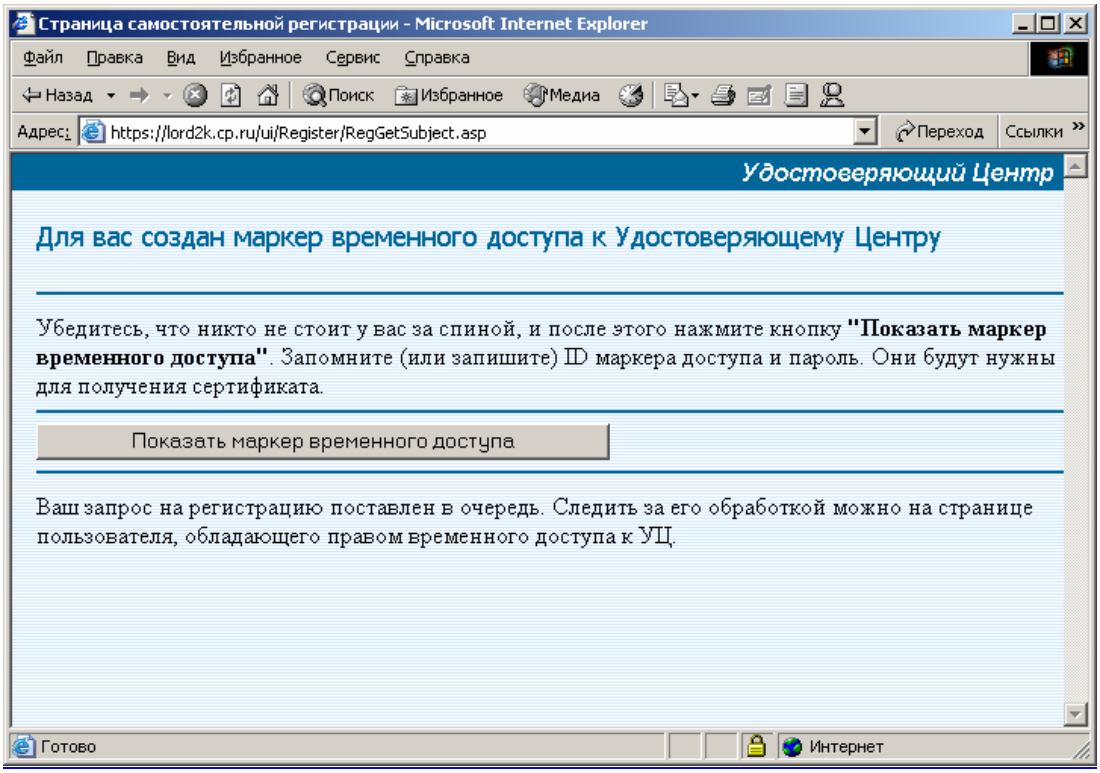
При этом происходит формирование запроса на регистрацию и постановка его в очередь на обработку на Центре Регистрации.

Дальнейшие действия зависят от настройки параметров работы Центра Регистрации.

5.2.2. Обработка запроса на регистрацию администратором Центра Регистрации

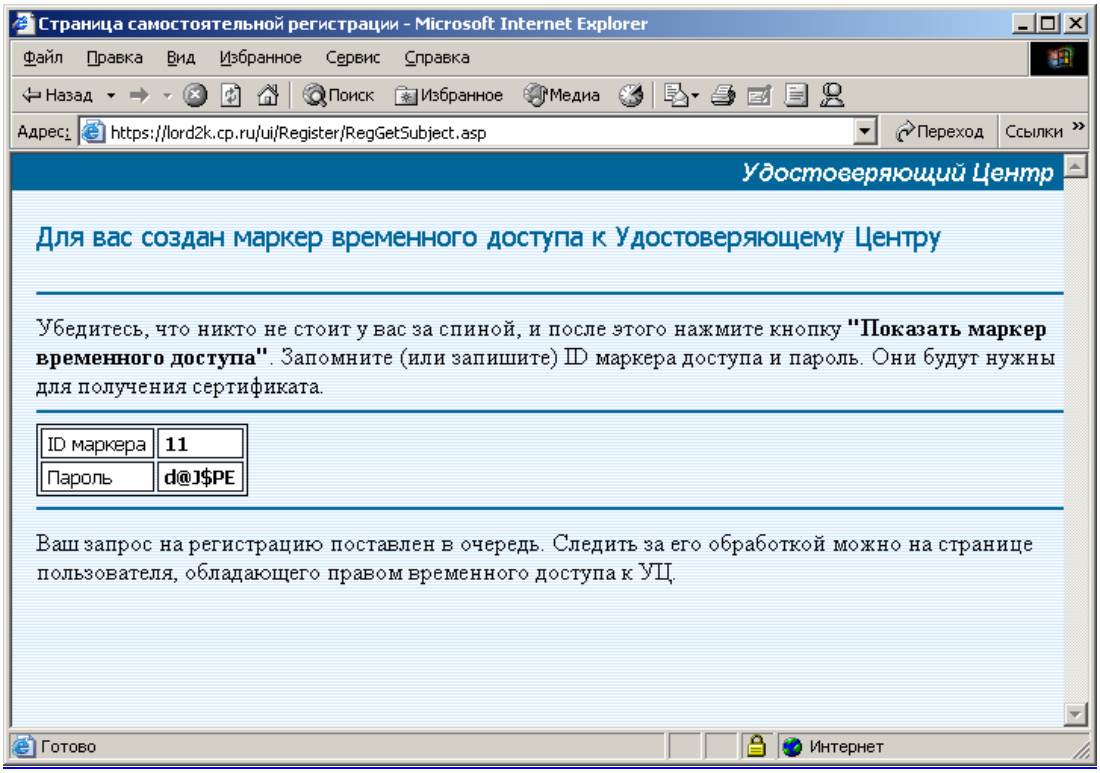
Если параметры работы Центра Регистрации настроены на обработку запроса на регистрацию, стоящего в очереди, администратором/оператором Центра Регистрации, то в окне браузера отразится экранная форма, приведенная на Рисунок 55.

