

Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Казанский национальный исследовательский технический университет
им. А.Н. Туполева-КАИ»

Кафедра систем информационной безопасности

Д.В. Катасёва

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

по дисциплине

«Защищенный электронный документооборот»

для бакалавров направления 090900.62

«Информационная безопасность»

Казань - 2014 г.

ЛАБОРАТОРНАЯ РАБОТА №1

Тема лабораторной работы

Подготовка к установке удостоверяющего центра: настройка общесистемного программного обеспечения, установка дополнительных компонент Windows, изготовление первого сертификата

Цель работы

Изучить процедуры подготовки к установке удостоверяющего центра «КриптоПро УЦ»

ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

Служба очередей сообщений

Служба очередей сообщений – это приложение, гарантирующее надежную посылку и получение сообщения. Сообщения могут быть всем, чем угодно, начиная от XML-файлов и заканчивая наборами записей ADO и документами Microsoft Word. Не имеет значения, что посылать, важно знать, что все, что поступило в очередь, будет с гарантией доставлено.

Ниже приведено несколько факторов, указывающих на необходимость службы очередей сообщений в приложении:

- прямые вызовы между клиентами и серверами по соединениям могут завершиться неудачей.
- сообщения могут быть посланы очередям, когда ресурсы недоступны, к примеру, это другие очереди, и получены, когда ресурсы вновь становятся доступными;
- сообщения имеют приоритеты: заказы продуктов доставляются раньше, чем журнальные файлы или другие неважные ресурсы;
- служба на 100% поддерживает транзакции, поэтому она может быть частью транзакции COM+, поддерживает механизм доставки "все или ничего";
- доступ к службе основан на Windows Security, что гарантирует работу в защищенной среде.

Service Pack 4

Service pack 4 представляет из себя сборник обновлений, исправлений и дополнений для Windows 2000 server.

MSCA

MSCA (Microsoft Certified Systems Administrator - сертифицированный системный администратор) Windows® 2000 предоставляют потребителям встроенную инфраструктуру открытых ключей (Public Key Infrastructure, PKI), позволяющую осуществлять безопасный обмен информацией через сеть Интернет, внешние сети, а также интрасети. Службы сертификации осуществляют проверку и подтверждают подлинность каждой из сторон, участвующих в обмене электронными данными. Кроме этого они позволяют пользователям дома входить в него с помощью смарт-карт, обеспечивая тем самым дополнительную безопасность.

КриптоПро CSP

Средство криптографической защиты информации КриптоПро CSP используется в качестве средства, реализующего криптографические функции на базе российских криптографических алгоритмов.

Основные функции, реализуемые КриптоПро CSP:

- генерация закрытых (256 бит), открытых (1024 бита для ГОСТ Р 34.10-94 и 512 бит для ГОСТ Р 34.10-2001) ключей ЭЦП и шифрования;
- формирование закрытых ключей с записью на ключевые носители;
- возможность хранения сертификатов открытых ключей в ключевом контейнере;
- возможность генерации ключей с различными параметрами в соответствии с ГОСТ Р 34.10-94;
- возможность генерации ключей с различными параметрами в соответствии с ГОСТ Р 34.10-2001;

- хеширование данных в соответствии с ГОСТ Р 34.11-94;
- шифрование данных во всех режимах, определенных ГОСТ 28147-89;
- имитозащита данных в соответствии с ГОСТ 28147-89;
- формирование электронной цифровой подписи в соответствии с ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001;
- опциональное использование пароля (пин-кода) для дополнительной защиты ключевой информации;
- реализация мер защиты от НСД ключевой информации пользователя.

Ключевая система СКЗИ КриптоПро CSP обеспечивает возможность парно-выборочной связи пользователей сети с использованием для каждой пары пользователей уникальных ключей, создаваемых на основе принципа открытого распределения ключей.

Средство криптографической защиты информации КриптоПро CSP является системой с открытым распределением ключей. Открытые ключи подписи и шифрования представляются в виде сертификатов открытых ключей. Закрытый ключ ЭЦП может быть использован только для формирования ЭЦП. Закрытый ключ шифрования может быть использован как для формирования ключа связи с другим пользователем, так и для формирования ЭЦП.

КриптоПро TLS

Средство сетевой аутентификации КриптоПро TLS используется совместно с КриптоПро CSP и предназначено для клиент-серверной аутентификации и шифрования сообщений.

Основные функции, реализуемые модулем КриптоПро TLS:

- две схемы аутентификации с использованием обмена ключей по алгоритму Диффи-Хэллмана и хеширования в соответствии с ГОСТ Р 34.11-94: односторонняя – анонимный клиент, аутентифицируемый сервер и двухсторонняя – аутентифицируемые клиент и сервер;

- выработка и проверка электронной цифровой подписи в соответствии с ГОСТ Р 34.10-94 или ГОСТ Р 34.10-2001;
- шифрование соединения в соответствии с ГОСТ 28147-89;
- вычисление имитовставки передаваемых данных в соответствии с ГОСТ 28147-89;

КОНТРОЛЬНЫЕ ВОПРОСЫ

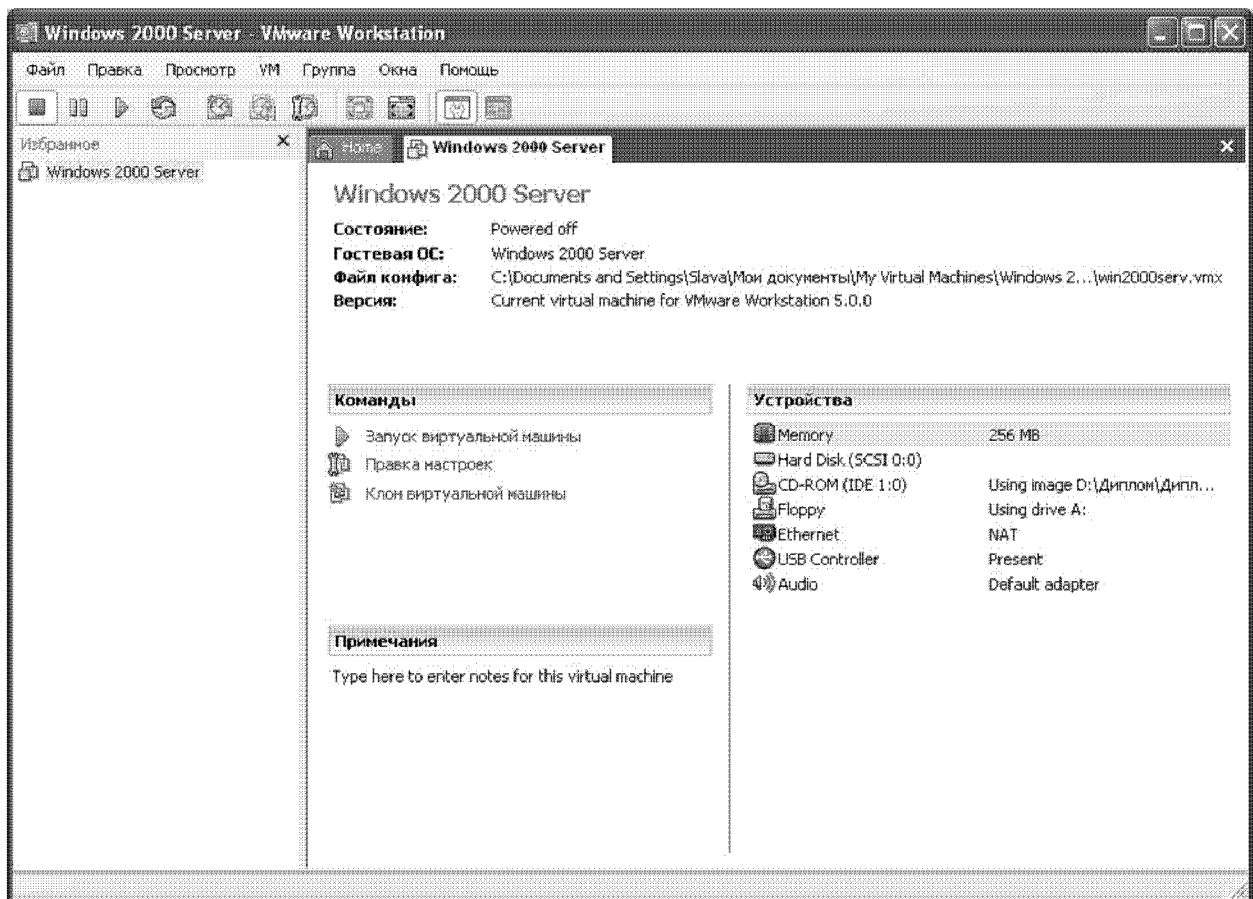
1. Что представляет из себя Service Pack?
2. Что такое служба очередей сообщений?
3. Что такое MSCA?
4. Что такое «Крипто Про CSP»?
5. Что такое «Крипто Про TLS»?

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

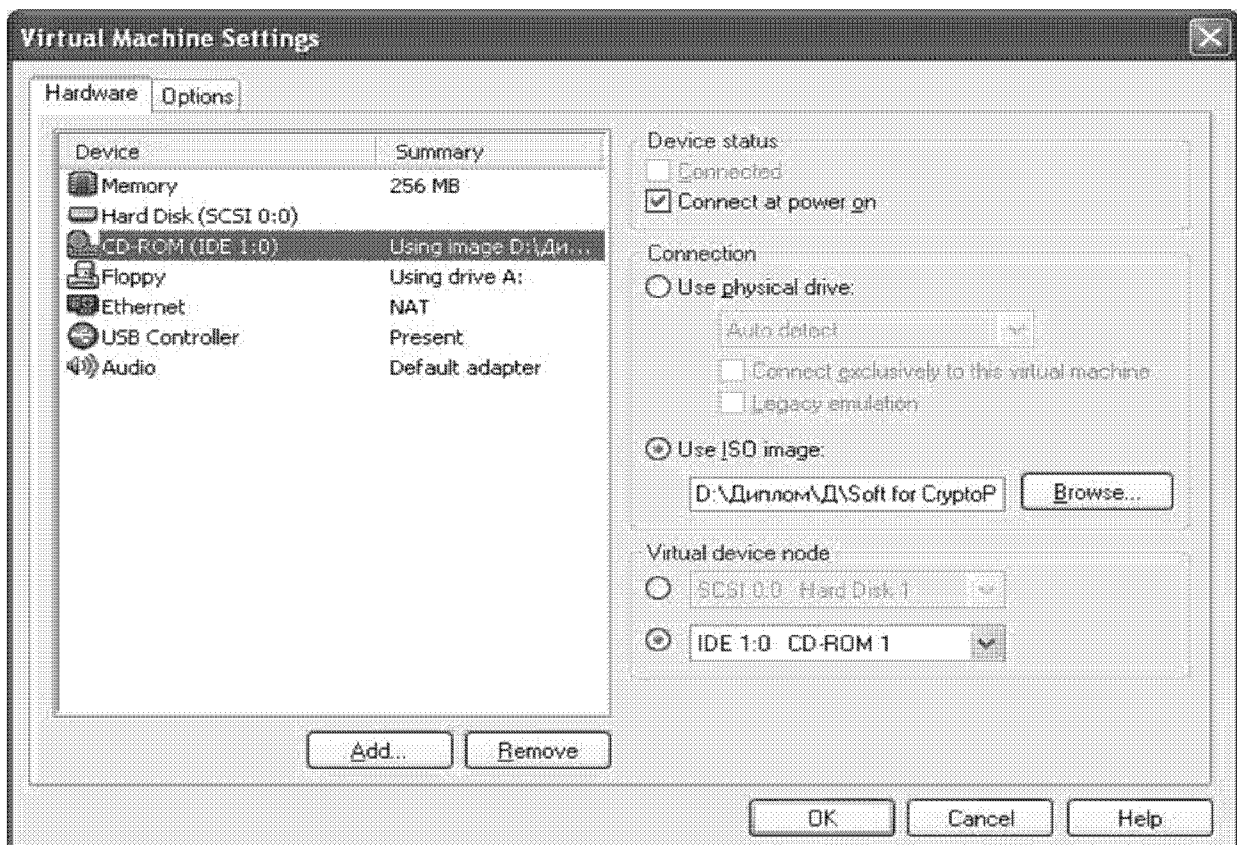
1. Установить на виртуальную машину Service Pack 4.
2. Установить на виртуальную машину службу очередей сообщений.
3. Установить на виртуальную машину «КРИПТОПРО CSP» и «КРИПТОПРО TLS»
4. Установить на виртуальную машину MSCA.
5. Изготовить первый сертификат.

Установка Service Pack 4

Для установки нужно запустить VMware Workstation.



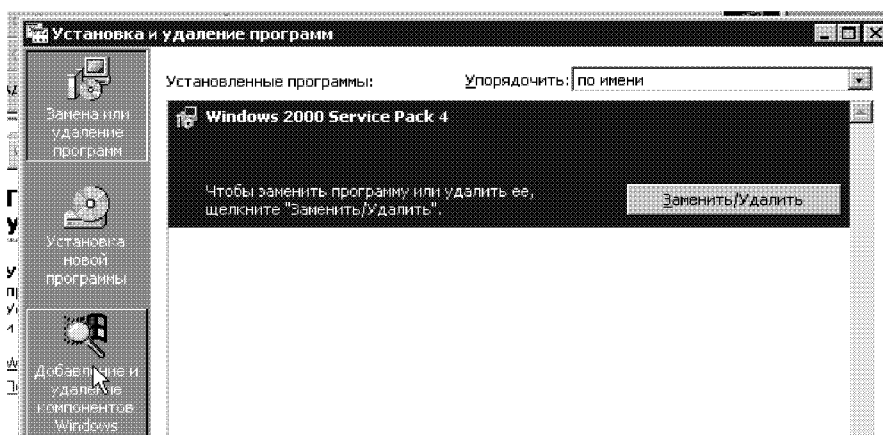
Потом с помощью правки настроек для дисковода указываем путь к Service Pack 4 расположенного на ISO образе “Soft for cryptoPro”.



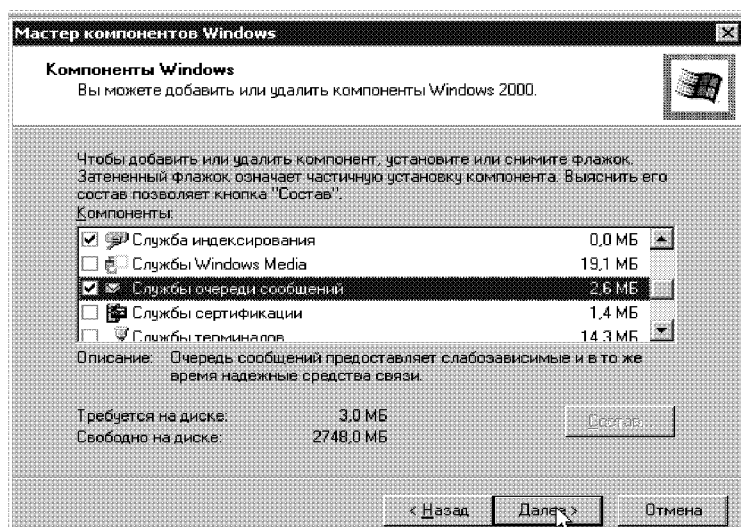
Затем запускаем Windows 2000 server и указываем путь кдистрибутиву, расположенного в директории «КриптоПро УЦ\SP4\» после чего запускаем его. Далее следуем советам установщика.