Рисунок 55. Окно получения маркера временного доступа регистрируемого пользователя при обработке запроса администратором Центра Регистрации



Нажмите кнопку **Показать маркер временного доступа** для того, чтобы увидеть его и запомнить. Маркер временного доступа отображается в экранной форме, представленной ниже (см. Рисунок 56).

Рисунок 56. Окно отображения маркера временного доступа



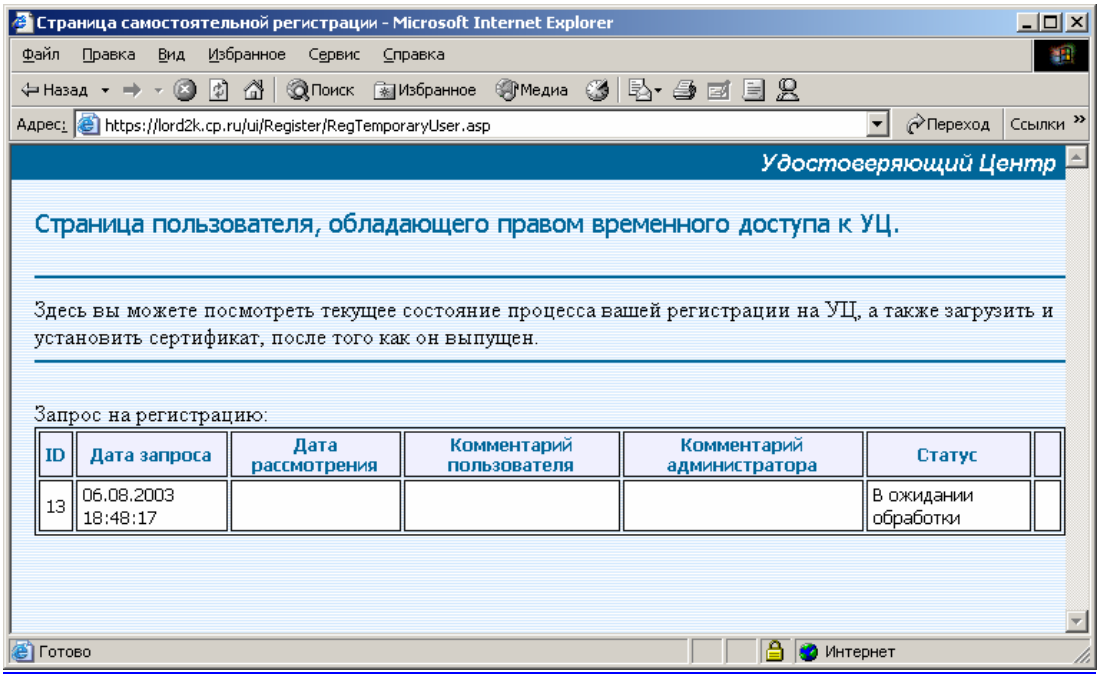
Запрос на регистрацию будет стоять в очереди Центра Регистрации до его обработки администратором/оператором Центра Регистрации.

До получения официального уведомления о завершении обработки запроса на регистрацию (как правило, уведомление рассылается по электронной почте) пользователь может получить статус обработки запроса.

Для этого надо открыть окно браузера MS IE и перейти по адресу https://имя-Web-сервера-ЦР/ui/Register/RegTemporaryUser.asp, где имя сервера ЦР – имя Web-узла Центра регистрации или выбрать режим **Вход для пользователей, обладающих маркером временного доступа** со стартовой страницы Web-приложений Центра регистрации (см. Рисунок 18).

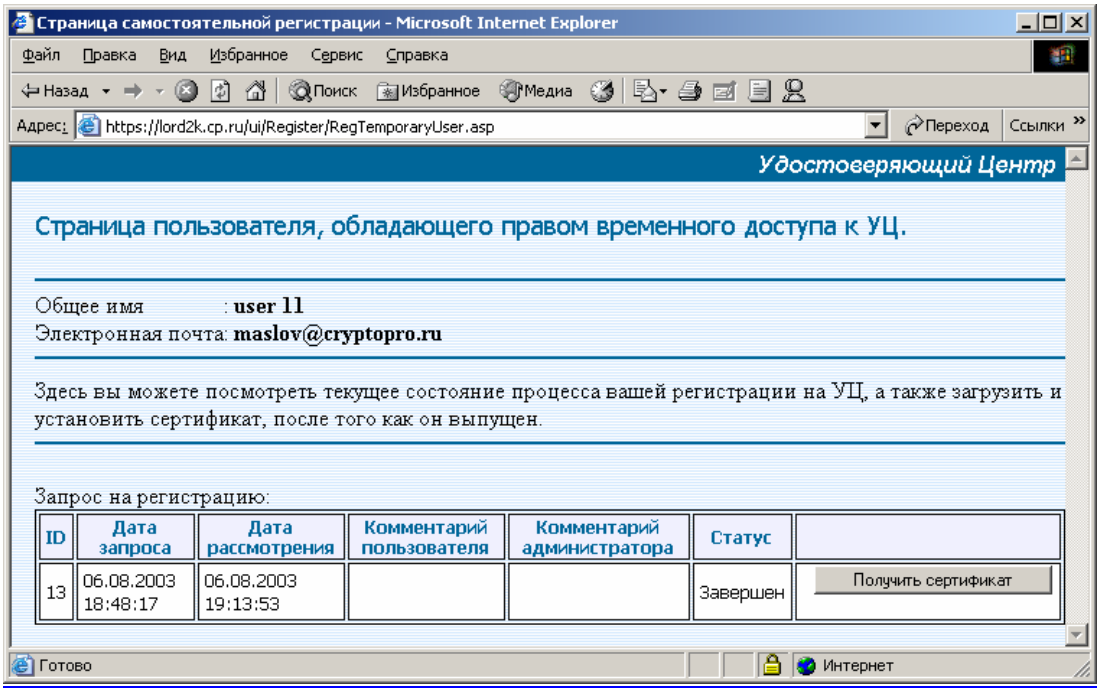
Статус обработки отражается в экранной форме, приведенной ниже (см. Рисунок 57).

Рисунок 57. Окно состояния обработки запроса на регистрацию



По завершению обработки запроса на регистрацию, экранная форма отображения статуса запроса принимает следующий вид (см. Рисунок 58).

Рисунок 58. Окно подтверждения обработки запроса на регистрацию

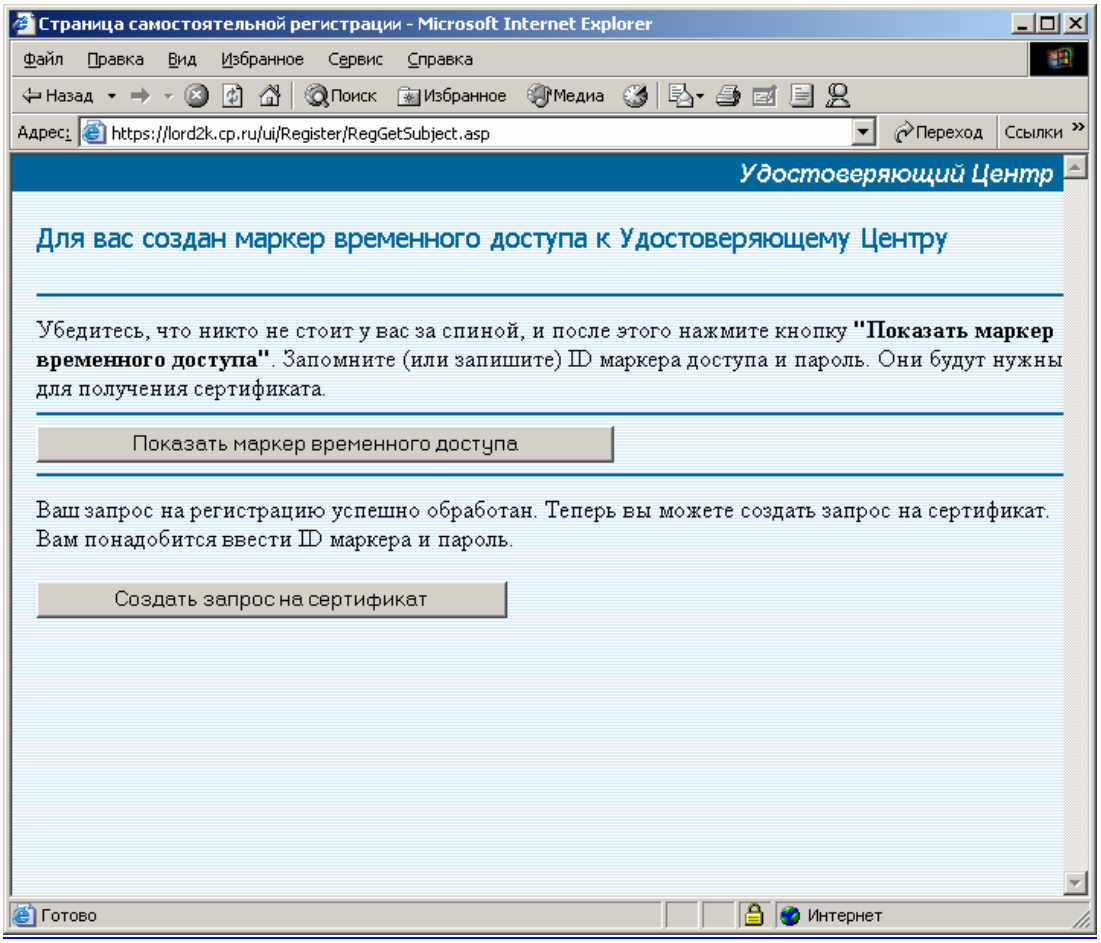


После этого нажмите кнопку **Получить сертификат** для перехода к процедуре формирования ключей и запроса на сертификат открытого ключа.

5.2.3. Автоматическая обработка запроса на регистрацию Центром Регистрации

Если параметры работы Центра Регистрации настроены на автоматическую обработку запроса на регистрацию, стоящего в очереди, то в окне браузера отразиться экранная форма, приведенная на Рисунок 59.

Рисунок 59. Окно получения маркера временного доступа регистрируемого пользователя при автоматической обработке запроса Центром Регистрации