УСТАНОВКА СЛУЖБЫ ОЧЕРЕДЕЙ СООБЩЕНИЙ

Для установки службы очередей сообщений нажимаем «Пуск» «Настройка» «Панель управления», после появления окна «Панель управления» выбираем «Установка и удаление программ и компонентов Windows» далее «Добавление и удаление компонентов Windows».



В открывшемся окне находим службу очередей сообщений отмечаем ее и нажимаем далее.

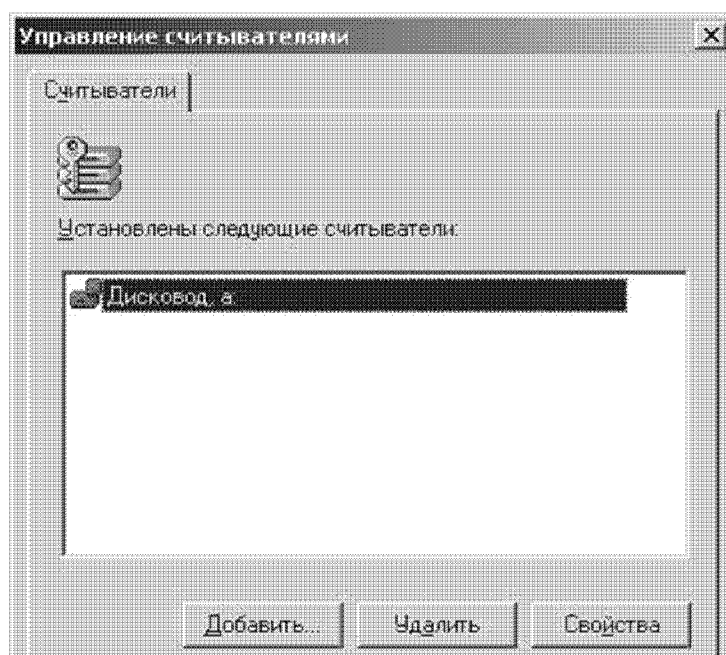
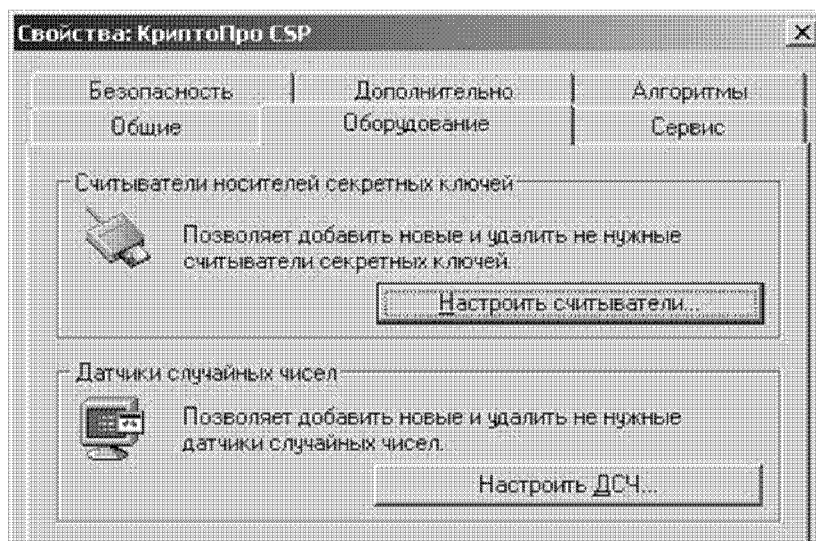


Служба очереди сообщений установлена.

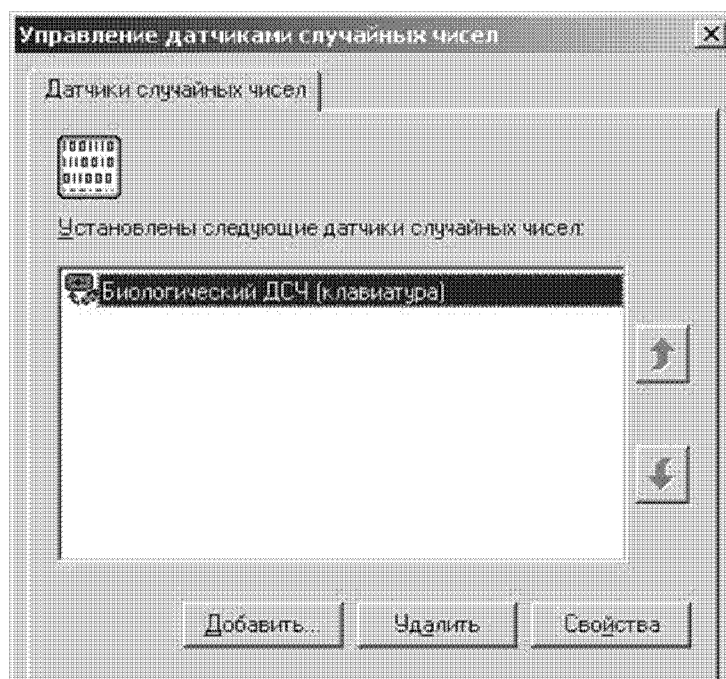
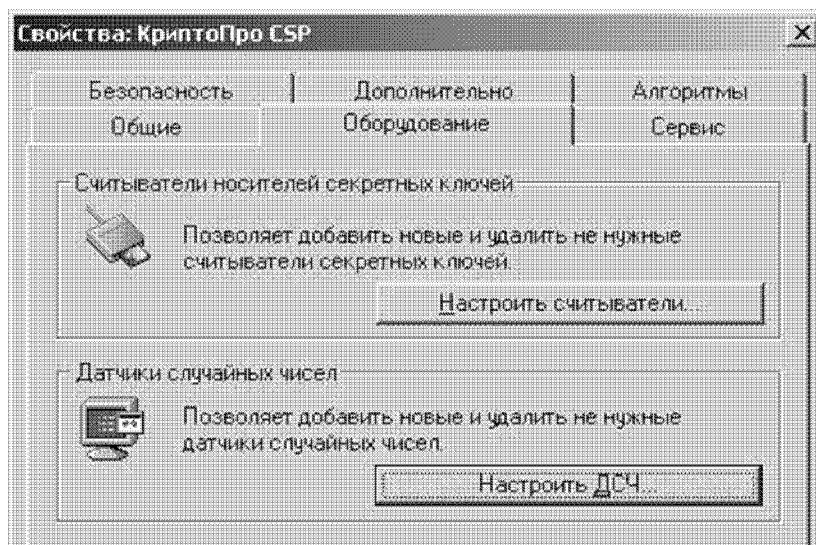
УСТАНОВКА И НАСТРОЙКА СКЗИ «КРИПТОПРО CSP» И СРЕДСТВА СЕТЕВОЙ АУТЕНТИФИКАЦИИ «КРИПТОПРО TLS»

Установка КристоПро CSP и КристоПро TLS осуществляется запуском файла «all_inst.bat» из папки «КристоПро CSP TLS» либо вручную из папки «КристоПро CSP TLS\SETUP\»

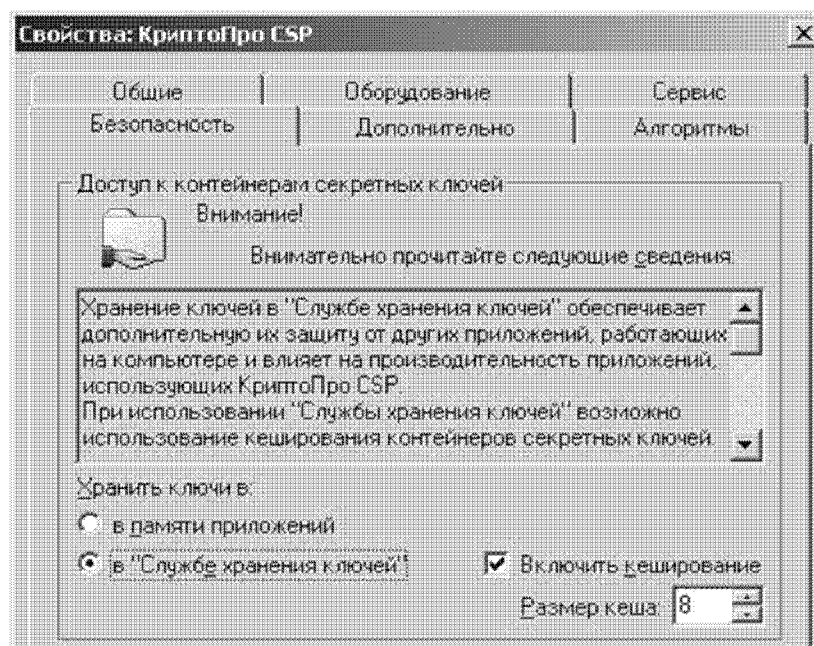
- поочередно установить КристоПро CSP и КристоПро TLS;
- ввести ключи активации для КристоПро CSP и КристоПро TLS;
- произвести перезагрузку компьютера;
- открыть панель управления компьютером, используя пункты меню «Пуск, Настройка, Панель управления» и в окне панели управления выбрать значок «КристоПро CSP».
- настроить КристоПро CSP на считыватель «Дисковод, а:»;



- настроить на КриптоПро CSP поддержку биологического датчика случайных чисел;

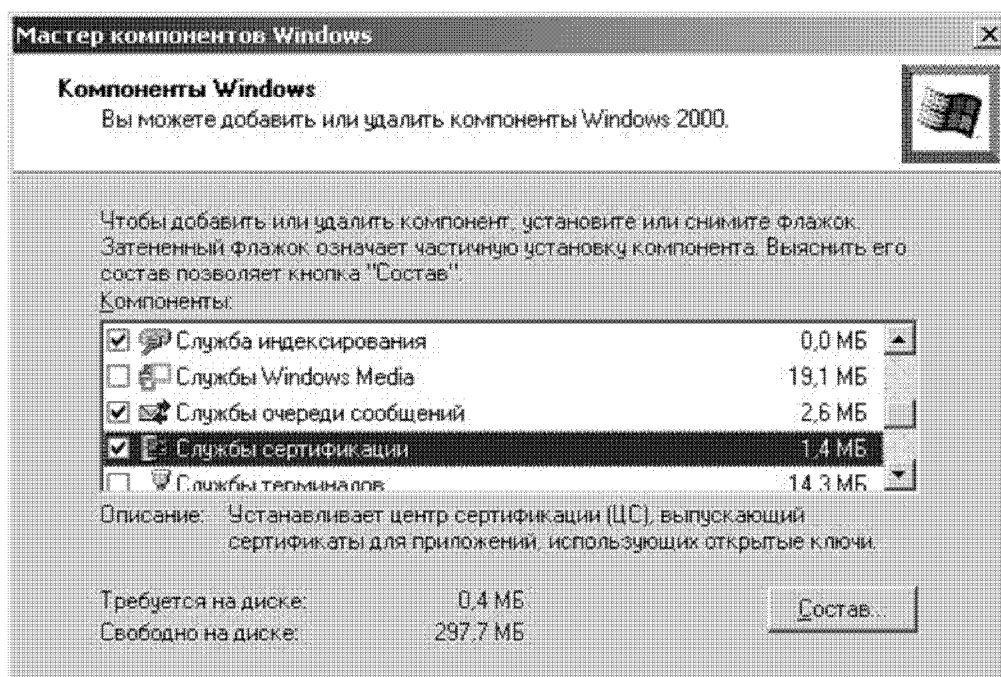


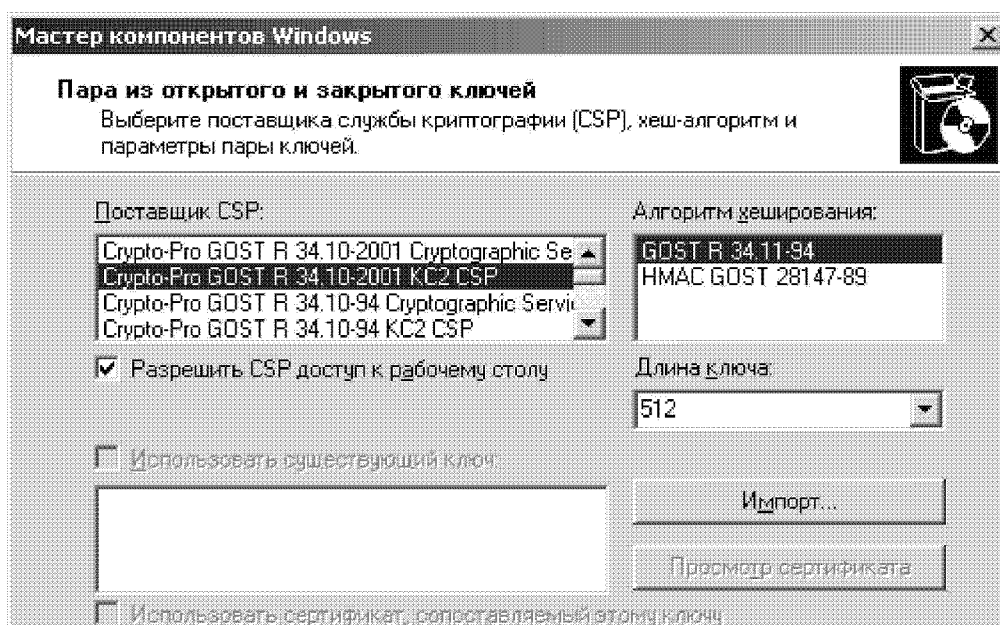
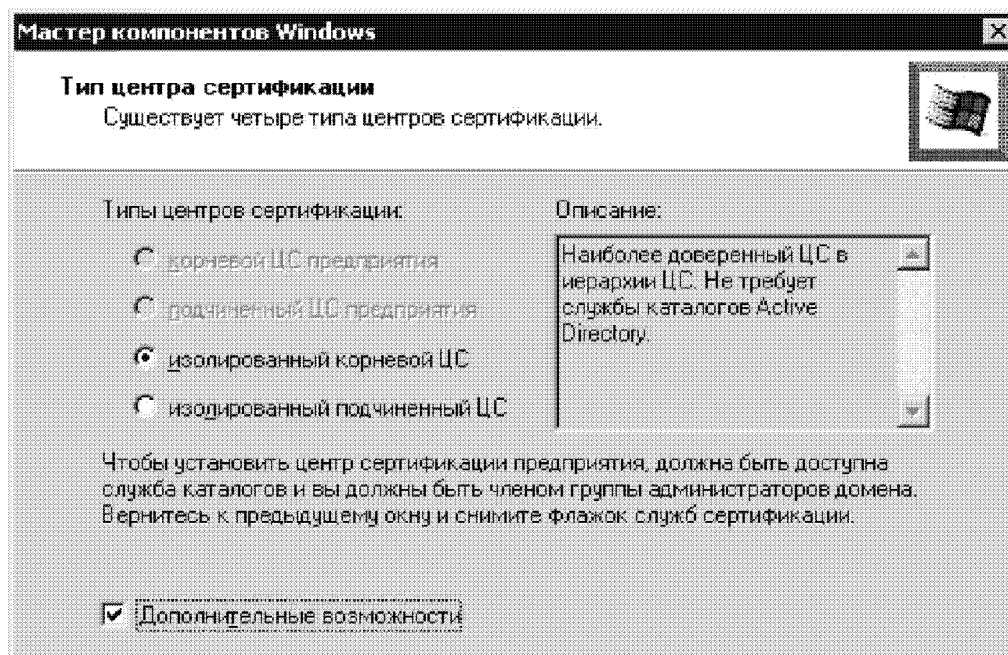
- настроить КриптоПро CSP на работу со службой хранения ключей и включить кэширование.