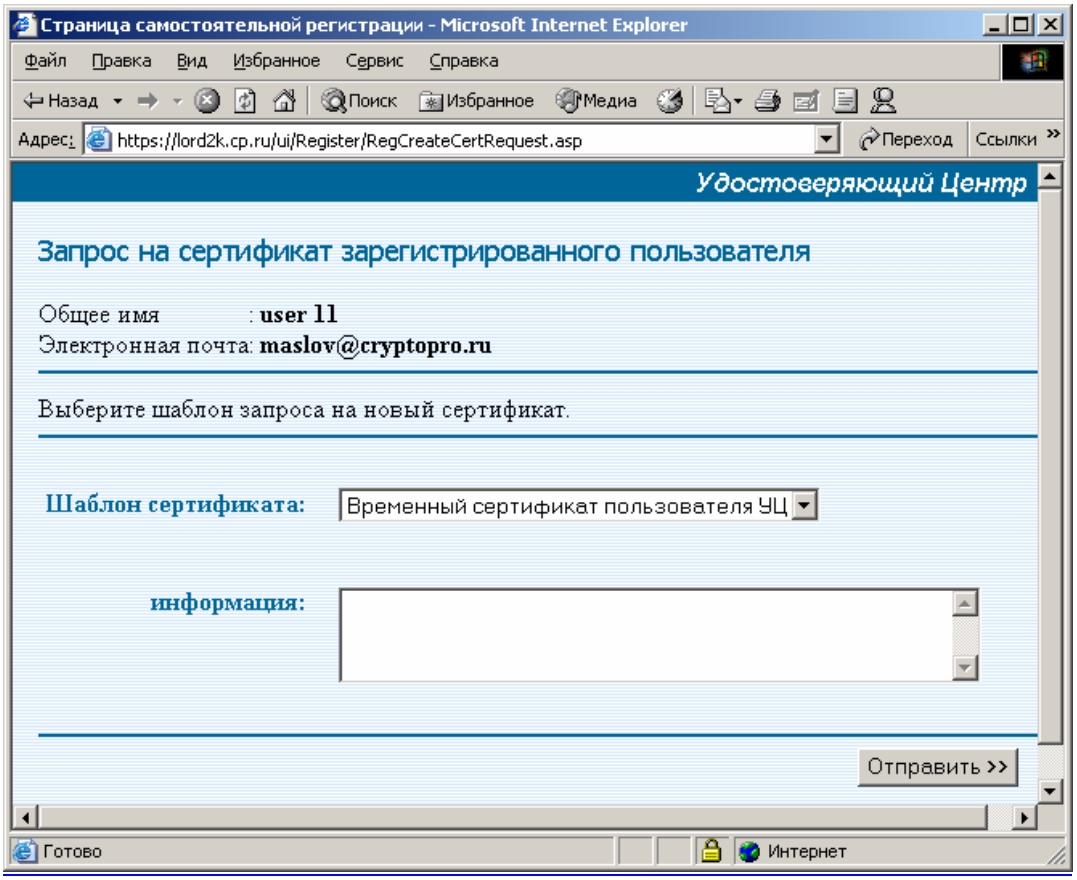
Нажмите кнопку **Показать маркер временного доступа** для того, чтобы увидеть его и запомнить.

После этого нажмите кнопку **Создать запрос на сертификат** для перехода к процедуре формирования ключей и запроса на сертификат открытого ключа.

5.2.4. Формирование ключей и запроса на сертификат открытого ключа

В экранной форме формирования ключей и запроса на сертификат открытого ключа (см. Рисунок 60) необходимо выбрать шаблон сертификата открытого ключа, ввести дополнительную информацию (по необходимости) и нажать кнопку **Отправить**.

Рисунок 60. Окно формирования запроса на сертификат открытого ключа процедуры удаленной регистрации пользователя



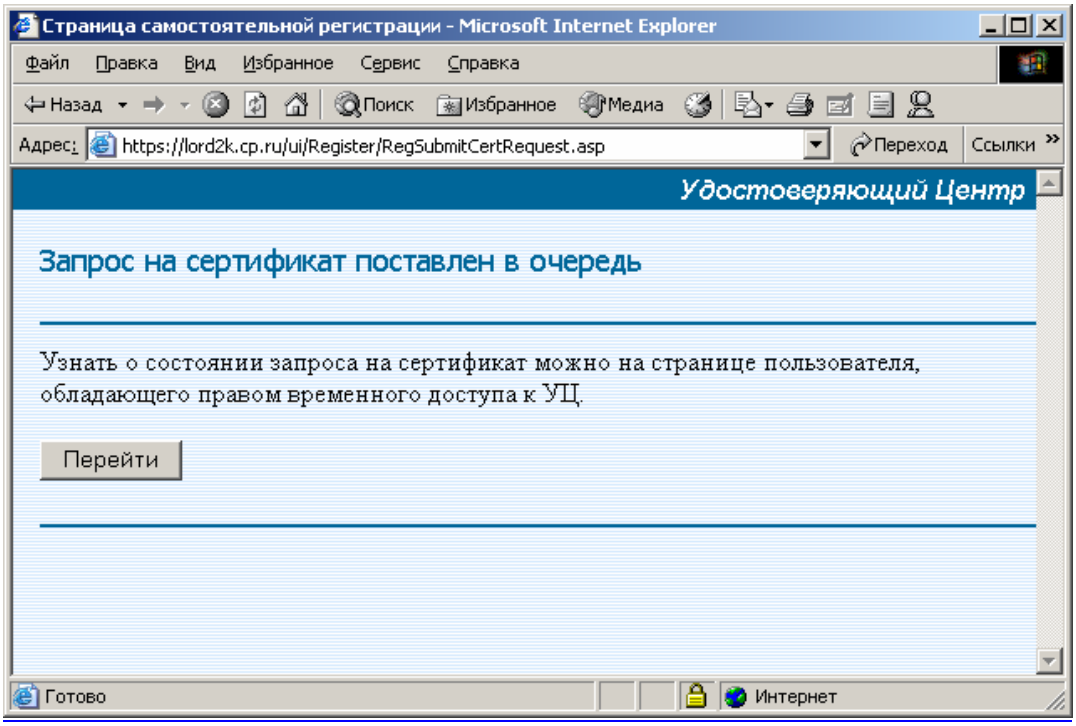
При этом происходит генерация ключей и формирование запроса на сертификат и постановка его в очередь на обработку на Центре Регистрации.

Дальнейшие действия зависят от настройки параметров работы Центра Регистрации.

5.2.5. Обработка запроса на сертификат администратором Центра Регистрации

Если параметры работы Центра Регистрации настроены на обработку запроса на сертификат, стоящего в очереди, администратором/оператором Центра Регистрации, то в окне браузера отразиться экранная форма, приведенная на Рисунок 61.