УСТАНОВКА СЛУЖБЫ СЕРТИФИКАЦИИ

Установка центра сертификации во многом схожа с установкой службы очереди сообщений:





Служба сертификации установлена.

ЛАБОРАТОРНАЯ РАБОТА №2

Тема лабораторной работы

Установка и настройка центра сертификации

Цель работы

Изучить процедуру установки и настройки программного обеспечения центра сертификации удостоверяющего центра «КриптоПро УЦ»

ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

Общие сведения

Программно-аппаратный комплекс «Удостоверяющий Центр «КриптоПро УЦ» является средством поддержки инфраструктуры открытых ключей и предназначен для регистрации пользователей, изготовления сертификатов их открытых ключей и управления данными сертификатами.

В состав комплекса «КриптоПро УЦ» входят следующие компоненты:

- средство криптографической защиты информации КриптоПро CSP;
- средство сетевой аутентификации КриптоПро TLS;
- центр сертификации;
- центр регистрации;
- АРМ администратора центра регистрации;
- АРМ пользователя.

В предыдущей лабораторной работе мы узнали что такое «КриптоПро CSP» и «КриптоПро TLS».

Центр сертификации

Центр сертификации – компонент «КриптоПро УЦ», предназначенный для формирования сертификатов открытых ключей пользователей, списков отозванных сертификатов, хранения эталонной базы сертификатов и списков отозванных сертификатов. Центр сертификации функционирует в операционной системе Microsoft Windows 2000 Server и использует базу данных SQL 2000 Server Desktop Edition.

Центр сертификации взаимодействует только с центром регистрации или несколькими Центрами Регистрации по отдельному сегменту локальной сети с использованием защищенного сетевого протокола.

К функциям ЦС относятся:

- генерация ключей и сертификата открытого ключа уполномоченного лица удостоверяющего центра;
- смена ключей и сертификата открытого ключа уполномоченного лица удостоверяющего центра;
- формирование сертификата открытого ключа по запросам центра регистрации;
- ведение базы данных сертификатов с предоставлением доступа к ней ограниченному кругу компонентов системы;
- изменение базы данных сертификатов по запросам от центра регистрации, включая выполнение следующих операций: аннулирование (отзыв) сертификата, приостановление действия сертификата, возобновление действия сертификата;
- формирование списка аннулированных (отозванных) сертификатов открытых ключей по запросам центра регистрации;
- формирование списка аннулированных (отозванных) сертификатов открытых ключей по запросам центра регистрации в автоматическом режиме с периодичностью, заданной в расписании;
- обеспечение уникальности следующей информации в сертификатах пользователей: открытый ключ сертификата, серийный номер сертификата;
- взаимодействие с центрами регистрации: их аутентификация и определение прав доступа с использованием ключей и сертификатов открытых ключей центров регистрации, прием от центров регистрации запросов, проверка наличия подписи данной информации на ключе центров регистрации, обработка полученных от центров регистрации запросов, передача на центры регистрации результатов обработки за-

просов, шифрование информации, передаваемой между ЦС и ЦР в ходе сетевого взаимодействия по протоколу TLS;

- протоколирование работы центра сертификации.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Каково назначение ПАК «Крипто Про УЦ»?
2. Основные компоненты ПАК «Крипто Про УЦ»?
3. Назначение и функции центра сертификации «Крипто Про УЦ»?
4. Какова последовательность установки центра сертификации?
5. Основное назначение сертификата Web – сервера центра сертификации?

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

1. Установить и настроить на виртуальной машине центр сертификации «Крипто Про УЦ».

Установка программного обеспечения центра сертификации «Крипто Про УЦ»

Установка программного обеспечения центра сертификации осуществляется с дистрибутива ЦС на установочном CD

1. Запустите приложение Setup, расположенное в корневой директории дистрибутива.
2. Установка осуществляется с использованием программы InstalShield Wizard для центра сертификации Крипто – Про УЦ. Вначале установки программа осуществит проверку установки необходимых компонентов общесистемного программного обеспечения. К ним относятся:
 - а. СКЗИ Крипто ПРО CSP
 - б. Служба MS IIS
 - в. Служба очередей сообщений

г. Служба сертификации MSCA

д. Инсталлированный сертификат серверной аутентификации Web-сервера

3. После выполнения проверок, в случае положительного результата, программа установки отобразит диалоговое окно продолжения установки. Для продолжения нажмите кнопку «Далее»

4. Следующим шагом необходимо ввести информацию о пользователе, производящем установку и серийный номер лицензии, предоставляющей право на эксплуатацию ЦС. После ввода данных нажмите кнопку «Далее»

5. После нажатия кнопки «Далее» программа установки отобразит диалоговое окно на котором необходимо выбрать вид установки. Программа установки определены два вида установки: полная и выборочная. Использование вида «выборочная» позволяет сместить каталог назначения, в который производится установка программного обеспечения ЦС. При использовании вида «полная» установка производится в определенный каталог.

6. После определения вида установки следующим отображается диалоговое окно в котором необходимо определить внешний адрес ЦС. По этому адресу ЦС должен быть доступен по протоколу HTTP(S). После ввода данных нажмите кнопку «Далее»

7. В следующем окне Мастера необходимо задать пароль учетной записи CPSCAComPlusAcct. Пароль задается при регистрации этой учетной записи. Если учетная запись уже зарегистрирована, то данное диалоговое окно не отображается, а отображается окно для ввода пароля зарегистрированной учетной записи

8. После определения всех необходимых параметров, выполненных на предыдущих шагах, программа установки выведет диалоговое окно подтверждения продолжения установки. При необходимости можно вернуться на переопределение параметров установки. Для этого надо нажать кнопку «Назад». Для подтверждения установки нажмите кнопку «Установить»

9. После нажатия кнопки «Установить», программа установки производит:

- а. копирование необходимых файлов в каталог назначения
 - б. регистрацию новых учетных записей
 - в. установку COM+приложений
 - г. добавление в web-сервере MS IIS виртуальной директории с именем СА
 - д. создание раздела с именем «Доверенные ЦР на ЦС Крипто-Про УЦ» в хранилище сертификатов локального компьютера
10. После завершения установки программного обеспечения ЦС программа установки выведет диалоговое окно с соответствующим сообщением. Для завершения установки нажмите кнопку «Готово»

Конфигурация программного обеспечения ЦС

Конфигурация программного обеспечения ЦС выполняется в случаях:

1. После установки программного обеспечения ЦС
2. При подключении Центра регистрации в процессе установки программного обеспечения «Удостоверяющий центр»
3. При подключении следующих Центров регистрации при изменении конфигурации или масштабирования в процессе эксплуатации УЦ
4. При изменении параметров политики ЦС по выпуску сертификатов открытых ключей в процессе эксплуатации УЦ
5. При изменении параметров публикации списков отозванных сертификатов (CRL)
6. При выполнении мероприятий по смене ключей аутентификации программного компонента Центра регистрации.

Конфигурация программного обеспечения ЦС заключается в настройке параметров работы следующих компонентов:

- Настройка разрешения безопасности службы сертификации ЦС
- Модуль выхода Крипто-Про УЦ службы сертификации ЦС
- Модуль политики Крипто-Про УЦ службы сертификации ЦС
- Модуль взаимодействия с центром сертификации

ЛАБОРАТОРНАЯ РАБОТА № 3

Тема лабораторной работы

Установка и настройка центра регистрации

Цель работы

Изучить процедуру установки и настройки программного обеспечения центра регистрации удостоверяющего центра «КриптоПро УЦ»

ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

Центр регистрации «Крипто Про УЦ»

Центр Регистрации – компонент «КриптоПро УЦ», предназначенный для хранения регистрационных данных пользователей, запросов на сертификаты и сертификаты пользователей, предоставления интерфейса взаимодействия пользователей с удостоверяющим центром. Центр Регистрации функционирует в операционной системе (ОС) Microsoft Windows 2000 Server и использует базу данных Microsoft SQL 2000 Server (Desktop Edition, Standard Edition или Enterprise Edition).

Центр Регистрации взаимодействует с центром сертификации по отдельному сегменту локальной сети с использованием защищенного сетевого протокола. Взаимодействие пользователей с удостоверяющим центром обеспечивается за счет использования приложений (АРМ зарегистрированного пользователя с ключевым доступом, АРМ зарегистрированного пользователя с маркерным доступом, АРМ регистрации пользователя), предоставляемых центром регистрации.

Центр регистрации является единственной точкой входа (регистрации) пользователей в системе. Только зарегистрированный в центре регистрации пользователь может получить сертификат на свой открытый ключ в удостоверяющем центре.

К функциям центра регистрации относятся:

- обеспечение аутентификации приложений и пользователей при обращении к центру регистрации;
- ведение базы данных (реестра), содержащей информацию о пользователях и пользовательских сертификатах: данные о пользователях, включающиеся в сертификаты открытых ключей, данные о пользователях, не включающиеся в сертификаты открытых ключей, ключевая фраза пользователя, необходимая для его идентификации администратором, открытые ключи пользователей, зарегистрированных в системе, сертификаты пользователей, зарегистрированных в системе;
- управление шаблонами сертификатов, обеспечивающих определение области применения ключей и сертификатов открытых ключей пользователей;
- обеспечение уникальности информации в сертификатах открытых ключей пользователей;
- взаимодействие с ЦС и внешними приложениями;
- управление режимами работы удостоверяющего центра по регистрации и управлению ключами и сертификатами;
- обеспечение доступа к базе данных внешним приложениям через SOAP-интерфейс на базе HTTP(S);
- обеспечение выполнения центром регистрации в автоматическом режиме следующих задач: оповещение пользователей по электронной почте об истечении срока действия сертификатов, оповещение пользователей по электронной почте о необходимости замены ключей, оповещение администратора о возникновении критических ситуаций, получение списка отозванных сертификатов от соответствующего центра сертификации, получение списка отозванных сертификатов от центров регистрации вышестоящих по иерархии удостоверяющих центров, удаление зарегистрированных пользователей, не имеющих ни одного действующего сертификата открытого ключа;
- протоколирование работы центра регистрации.

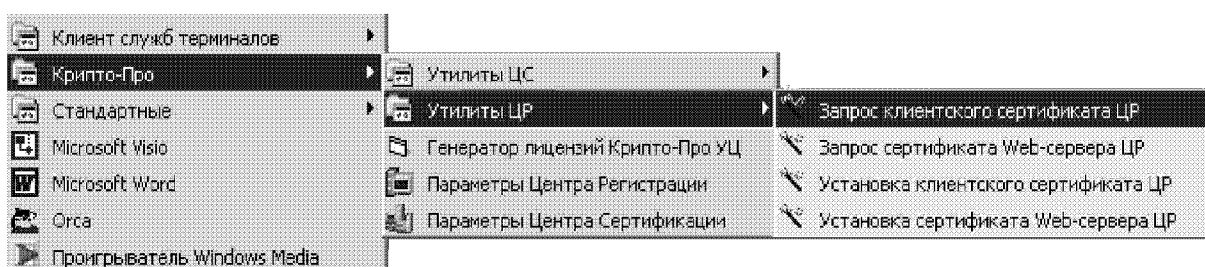
КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Назначение и функции центра регистрации «Крипто Про УЦ»?
2. Какова последовательность установки центра регистрации?
3. Основные параметры конфигурирования центра регистрации?

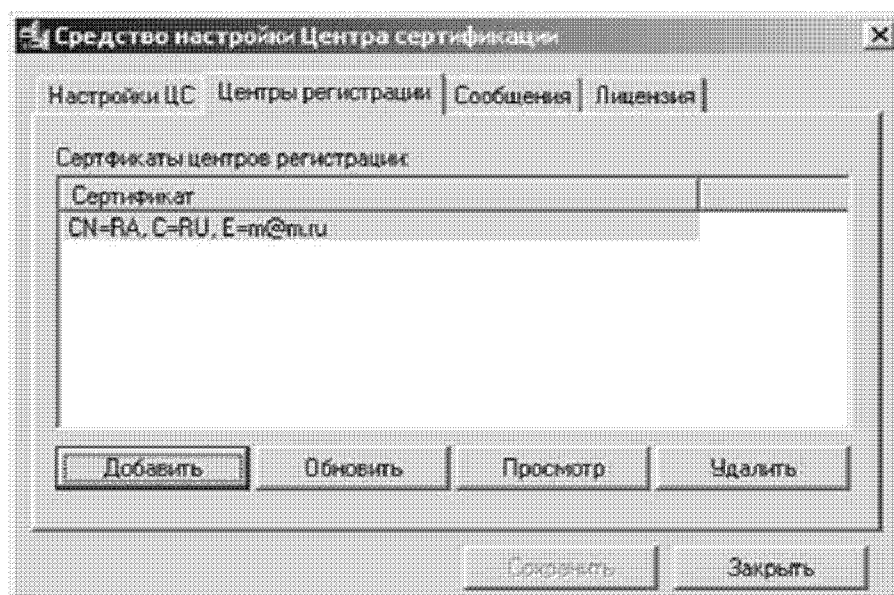
ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

Установить и настроить на виртуальной машине центр регистрации «Крипто Про УЦ».