Рисунок 61. Окно уведомления о поставке в очередь запроса на сертификат процедуры удаленной регистрации пользователя



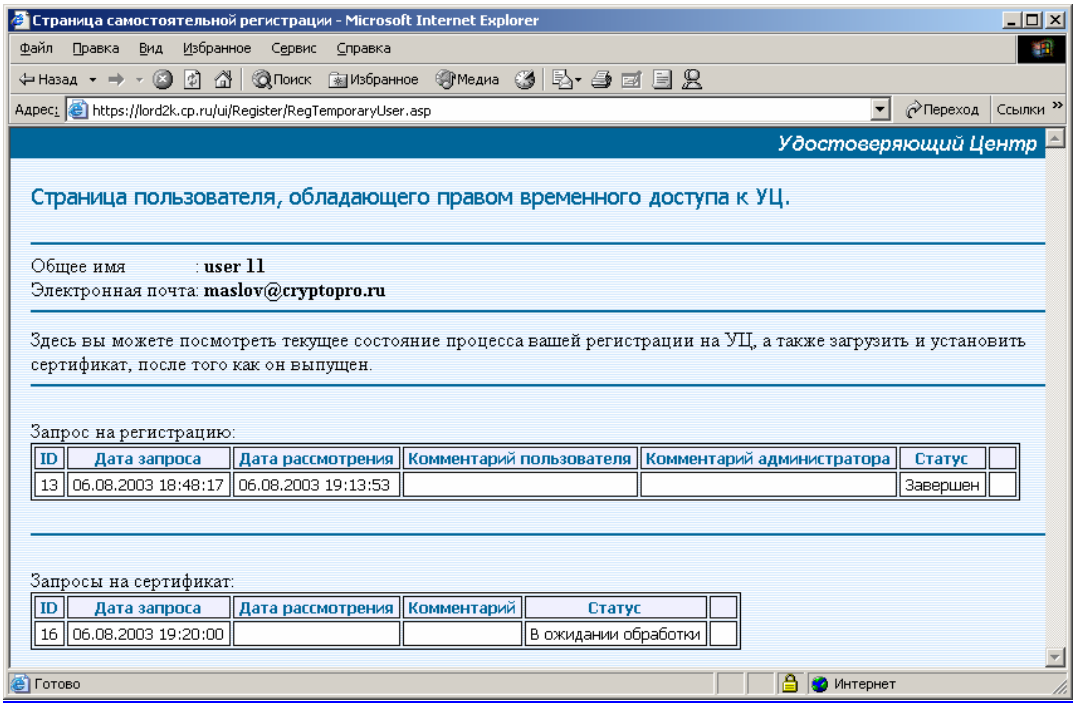
Запрос на сертификат будет стоять в очереди Центра Регистрации до его обработки администратором/оператором Центра Регистрации.

До получения официального уведомления о завершении обработки запроса на сертификат (как правило, уведомление рассылается по электронной почте) пользователь может получить статус обработки запроса.

Для этого надо открыть окно браузера MS IE и перейти по адресу https://имя-Web-сервера-ЦР/ui/Register/RegTemporaryUser.asp, где имя_сервера_ЦР – имя Web-узла Центра регистрации, или выбрать режим **Вход для пользователей, обладающих маркером временного доступа** со стартовой страницы Web-приложений Центра регистрации (см. Рисунок 18).

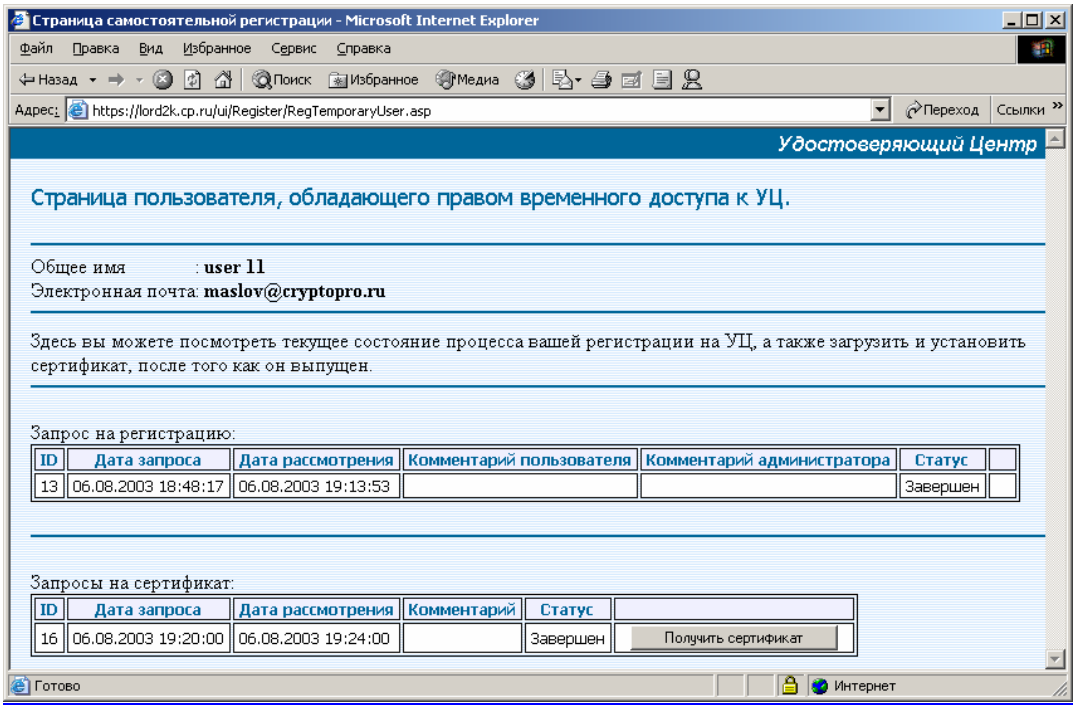
Статус обработки отражается в экранной форме, приведенной ниже (см. Рисунок 62).

Рисунок 62. Окно просмотра состояния обработки запроса на сертификат при регистрации пользователя



По завершению обработки запроса на сертификат администратором/оператором Центра Регистрации, экранная форма отображения статуса запроса принимает следующий вид (см. Рисунок 63).

Рисунок 63. Окно получения сертификата открытого ключа процедуры при регистрации пользователя



Нажмите кнопку **Получить сертификат** для получения и установки выпущенного сертификата.

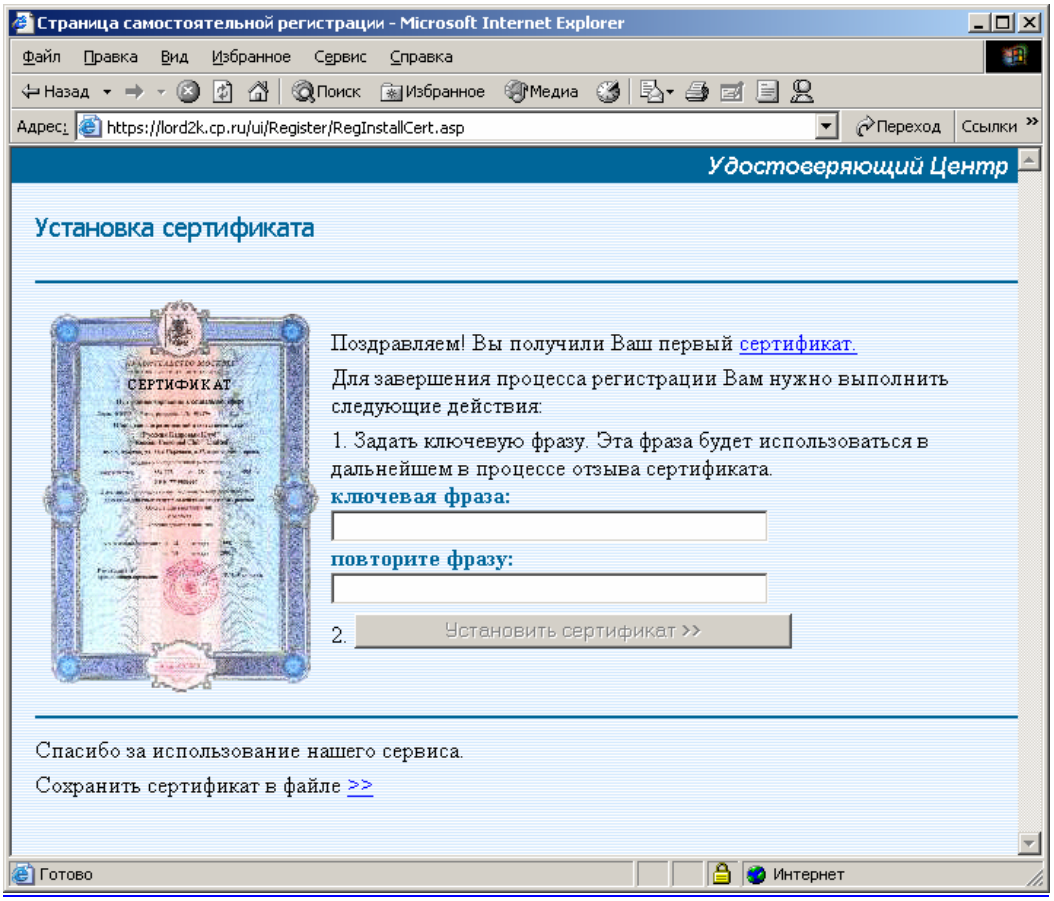
Получение и установка выпущенного сертификата выполняется в экранной форме, приведенной на Рисунок 64.

5.2.6. Автоматическая обработка запроса на сертификат Центром Регистрации

При автоматической обработке запроса на сертификат, пользователю отображается экранная форма формирования ключей и запроса на сертификат открытого ключа (см. Рисунок 60) в которой необходимо выбрать шаблон сертификата открытого ключа, ввести дополнительную информацию (по необходимости) и нажать кнопку **Отправить**.

Следующей экранной формой отображается форма получения и установки изготовленного по запросу сертификата открытого ключа (см. Рисунок 64).

Рисунок 64. Окно получения и установки первого сертификата открытого ключа



При нажатии на кнопку **Установить сертификат**, происходит установка выпущенного сертификата в хранилище сертификатов текущего пользователя, в раздел **Личные**.

6. Работа зарегистрированного пользователя, получившего маркер временного доступа

АРМ зарегистрированного пользователя с маркерным доступом предназначен для выполнения следующих задач:

- Генерация ключей;
- Формирование запроса на сертификат открытого ключа и постановка его в очередь на обработку на Центр Регистрации;
- Получение и установка выпущенного сертификата открытого ключа.

АРМ предназначен для использования следующими категориями пользователей УЦ:

- Пользователи, проходящие процедуру регистрации в распределенном режиме и разрывающие соединение с Центром Регистрации в процессе работы;
- Пользователи, в адрес которых был сформирован администратором ЦР маркер временного доступа.

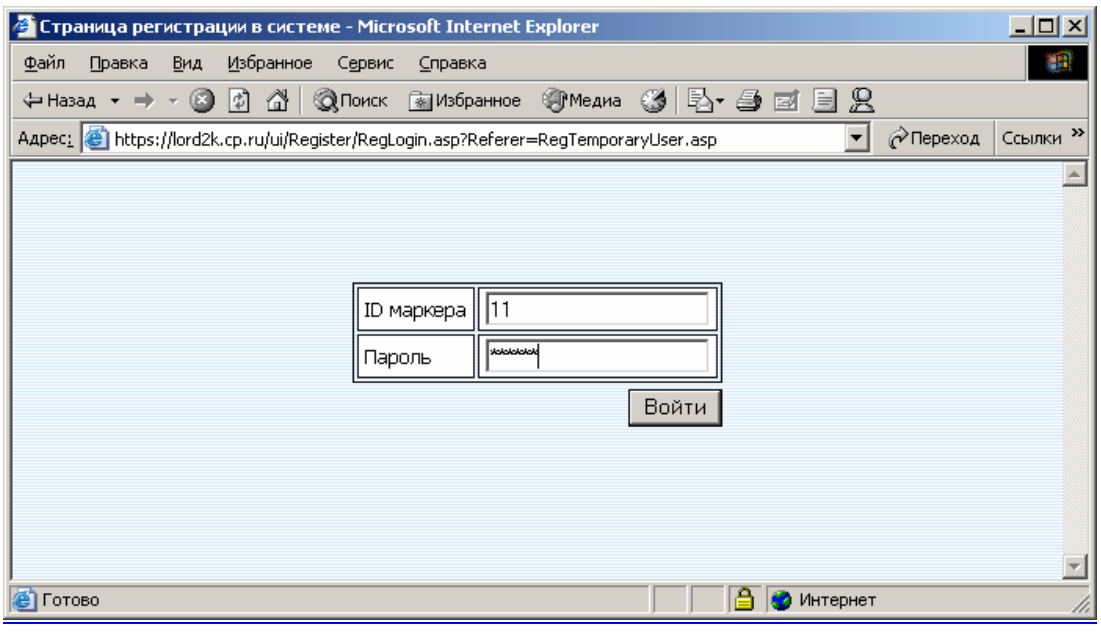
Если зарегистрированный пользователь УЦ не имеет ни одного действующего сертификата открытого ключа, администратор/оператор Центра Регистрации может сформировать для него маркер временного доступа для получения доступа к программным средствам АРМ зарегистрированного пользователя с маркерным доступом.