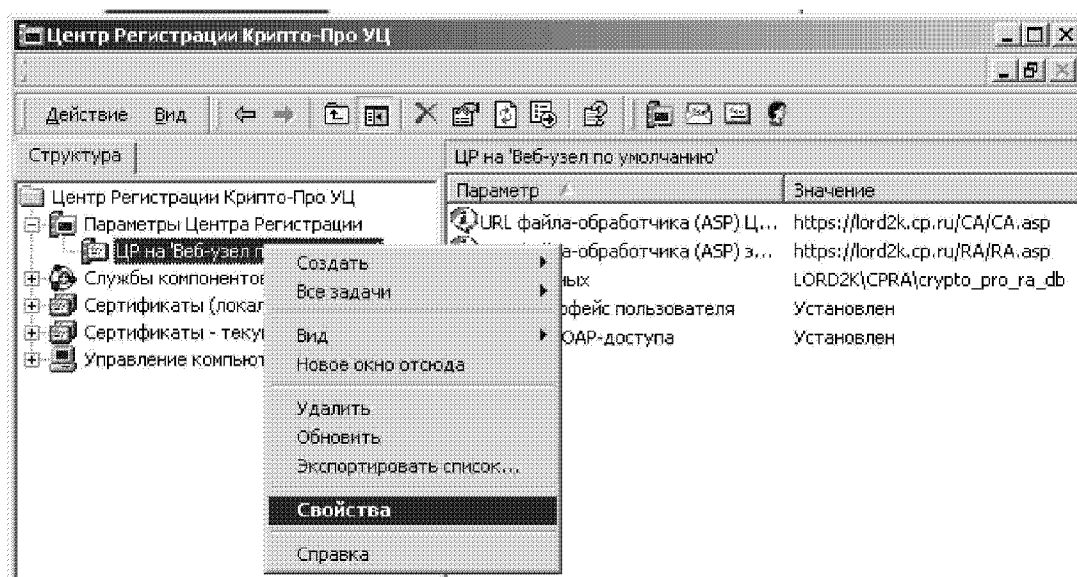
- установить приложения мастеров центра регистрации из дистрибутива, расположенного в директории «КриптоПро УЦ\RATools\»;
- сформировать запрос на выпуск сертификата центра регистрации, используя утилиту «Запрос клиентского сертификата центра регистрации», расположенную в меню «Пуск, Программы, КриптоПро, Утилиты центра регистрации»;

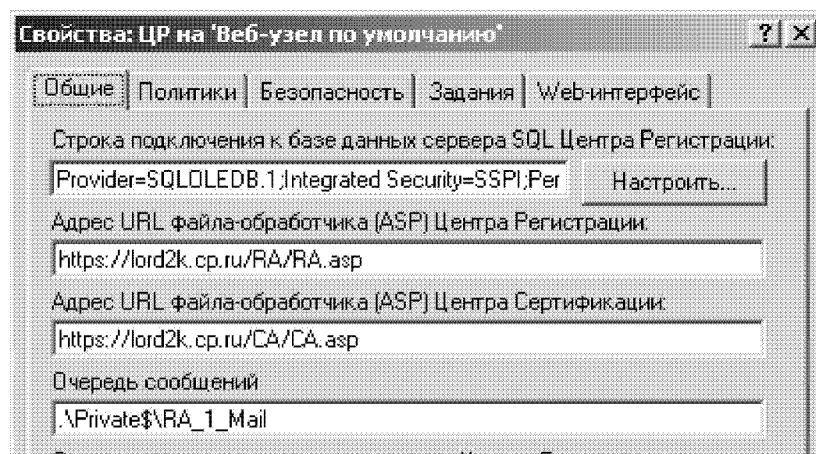


- используя контекстное меню службы сертификации, обработать запрос клиентского сертификата центра регистрации;
- установить сертификат центра регистрации, используя утилиту «Установка клиентского сертификата центра регистрации», расположенную в меню «Пуск, Программы, КриптоПро, Утилиты центра регистрации»;
- в меню «Пуск, Программы, КриптоПро, Параметры центра сертификации» в разделе «Центры регистрации» добавить установленный сертификат центра регистрации в список доверенных центров регистрации на центре сертификации;

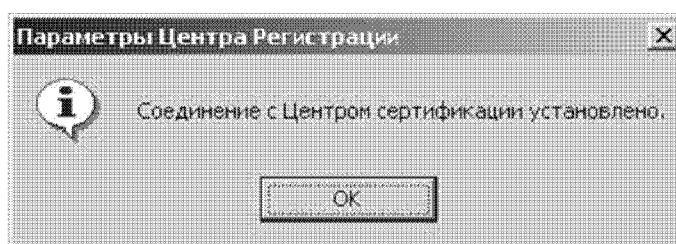
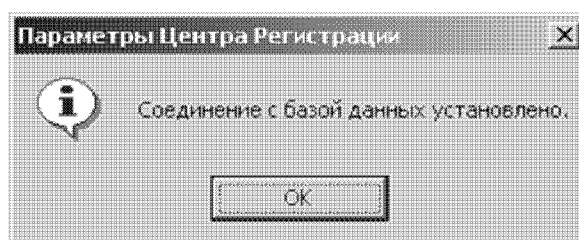


- установить программное обеспечение центра регистрации, расположенное в папке «КриптоПро УЦ\РА\»;
- произвести перезагрузку компьютера;
- сконфигурировать программное обеспечение центра регистрации в части взаимодействия с центром сертификации: для этого в меню «Пуск, Программы, КриптоПро, Параметры центра регистрации» выбрать «Свойства центра регистрации на Веб-узле по умолчанию», изменив в разделе «Адрес URL файла-обработчика ЦС» параметр «localhost» на доменное имя ЦС и выбрав соответствующий сертификат подписи и аутентификации центра регистрации;

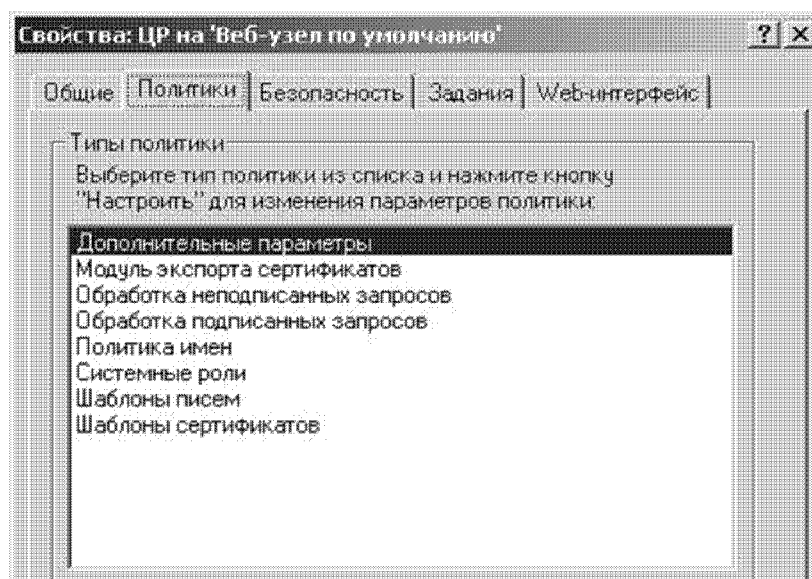




- протестировать соединение с базой данных SQL 2000 Server и центром сертификации;



- изучить политики центра регистрации.



ЛАБОРАТОРНАЯ РАБОТА № 4

Тема лабораторной работы

Установка и настройка АРМа администратора центра регистрации. Создание привилегированных пользователей (администратора и оператора). Подключение к центру регистрации, используя роли администратора и оператора.

Цель работы

Изучить процедуру установки и настройки программного обеспечения АРМа администратора центра регистрации «КриптоПро УЦ»

ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

АРМ администратор центра регистрации «Крипто Про УЦ»

АРМ администратора центра регистрации предназначен для выполнения организационно-технических мероприятий, связанных с регистрацией пользователей, формированием служебных ключей и сертификатов пользователей и управлением центром регистрации.

АРМ администратора функционирует в ОС Microsoft Windows 2000 Professional или Windows 2000 Server. АРМ администратора взаимодействует с центром регистрации по локальной сети с использованием защищенного сетевого протокола.

Программное обеспечение АРМа администратора используется для всех ролей привилегированных пользователей (администраторов, операторов и т.д.).

К основным функциям АРМ администратора относятся:

- обеспечение взаимодействия с одним или несколькими центрами регистрации;
- обеспечение возможности выбора администратором сертификата, с помощью которого будет осуществляться взаимодействие с центром регистрации;
- шифрование информации, передаваемой центру регистрации с использованием протокола TLS с двусторонней аутентификацией;
- регистрация пользователей в центре регистрации;

- удаление зарегистрированных пользователей из центра регистрации, не имеющих ни одного действующего сертификата;
- генерация служебных и рабочих ключей пользователей;
- организация просмотра информации из базы данных центра регистрации, относящейся к пользователю, зарегистрированному в системе;
- создание запросов на формирование сертификатов;
- обеспечение возможности получения пользователем нескольких сертификатов;
- вывод сертификата открытого ключа пользователя на бумажный носитель;
- создание запросов на отзыв сертификатов;
- создание запросов на приостановление действия сертификатов;
- создание запросов на возобновление действия сертификатов;
- проверка состояния и обработка запросов на формирование сертификатов, поступающих от пользователей;
- проверка состояния и обработка запросов на отзыв, приостановление и возобновление действия сертификатов, поступающих от пользователей;
- просмотр протокола работы центра регистрации;
- публикация списков отозванных сертификатов открытых ключей пользователей;
- вывод сертификата открытого ключа центра сертификации (уполномоченного лица удостоверяющего центра) на бумажный носитель;
- сохранение списка отозванных сертификатов в виде файла;
- сохранение сертификата (цепочки сертификатов) центра сертификации в виде файла.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Назначение и функции АРМ администратора ЦР «Крипто Про УЦ»?
2. Назначение и функции АРМ пользователя «Крипто Про УЦ»?
3. Состав и назначение ролей пользователей в «Крипто Про УЦ»?

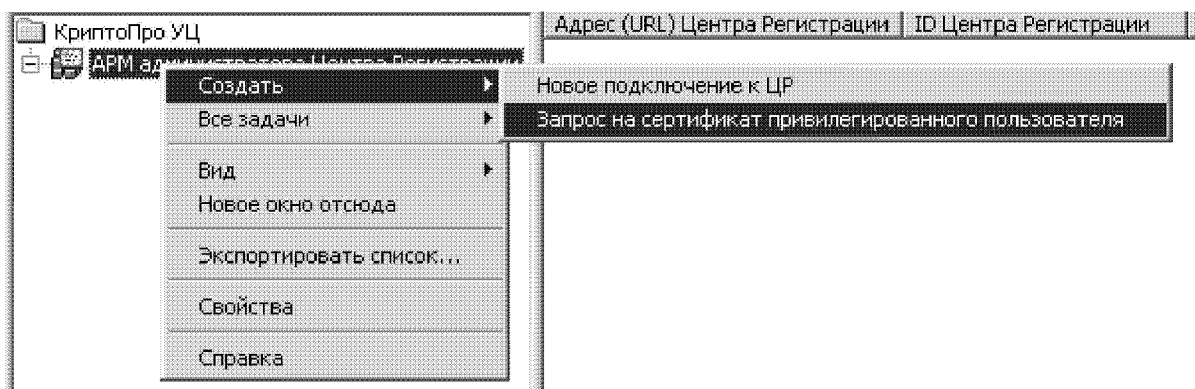
4. Какова последовательность установки АРМ администратора ЦР?
5. Основные параметры конфигурирования АРМ администратора ЦР?

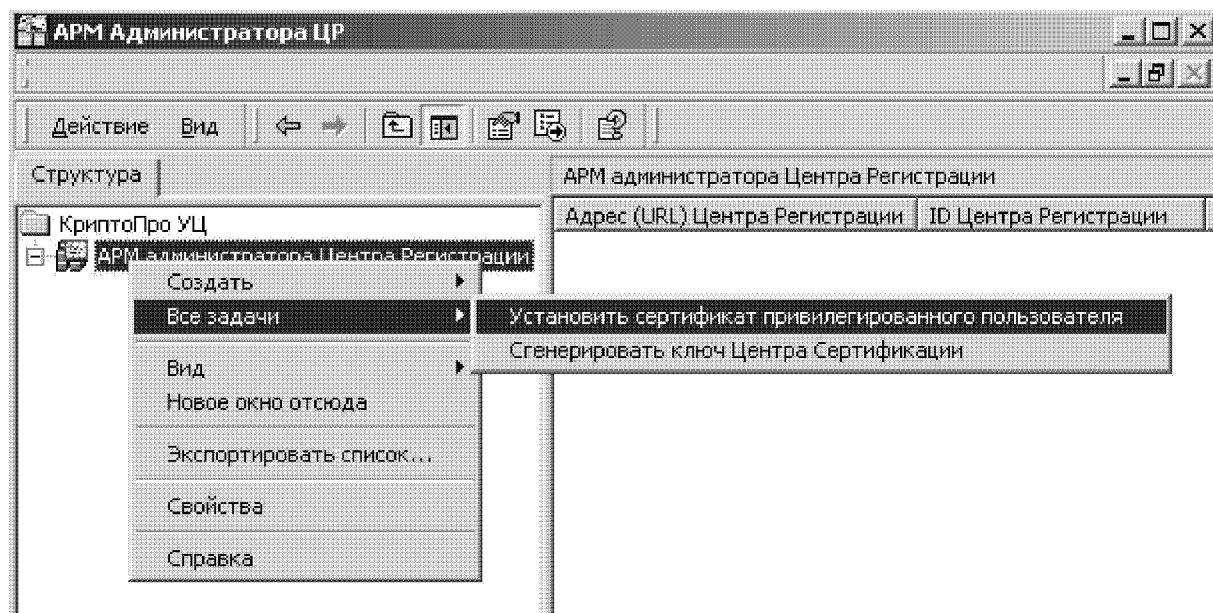
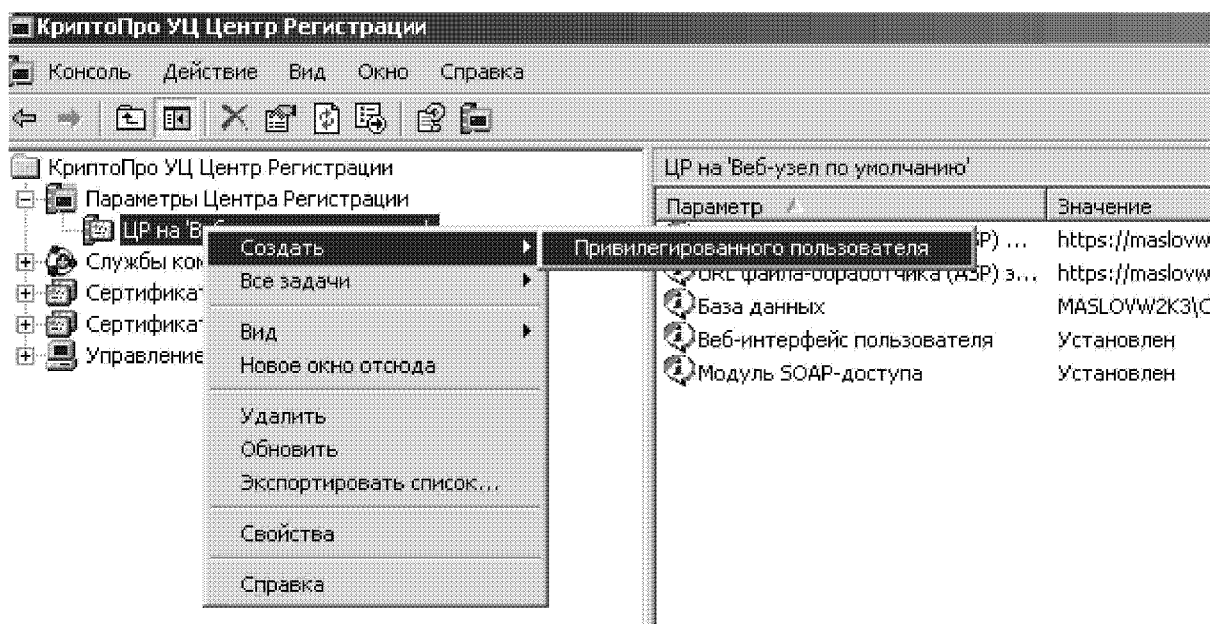
ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

1. Установить и настроить на виртуальной машине центр регистрации «Крипто Про УЦ».
2. Создать привилегированных пользователей (администратора и оператора).
3. Подключиться к центру регистрации, используя роли администратора и оператора.

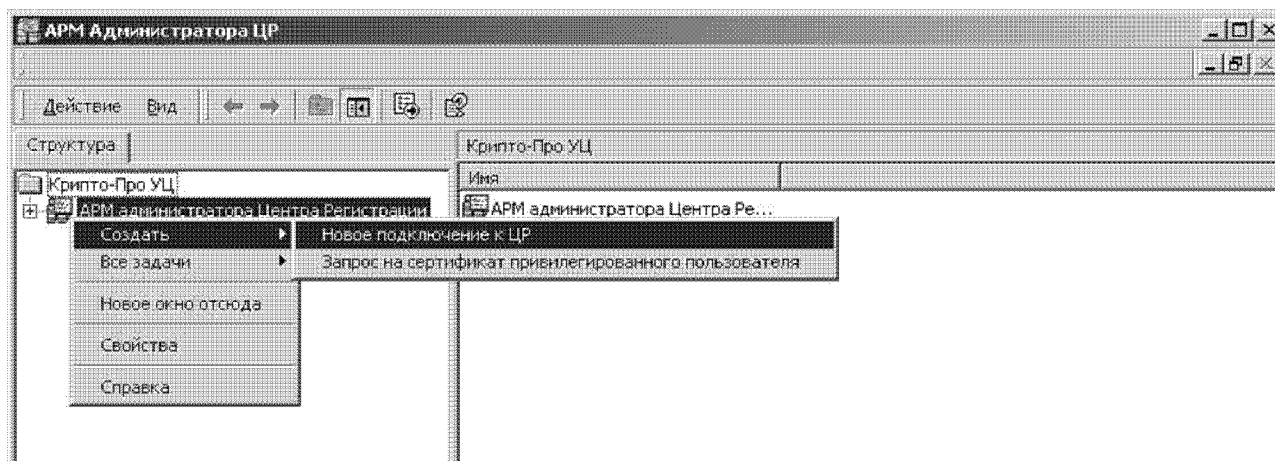
Установка и настройка АРМ администратора центра регистрации «КриптоПро УЦ»

- установить программное обеспечение АРМ администратора, расположенное в папке «КриптоПро УЦ\CRAdmin2\»;
- зарегистрировать привилегированного пользователя с ролью «администратор»: создать запрос на сертификат администратора ЦР (данное действие производится на рабочем месте администратора ЦР в разделе «Создать -> Запрос на сертификат привилегированного пользователя»), выпустить сертификат администратора ЦР (действие производится на центре регистрации в разделе «Создать -> Привилегированного пользователя»), установить сертификат администратора ЦР (действие производится на рабочем месте администратора ЦР в разделе «Все задачи -> Установить сертификат привилегированного пользователя»);





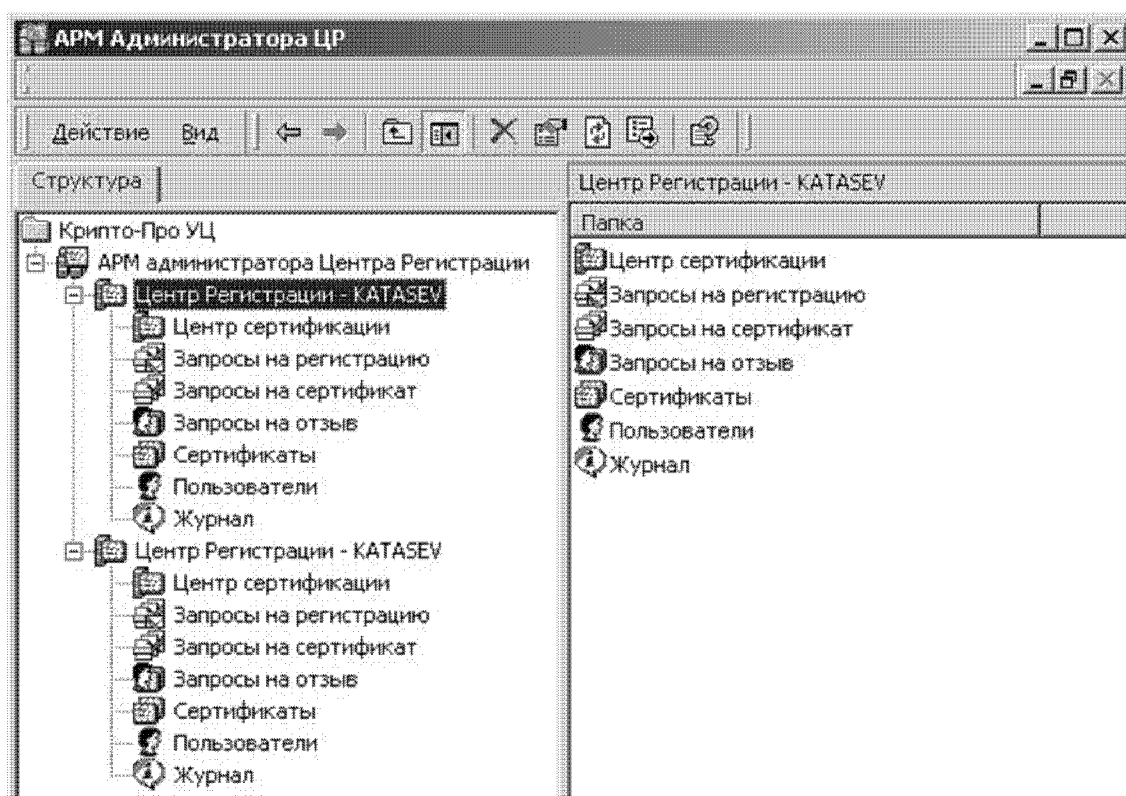
- зарегистрировать привилегированного пользователя с ролью «оператор» (порядок выполнения действий аналогичен регистрации привилегированного пользователя с ролью «администратор», но при создании запрос на сертификат привилегированного пользователя выбирается роль «Оператор»);
- создать подключение к центру регистрации, используя сертификат с ролью «оператор» (действие производится на рабочем месте администратора ЦР в разделе «Создать -> Новое подключение к ЦР», в параметре «Адрес URL файла описания WSDL центра регистрации вместо localhost указывается имя центра регистрации»);



Адрес URL файла описания WSDL Центра Регистрации:

<https://localhost/ra/ra.wsdl>

- создать подключение к центру регистрации, используя сертификат с ролью «администратор»;
- активизировать подключение к центру регистрации, используя сертификат с ролью «администратор», а затем с ролью «оператор».



ЛАБОРАТОРНАЯ РАБОТА № 5

Тема лабораторной работы

Регистрация пользователей в централизованном режиме, изготовление и управление сертификатами.

Цель работы

Изучение возможностей и получение навыков регистрации пользователей в централизованном режиме, изготовления и управления сертификатами.

ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

Общие сведения

Программно-аппаратный комплекс «КриптоПро УЦ» обеспечивает:

- выполнение процедуры регистрации пользователя;
- формирование запросов на изготовление сертификатов открытых ключей;
- формирование запросов на отзыв сертификатов открытых ключей;
- формирование запросов на приостановление/возобновление действия сертификатов открытых ключей;
- формирование и доставку зарегистрированным пользователям списка отозванных сертификатов открытых ключей.

Данные процедуры могут выполняться как в централизованном, так и в распределенном режимах. В первом случае пользователь лично посещает удостоверяющий центр и инициирует выполнение той или иной процедуры. Во втором случае пользователь подключается в Web-серверу центра регистрации и удаленно инициирует выполнение необходимых процедур.

Регистрацию пользователей, изготовление и управление сертификатами осуществляют привилегированные пользователи АРМ администратора центра регистрации с ролями «администратор» и «оператор».

Администратор – лицо, осуществляющее управление объектами управления центра регистрации. Привилегированный пользователь с ролью «администратор» обеспечивает выполнение следующих задач:

- идентификация и регистрация пользователей;
- генерация ключей, получение и предоставление изготовленных сертификатов открытых ключей пользователей;
- получение от пользователей системы запросов на выпуск сертификата в электронном виде с подтверждением на бумажном бланке;
- верификация запросов на выпуск сертификата;
- отзыв сертификатов открытых ключей пользователей системы;
- публикация списка отозванных сертификатов;
- получение и обработка сообщений о компрометации ключей пользователями.

Оператор – лицо, осуществляющее выполнение следующих функций:

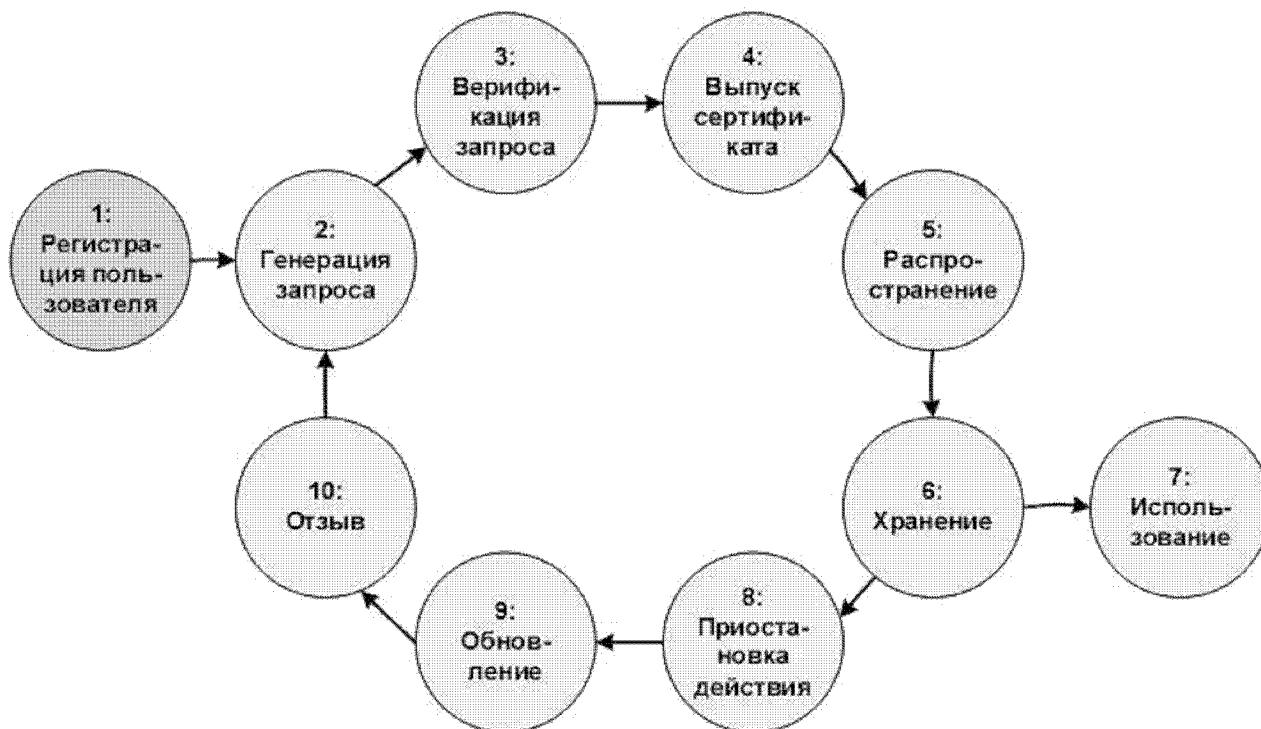
- регистрация пользователей в базе данных центра регистрации;
- генерация служебных ключей и сертификатов открытых ключей при выполнении процедуры регистрации пользователей в централизованном режиме;
- обработка запросов на регистрацию пользователей.

Таким образом, удостоверяющий центр «КриптоПро УЦ» осуществляет поддержку всего жизненного цикла сертификата открытого ключа:

- формирование запроса на выпуск сертификата открытого ключа;
- верификация запроса;
- выпуск сертификата в соответствии с данными, указанными в запросе и действующей политикой сертификации;
- распространение сертификата среди участников информационной системы;
- хранение и выдача сертификата по запросу пользователей и владельцев сертификатов;

- приостановление и возобновление действия сертификата;
- обновление информации, содержащейся в сертификате;
- отзыв сертификата по запросу владельца сертификата.

Жизненный цикл сертификата



Автоматизированное рабочее место пользователя

Маркер временного доступа

Маркер временного доступа представляет собой совокупность следующей информации:

- идентификатор маркера временного доступа;
- пароль маркера временного доступа.

Идентификатор маркера временного доступа представляет собой натуральное число. Пароль маркера временного доступа представляет собой символьную последовательность длиной в 6 символов, состоящую из букв латинского алфавита, цифр и специальных символов. Идентификатор маркера временного доступа и пароль маркера временного доступа находятся между собой во взаимно-однозначном соответствии.

Маркер временного доступа формируется центром регистрации либо по запросу из АРМ регистрации пользователя (веб-приложения), либо по запросу из АРМ администратора центра регистрации.

Маркер временного доступа имеет ограниченное по времени действие. Он становится неактивным после подтверждения получения сертификата открытого ключа, поступающего от пользователя на Центр Регистрации в момент установки сертификата на рабочем месте пользователя. Срок действия маркера определяется в настройках дополнительных параметров на вкладке «Политики» окна свойств приложения «Параметры Центра Регистрации».

Маркер временного доступа предназначен для аутентификации пользователя удостоверяющего центра в процессе его взаимодействия с центром регистрации посредством использования веб-приложения АРМ зарегистрированного пользователя с маркерным доступом.

Маркер временного доступа используется в следующих случаях:

- при регистрации пользователя в распределенном режиме с использованием АРМ регистрации пользователя;
- для предоставления возможности зарегистрированному пользователю, не имеющему ни одного действующего секретного ключа и сертификата открытого ключа, выполнить на своем рабочем месте следующие задачи:
 - сформировать ключи;
 - сформировать запрос на сертификат открытого ключа и поставить его в очередь центра регистрации на обработку;
 - сформировать бланк запроса на сертификат открытого ключа для печати его на бумажном носителе;
 - получить и установить выпущенный сертификат открытого ключа.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие функции поддерживает программно-аппаротный комплекс «Крипто Про УЦ» при управлении жизненным циклом сертификата?
2. Перечислите и охарактеризуйте основные этапы жизненного цикла сертификата открытого ключа?
3. Понятие и назначение маркера временного доступа?
4. Срок действия маркера временного доступа? От чего зависит данный параметр?
5. В чем заключается основное отличие маркерного доступа к центру регистрации от ключевого доступа?