6.1. Запуск АРМ зарегистрированного пользователя с маркерным доступом

Для запуска и работы с АРМ зарегистрированного пользователя с маркерным доступом необходимо открыть окно браузера MS IE и перейти по адресу https://имя_сервера_ЦР/UI/Register/RegTemporaryUser.ASP, где имя_сервера_ЦР – имя Web-узла Центра регистрации, или воспользоваться стартовой страничкой Web-приложений Центра регистрации (см. Рисунок 18), где выбрать режим **Вход для пользователей, обладающих маркером временного доступа**.

Для доступа к АРМ зарегистрированного пользователя с маркерным доступом требуется ввести параметры маркера временного доступа (см. Рисунок 65).

Рисунок 65. Окно ввода параметров маркера временного доступа



7. Перечень рисунков

8. Перечень терминов

Автоматизированная Система (АС)

Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций

Администратор безопасности

Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Безопасность информации

Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз

Документ в электронной форме (электронный документ)

Информация, представленная в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, могущая быть преобразованной в форму, пригодную для однозначного восприятия человеком, и имеющая атрибуты для идентификации документа;

Доступ к информации (Доступ)

Ознакомление с информацией, ее обработка, в частности, копирование и модификация

Закрытый ключ

Криптографический ключ, который хранится пользователем системы в тайне. Он используется для формирования электронной цифровой подписи и/или шифрования данных.

Запрос на регистрацию

Сообщение, содержащее необходимую информацию для предварительной регистрации в качестве временного пользователя на Центре регистрации. Формируется в Web-приложении самостоятельной регистрации, после чего передается через Центр регистрации, где и обрабатывается. Результатом обработки является сообщение по электронной почте о порядке дальнейших действий.

Запрос на сертификат

Сообщение, содержащее необходимую информацию для получения сертификата. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр регистрации Центру Сертификации, где и обрабатывается. Результатом обработки является выпущенный сертификат или сообщение об ошибке.

Запрос на отзыв сертификата

Сообщение, содержащее необходимую информацию для отзыва сертификата. Формируется в АРМ Пользователя или в АРМ Администратора, после чего передается через Центр регистрации Центру Сертификации, где и обрабатывается. Результатом обработки является отзыв сертификата или сообщение об ошибке.

Защита от несанкционированного доступа (Защита от НСД)

Предотвращение или существенное затруднение несанкционированного доступа.

Защищенное средство вычислительной техники (защищенная АС)

Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты

Идентификатор доступа

Уникальный признак субъекта или объекта доступа

Идентификация

Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационное обеспечение (ИО)

Совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в АС при ее функционировании

Класс защищенности средств вычислительной техники, автоматизированной системы

Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации

Ключ (криптографический ключ)

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Ключевая пара

Открытый и закрытый ключи.

Ключевой носитель

Объект системы, который может содержать один или несколько ключевых контейнеров. Каждый ключевой контейнер содержит следующую информацию: только ключ подписи, только ключ шифрования, ключ подписи и ключ шифрования одновременно. Дополнительно ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей и их целостности. Каждый контейнер является полностью самостоятельным и содержит всю необходимую информацию для работы как с самим контейнером, так и с закрытыми ключами.

Комплекс средств защиты (КСЗ)

Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации

Компрометация ключа

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

1. Потеря ключевых носителей.
2. Потеря ключевых носителей с их последующим обнаружением.
3. Увольнение сотрудников, имевших доступ к ключевой информации.
4. Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа.
5. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
6. Нарушение печати на сейфе с ключевыми носителями.
7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и

доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

Различают два вида компрометации секретного ключа: **явную** и **неявную**. Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

Многоуровневая защита

Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности

Модель защиты

Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа

Модуль автоматизированной системы (модуль АС)

Часть АС, реализующая одну или более взаимосвязанных функций АС

Нарушитель правил разграничения доступа (Нарушитель ПРД)

Субъект доступа, осуществляющий несанкционированный доступ к информации

Несанкционированный доступ к информации (НСД)

Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем

Объект доступа

Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа

Открытый ключ

Криптографический ключ, который связан с закрытым ключом с помощью особого математического соотношения. Открытый ключ известен другим пользователям системы и предназначен для проверки электронной цифровой подписи и шифрования. При этом открытый ключ не позволяет вычислить закрытый ключ.

Плановая смена ключей

Смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

Подтверждение подлинности ЭЦП

Положительный результат проверки правильности ЭЦП, выработанной правомочным лицом из исходной информации путем применения принадлежащего ему закрытого ключа ЭЦП, полученный с использованием зарегистрированного и сертифицированного открытого ключа ЭЦП

Показатель защищенности средств вычислительной техники (Показатель защищенности)

Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники

Пользователь автоматизированной системы (пользователь АС)

Лицо, участвующее в функционировании АС или использующее результаты ее функционирования.

Пользователь АС зарегистрированный

Пользователь АС или системный сервис, имеющий учетную запись в АС.