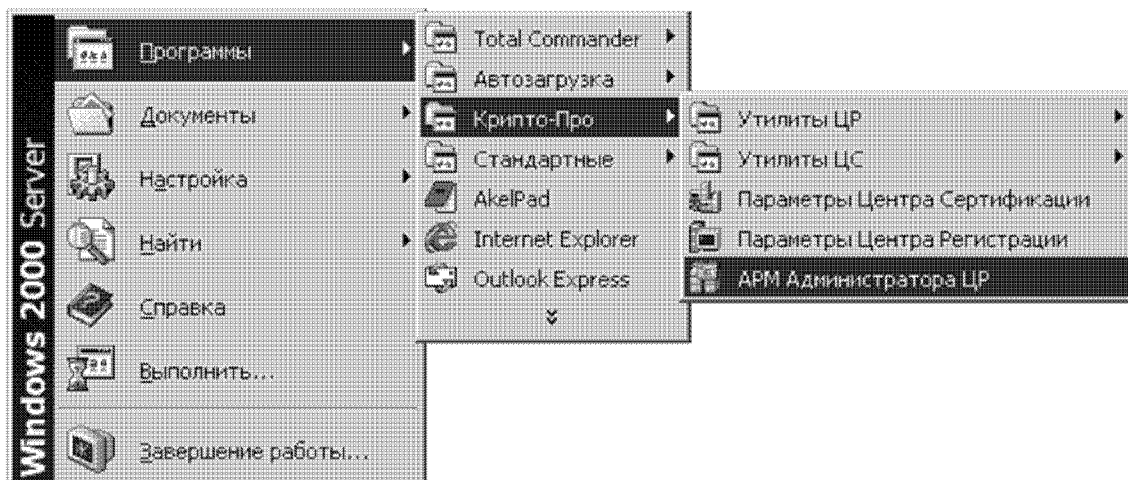
ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

1. Провести регистрацию пользователей в централизованном режиме
2. Отработать процесс изготовления и управления сертификатами

Регистрация пользователей, изготовление и управление сертификатами в централизованном режиме

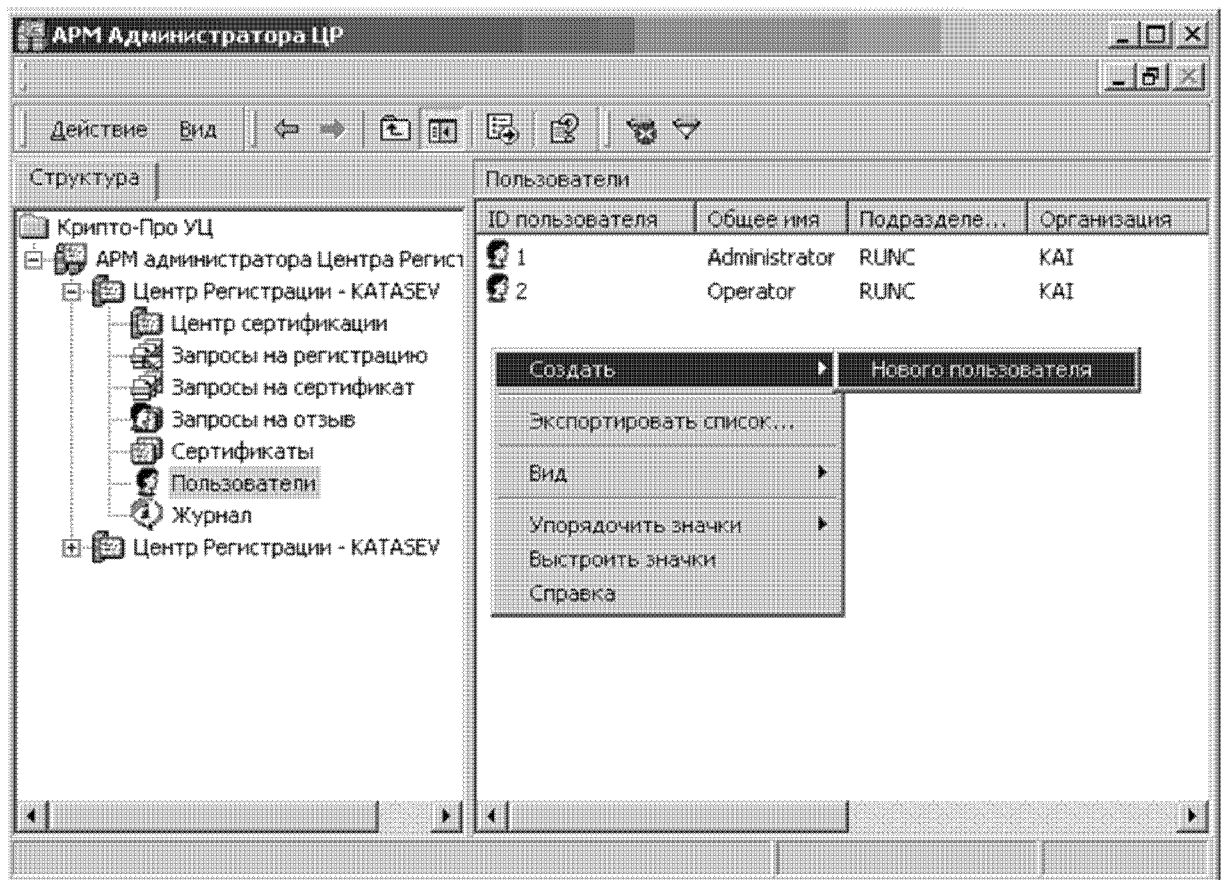
В централизованном режиме управление пользователями и их сертификатами осуществляется на АРМ администратора центра регистрации.

- запустить АРМ администратора центра регистрации;



- активизировать подключение к центру регистрации, используя сертификат с ролью оператора;

- зарегистрировать пользователя с генерацией ключей в системный реестр и шаблоном сертификатов «Временный сертификат пользователя УЦ»;



Мастер регистрации пользователя

Источник запроса на сертификат
Выберите способ получения запроса на сертификат

Выберите источник запроса на сертификат и нажмите кнопку "Далее".

☒ Генерация нового запроса на сертификат
Выберите этот параметр, если желаете сгенерировать пару ключей и создать запрос на сертификат для нового открытого ключа.

☐ Чтение запроса на сертификат из файла
Выберите этот параметр, если желаете взять существующий запрос на сертификат из файла, предоставленного пользователем.

Для продолжения нажмите кнопку "Далее".

< Назад Далее > Отмена

Мастер регистрации пользователя

Ввод информации о сертификате пользователя
 Укажите параметры запроса на сертификат пользователя.

Выберите тип запроса на сертификат пользователя. Будьте внимательны: тип запроса определяет права пользователя в системе.

Тип запроса на сертификат:
 Временный сертификат пользователя УЦ

Для продолжения нажмите кнопку "Далее".

< Назад Далее > Отмена

- активизировать подключение к центру регистрации, используя сертификат с ролью администратора;
- создать два новых сертификата для зарегистрированного пользователя с генерацией ключей в системный реестр и шаблоном сертификатов «Сертификат пользователя УЦ»;

АРМ Администратора ЦР

Действие Вид

Структура Пользователи

Крипто-Про УЦ

- АРМ администратора Центра Регистрации - KATASEV
 - Центр Регистрации - KATASEV
 - Центр сертификации
 - Запросы на регистрацию
 - Запросы на сертификат
 - Запросы на отзыв
 - Сертификаты
 - Пользователи
 - Журнал
 - Центр Регистрации - KATASEV
 - Центр сертификации
 - Запросы на регистрацию
 - Запросы на сертификат
 - Запросы на отзыв
 - Сертификаты
 - Пользователи
 - Журнал

| ID пользователя | Общие имя | Подразделе... | Организация |
|-----------------|---------------|---------------|-------------|
| 1 | Administrator | RUNC | KAI |
| 2 | Operator | RUNC | KAI |
| 3 | User | | |

Все задачи Показать

Новый сертификат Создать

Макер временного доступа к УЦ Удалить

Справка

Мастер создания сертификата пользователя

Ввод информации о сертификате пользователя
Укажите параметры запроса на сертификат пользователя.

Выберите тип запроса на сертификат пользователя. Будьте внимательны: тип запроса определяет права пользователя в системе.

Тип запроса на сертификат:
Сертификат пользователя УЦ

Для продолжения нажмите кнопку "Далее".

< Назад Далее > Отмена

- отозвать последний изданный сертификат пользователя;

АРМ Администратора ЦР

Действительно хотите отозвать выделенные сертификаты?

Да Нет

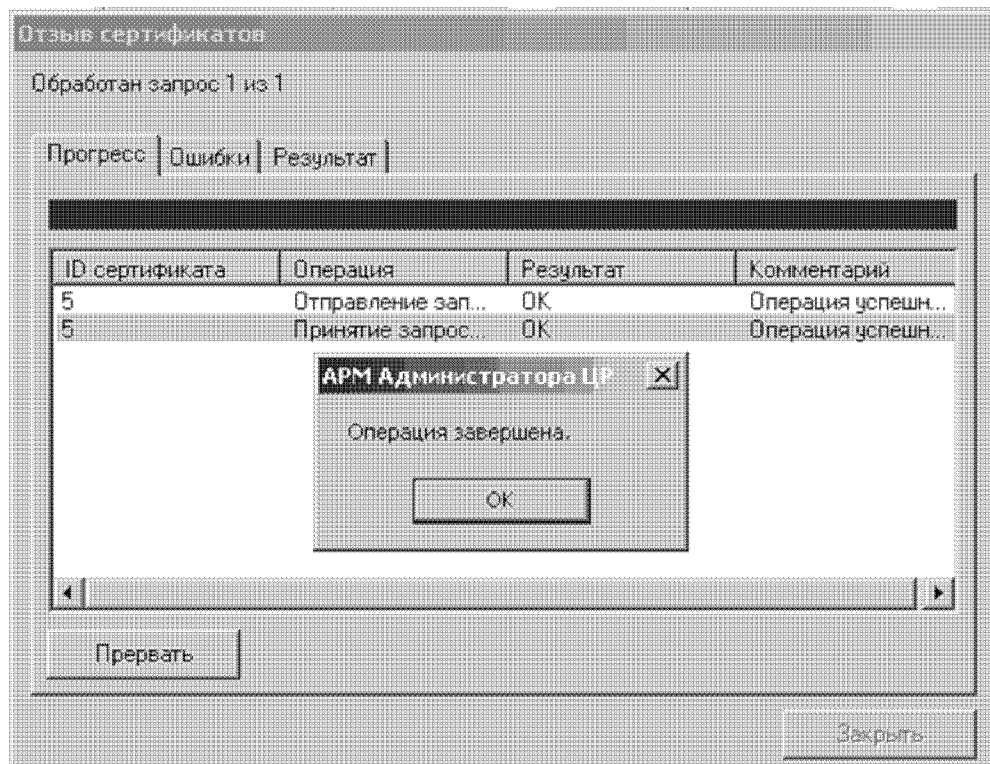
Отзыв сертификата

Серийный номер: 61236871000000000008

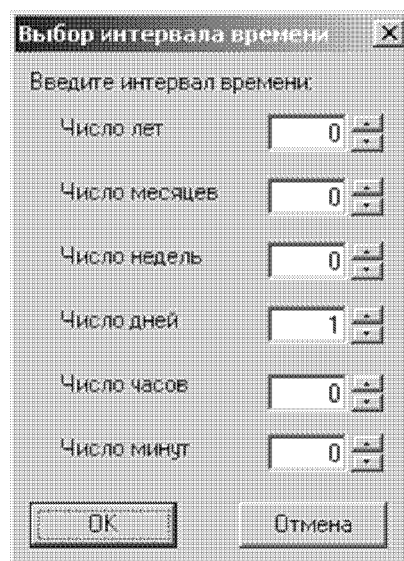
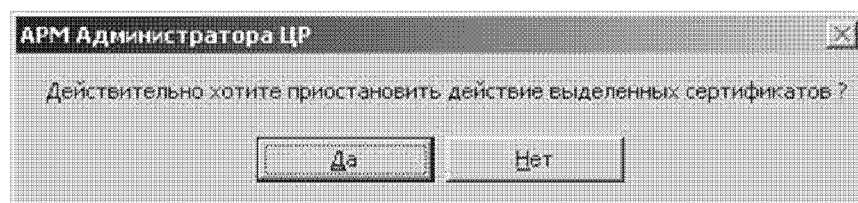
Причина отзыва:
Компрометация ключа

☐ Использовать для всех

Отозвать Отмена



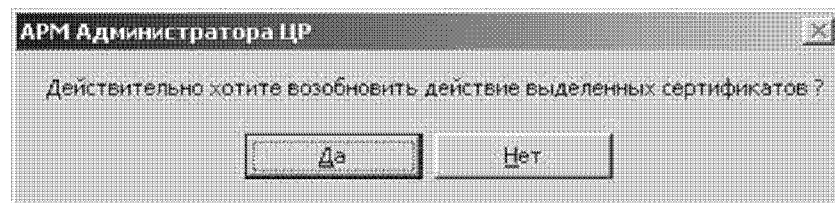
- открыть текущий CRL;
 - приостановить на 1 день первый сертификат пользова-
- теля;



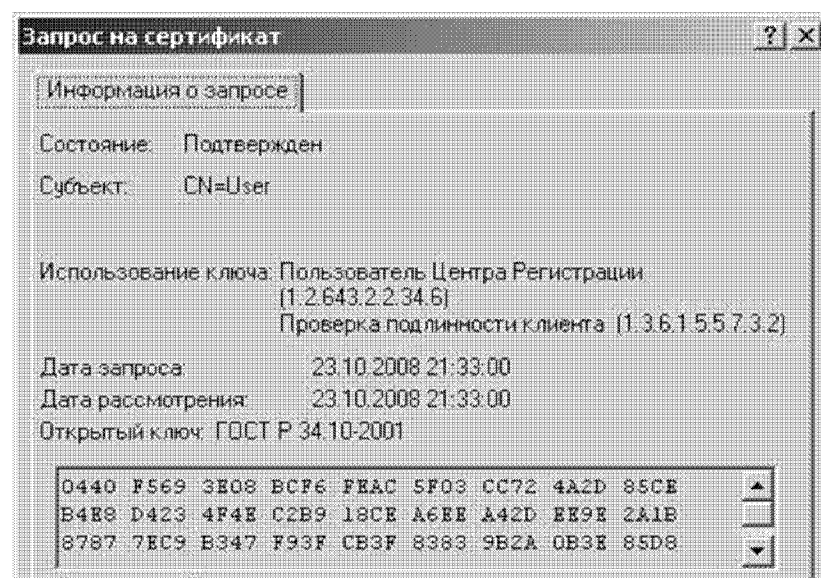
- открыть текущий CRL и выполнить задачу публикации CRL;



- открыть текущий CRL и возобновить первый сертификат пользователя;

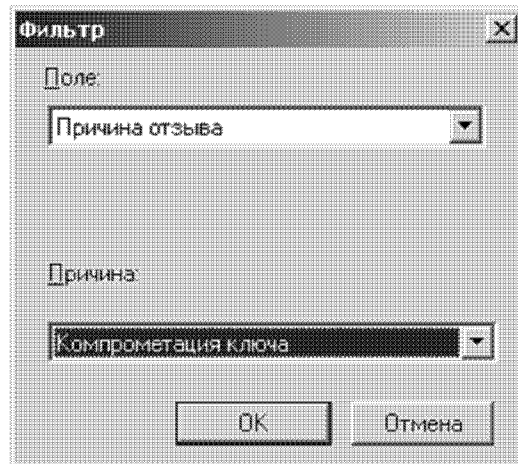


- открыть текущий CRL;
- выполнить задачу публикации CRL;
- открыть окно запросов на регистрацию пользователя;
- открыть окно запросов на сертификат пользователя;
- открыть окно свойств запроса на первый сертификат пользователя и изучить свойства запроса;

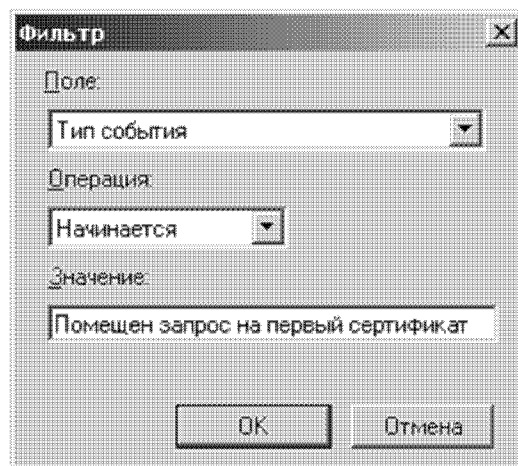


- открыть окно свойств запроса на второй сертификат пользователя и изучить свойства запроса;

- отфильтровать список запросов на отзыв по причине отзыва «Компрометация ключа»;



- открыть окно свойств запроса на приостановление сертификата пользователя;
- открыть окно свойств запроса на возобновление сертификата пользователя;
- открыть список журнала АРМ администратора;
- отфильтровать журнал по типу события «Помещен запрос на первый сертификат».