Правила разграничения доступа (ПРД)

Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Проверка электронной подписи документа

Проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ подписавшего пользователя. Если рассматриваемое соотношение оказывается выполненным, то подпись признается правильной, а сам документ - подлинным, в противном случае документ считается измененным, а подпись под ним - недействительной.

Программное обеспечение (ПО)

Совокупность программ на носителях информации и программных документов, предназначенных для отладки, функционирования и проверки работоспособности АС

Санкционированный доступ к информации (СД)

Доступ к информации, не нарушающий правила разграничения доступа

Сертификат

1. Документ, выданный и заверенный удостоверяющим центром, подтверждающий принадлежность открытого ключа ЭЦП определенному лицу. Сертификат может содержать дополнительную информацию, необходимую для обеспечения безопасности использования открытого ключа ЭЦП. В случае, когда сертификат выдается в форме электронного документа, он подписывается ЭЦП этого центра

2. Электронный документ, который содержит открытый ключ субъекта и подписан электронной цифровой подписью его издателя. Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, которая его идентифицирует.

Формат сертификата определен в рекомендациях ITU-T 1997 года X.509 [X.509] и рекомендациях IETF 1999 года RFC 2459 [RFC 2459].

Сертификат защиты

Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных

Сертификация уровня защиты

Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите

Система защиты информации от несанкционированного доступа (СЗИ НСД)

Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Система защиты секретной информации (СЗСИ)

Комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах

Система разграничения доступа (СРД)

Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах

Список отзыва

Список отозванных сертификатов (CRL – Certificate Revocation List). УЦ поддерживает отзыв сертификатов и публикацию списков отозванных сертификатов.

Пользователи УЦ могут получить эту информацию и записать ее в свое локальное хранилище, чтобы использовать для последующей проверки сертификатов.

Средство защиты от несанкционированного доступа (Средство защиты от НСД)

Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа

Средство криптографической защиты информации (СКЗИ)

Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности

Средство электронной цифровой подписи

Совокупность программных и технических средств, реализующих функцию выработки и проверки электронной цифровой подписи

Субъект доступа

Лицо или системный сервис (процесс), действия которого регламентируются правилами разграничения доступа.

Техническое обеспечение (ТО)

Совокупность средств реализации управляющих воздействий, средств получения, ввода, подготовки, преобразования, обработки, хранения, регистрации, вывода, отображения, использования и передачи данных с конструкторской и эксплуатационной документацией.

Уровень полномочий субъекта доступа

Совокупность прав доступа субъекта доступа

Учетная запись

Информация, хранимая в АС, служащая для идентификации, аутентификации, авторизации действий пользователей АС и системных сервисов (Login, пароль, цифровой сертификат), а также содержащая прочие, необходимые для функционирования АС характеристики пользователей и сервисов (E-mail, адрес и т.п.)

Функция автоматизированной системы (функция АС)

Совокупность действий АС, направленная на достижение определенной цели, на выполнение определенного технологического процесса.

Центр по удостоверению подлинности электронной цифровой подписи (удостоверяющий центр)

Юридическое лицо или выделенное подразделение юридического лица, обладающие правомочиями на удостоверение принадлежности конкретного открытого ключа ЭЦП определенному пользователю

Целостность информации

Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения)

Центр Сертификации (Удостоверяющий центр)

Компонент Удостоверяющего центра. Выполняет функции службы сертификации: выпуск сертификатов, отзыв сертификатов, а также генерацию списков отзыва.

Центр регистрации

Компонент Удостоверяющего центра. Выполняет функции промежуточного звена, осуществляющего передачу запросов от пользователей и администраторов Центра регистрации центру сертификации. В процессе этой передачи осуществляется аутентификация пользователя, проверка корректности передаваемой им информации, а также фиксация этой информации в базе данных ЦР.

Шифрование

Процесс зашифрования или расшифрования.

Шифрование информации – взаимнооднозначное математическое (криптографическое) преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок шифрованной информации, также представленной в цифровой кодировке. Термин шифрование объединяет в себе два процесса: зашифрование и расшифрование информации.

Если зашифрование и расшифрование осуществляются с использованием одного и того же ключа, то такой алгоритм криптографического преобразования называется симметричным, в противном случае — асимметричным.

Прочитать зашифрованное сообщение (информацию) может только пользователь, имеющий тот же секретный ключ шифрования.

Электронная цифровая подпись (ЭЦП)

Последовательность символов, полученная в результате криптографического преобразования исходной информации с использованием закрытого ключа ЭЦП, которая позволяет подтверждать целостность и неизменность этой информации, а также ее авторство при условии использования открытого ключа ЭЦП и его сертификата.

9. Перечень сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
DN	Отличительное имя (Distinguished Name)
ITU-T	Международный комитет по телекоммуникациям (International Telecommunication Union)
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol. Упрощенный протокол доступа к справочнику
TM	Устройство хранения информации на таблетке touch-memory
PKI	Public Key Infrastructure. Аналог ИОК.
RDN	Относительное отличительное имя (Relative Distinguished Name)
URI	Единый идентификатор ресурса (Uniform Resource Identifier)
URL	Единый локатор ресурса (Uniform Resource Locator)
АС	Автоматизированная система
АРМ	Автоматизированное рабочее место
ДСЧ	Датчик случайных чисел
ИОК	Инфраструктура Открытых Ключей
КП	Конечный пользователь
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей. Сетевой справочник
ЦР	Центр Регистрации
ЦС	Центр Сертификации
УЦ	Удостоверяющий центр
ЭЦП	Электронная цифровая подпись

10. Перечень ссылочных документов

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.

[RFC 2459] RFC 2459. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999.

[PKCS-7] RSA Laboratories. *PKCS #7: Cryptographic Message Syntax Standard.* Version 1.5, November 1993.

[PKCS-10] RSA Laboratories. *PKCS #10:* Certification Request Syntax Standard.

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводи-тельного документа и дата	Подпись	Дата
Изм.	измененных	замененных	новых	аннулированных					