ЛАБОРАТОРНАЯ РАБОТА № 6

Тема лабораторной работы

Регистрация пользователей в распределенном режиме, изготовление и управление сертификатами.

Цель работы

Изучение возможностей и получение навыков регистрации пользователей в распределенном режиме, изготовления и управления сертификатами.

ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

Регистрация пользователя в распределенном режиме

Распределенный режим регистрации пользователя является опциональным режимом и используется при невозможности регистрации пользователей в централизованном режиме.

Идентификация пользователя осуществляется нотариусом путем совершения нотариальных действий при заверении заявления на регистрацию пользователя, на основании документов, удостоверяющих личность пользователя.

С помощью ПО АРМ регистрации пользователя регистрируемые пользователи формируют запрос на регистрацию в электронной форме. Регистрация пользователя в распределенном режиме осуществляется администратором удостоверяющего центра на основании нотариально заверенного заявления на регистрацию и запроса на регистрацию в электронной форме путем принятия запроса на регистрацию в электронной форме.

С помощью ПО АРМ зарегистрированного пользователя с маркерным доступом, зарегистрированные пользователи на своем рабочем месте генерируют служебные закрытый и открытый ключи, формируют и отправляют в центр регистрации запрос на служебный сертификат.

Зарегистрированный пользователь должен распечатать запрос на сертификат в бумажной форме, заверить его своей собственноручной подписью и отправить в Удостоверяющий Центр.

Администратор с использованием ПО АРМ администратора Центра Регистрации, на основании поступившего запроса на сертификат в электронной форме и запроса на сертификат в бумажной форме принимает запрос на сертификат для изготовления его.

С помощью ПО АРМ зарегистрированного пользователя с маркерным доступом, зарегистрированные пользователи на своем рабочем месте получают выпущенный служебный сертификат.

АРМ зарегистрированного пользователя с маркерным доступом

АРМ зарегистрированного пользователя с маркерным доступом представляет собой веб-приложение, размещаемое на Центре Регистрации в виртуальном каталоге `UI\register`. Доступ к приложению с рабочего места пользователя осуществляется с использованием MS Internet Explorer по протоколу HTTP(S) с односторонней аутентификацией. Аутентификация пользователя выполняется по маркеру временного доступа. Для работы с АРМ зарегистрированного пользователя с маркерным доступом отведена роль «Прошедший проверку».

АРМ зарегистрированного пользователя с маркерным доступом предназначен для выполнения организационно-технических мероприятий, связанных с генерацией первых ключей, формированием запроса на первый сертификат открытого ключа и получение первого сертификата открытого ключа. Также он предназначен для выполнения этих мероприятий при получении новых сертификатов в распределенном режиме (т.е. со своего рабочего места).

АРМ зарегистрированного пользователя с маркерным доступом, как правило, используется в двух случаях:

- в процедуре регистрации пользователя в распределенном режиме, после использования АРМ регистрации;
- в случае потери ключа аутентификации (при компрометации или в иных случаях) зарегистрированного пользователя и не имеющего возможности личного прибытия в удостоверяющий центр для получения ключей и сертификатов.

К основным функциям АРМ зарегистрированного пользователя с маркерным доступом относятся:

- обеспечение взаимодействия с центром регистрации;
- обеспечение аутентификации пользователя по паролю;
- шифрование информации, передаваемой между пользователем и центром регистрации, с использованием протокола TLS с односторонней аутентификацией;
- генерация ключей пользователя;
- создание запроса на формирование сертификата пользователя;
- печать запроса на формирование сертификата пользователя;
- обеспечение возможности получения пользователем выпущенного сертификата.

АРМ зарегистрированного пользователя с ключевым доступом

АРМ зарегистрированного пользователя с ключевым доступом представляет собой веб-приложение, размещаемое на центре регистрации в виртуальном каталоге U\user. Доступ к приложению с рабочего места пользователя осуществляется с использованием MS Internet Explorer по протоколу HTTP(S) с двухсторонней аутентификацией. Аутентификация пользователя выполняется по ключам и сертификату открытого ключа. Роль пользователя определяется в соответствии с ролью, занесенной в сертификат открытого ключа. По умолчанию (предустановленна) для работы с АРМ зарегистрированного пользователя с ключевым доступом роль «Пользователь Центра Регистрации».

АРМ зарегистрированного пользователя с ключевым доступом предназначен для выполнения организационно-технических мероприятий, связанных с управлением личной ключевой информацией и сертификатами, такими как формирование рабочих ключей и сертификатов, отзыв сертификатов, установка списка отозванных сертификатов.

К основным функциям АРМ зарегистрированного пользователя с ключевым доступом относятся:

- обеспечение взаимодействия с центром регистрации;
- обеспечение возможности выбора пользователем сертификата, с помощью которого будет осуществляться взаимодействие с ЦР;
- шифрование информации передаваемой в ЦР с использованием протокола TLS с двусторонней аутентификацией;
- генерация ключей пользователя;
- создание запросов на формирование сертификатов;
- печать запроса на формирование сертификата пользователя;
- обеспечение возможности получения пользователем выпущенных сертификатов;
- вывод электронного сертификата открытого ключа пользователя на бумажный носитель;
- проверка состояния запросов на формирование сертификатов;
- создание запросов на отзыв сертификата открытого ключа;
- получение сертификатов открытых ключей других пользователей.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Отличие и особенности централизованного и распределенного режимов регистрации пользователей?
2. Регламентные процедуры, выполняемые на АРМ администратора при регистрации пользователя в централизованном и распределенном режимах, а также при выдаче и управлении сертификатами?
3. В каких случаях пользователь должен отозвать свой сертификат и приостановить его действие?
4. Перечислите ситуации, когда у пользователя возникает необходимость в аннулировании сертификата своего открытого ключа?
5. Перечислите причины, по которым сертификат может быть признан недействительным?
6. Понятие и назначение списка отозванных сертификатов?

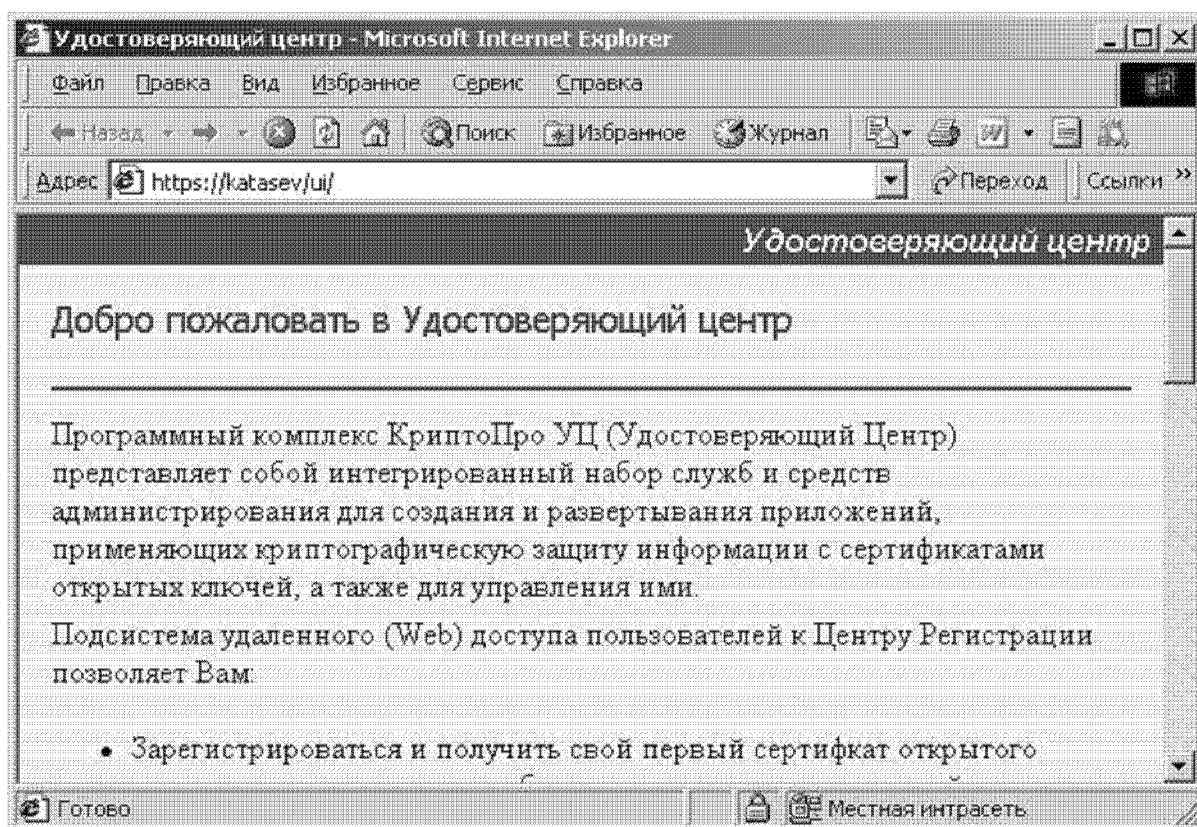
ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

1. Провести регистрацию пользователей в распределенном режиме
2. Отработать процесс изготовления и управления сертификатами в распределенном режиме

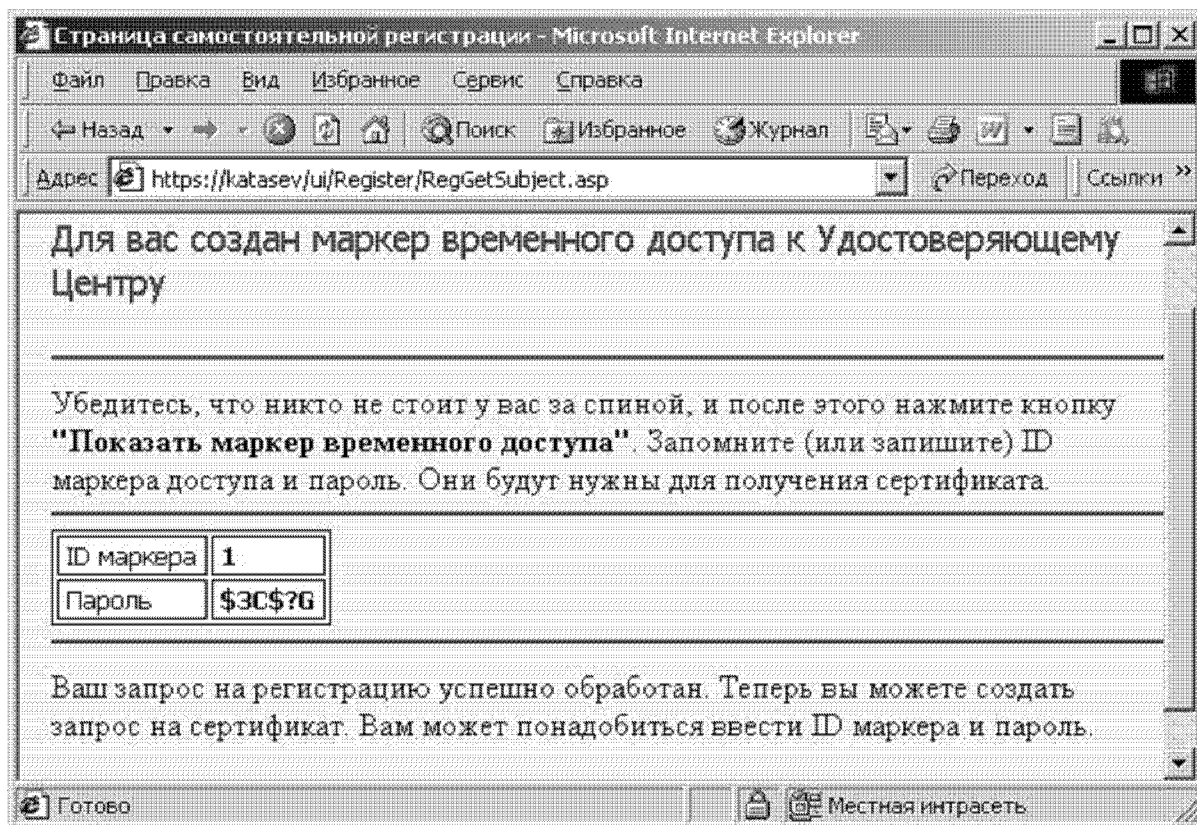
Регистрация пользователей, изготовление и управление сертификатами в распределенном режиме с автоматическим принятием запросов

В распределенном режиме управление пользователями и их сертификатами осуществляется удаленно с использованием web-интерфейса ЦР. Запросы на регистрацию пользователя, выпуск и управление сертификатами принимаются автоматически.

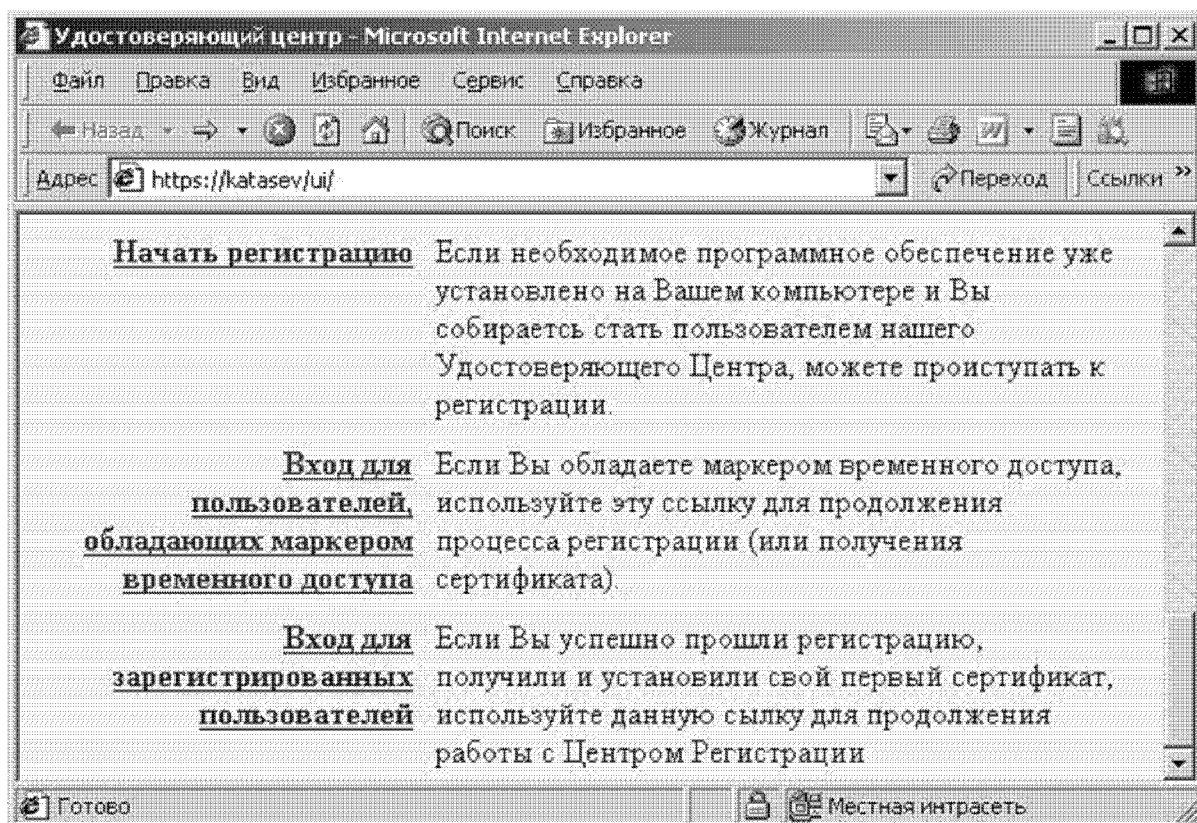
- открыть страницу по умолчанию web-интерфейса центра регистрации;

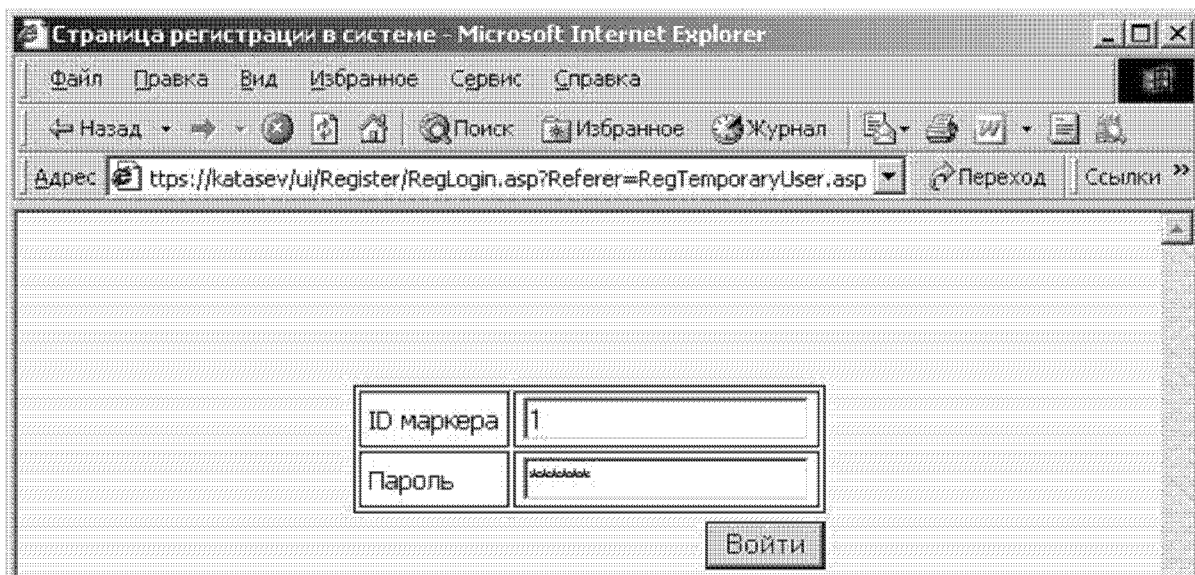


- сформировать запрос на регистрацию и поставить в очередь (запомнить маркер временного доступа);

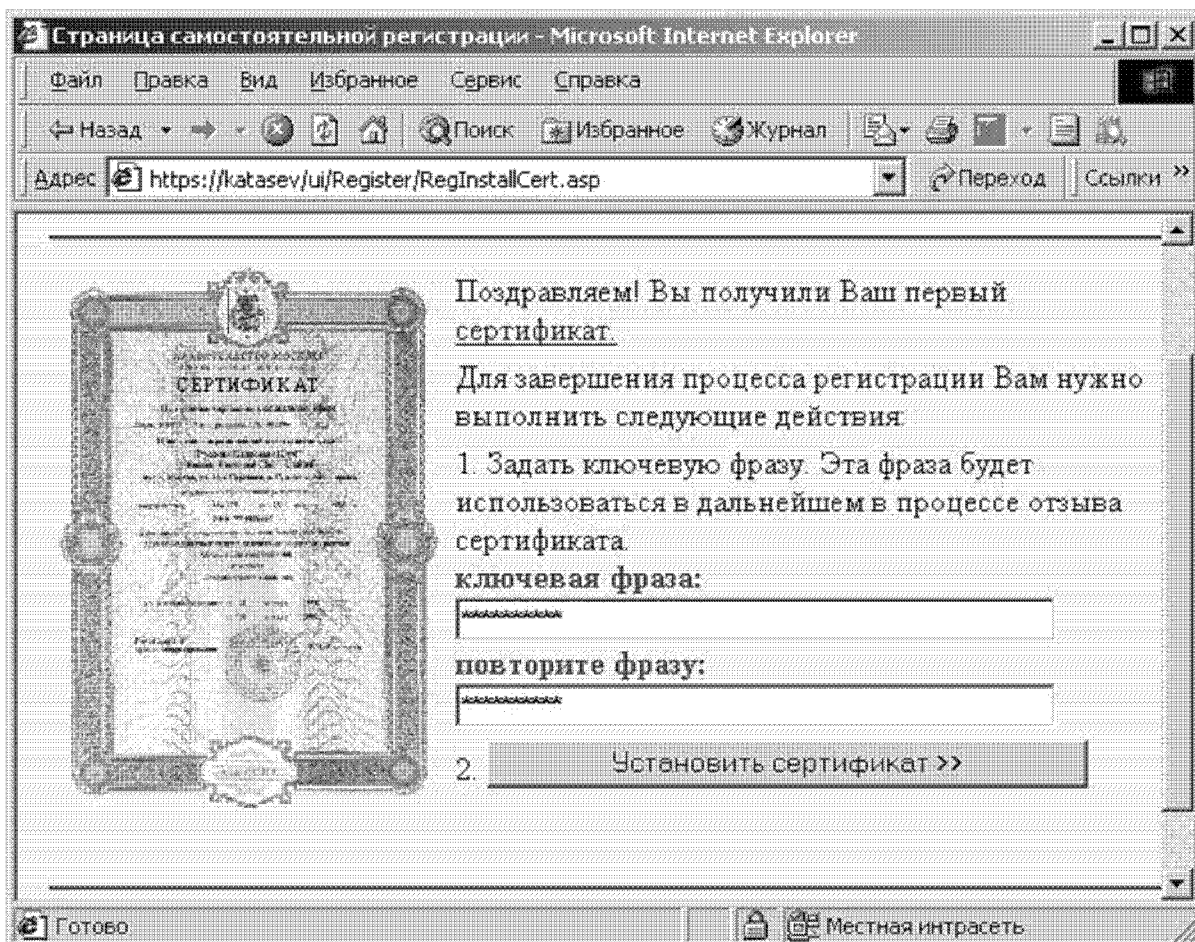


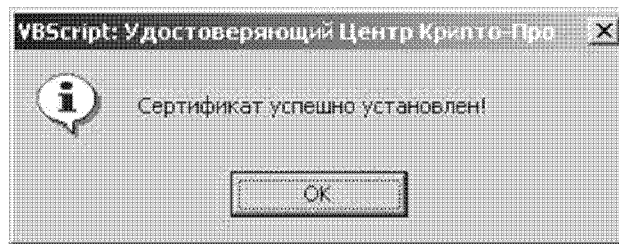
- закрыть страницу по умолчанию web-интерфейса ЦР;
- открыть страницу по умолчанию web-интерфейса ЦР;
- перейти на АРМ зарегистрированного пользователя с маркерным доступом;



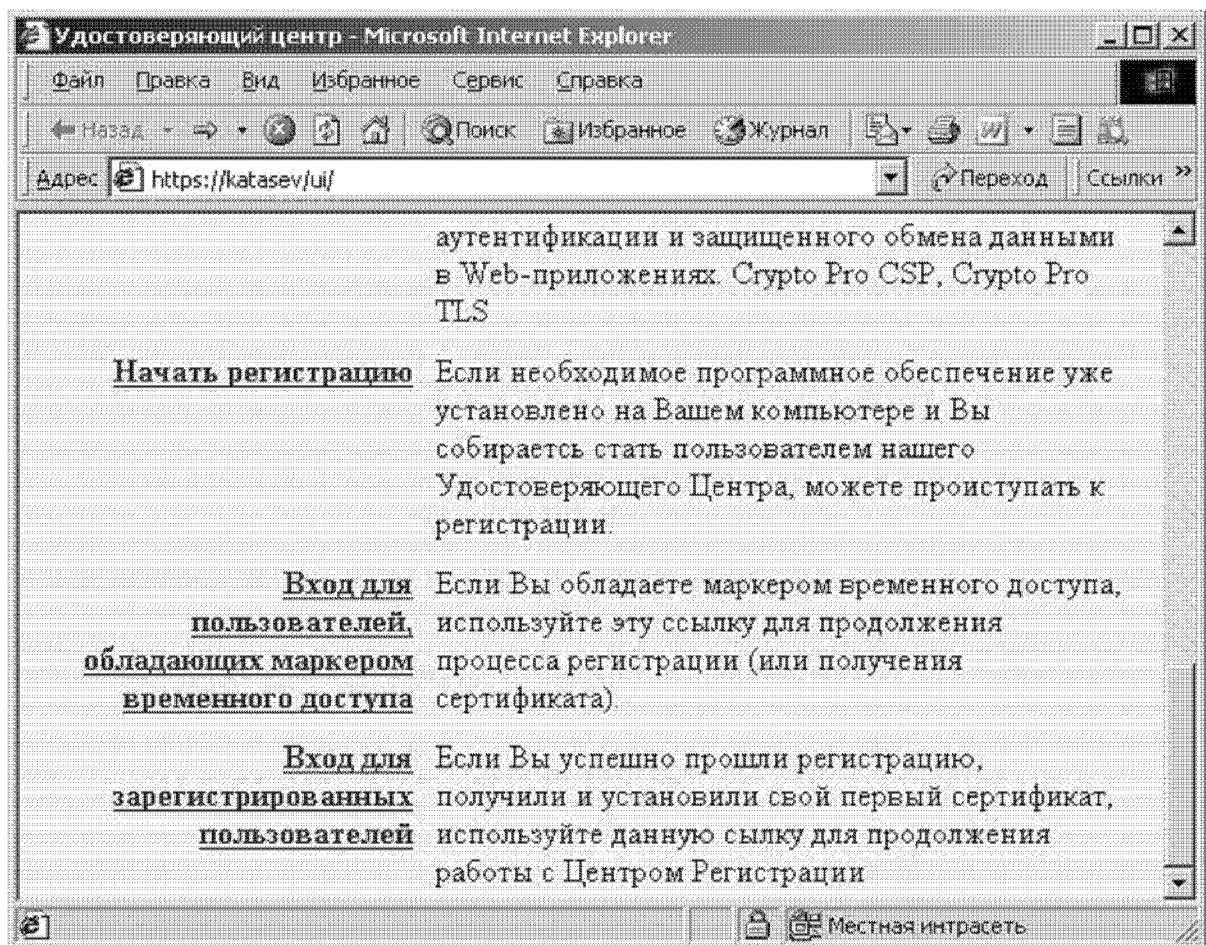


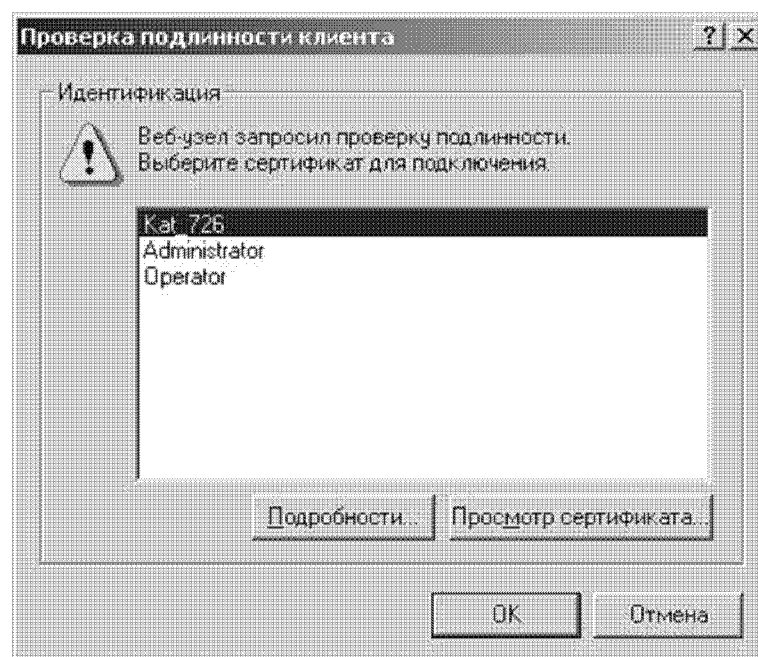
- сформировать запрос на сертификат и поставить в очередь;
- обновить страницу на АРМ зарегистрированного пользователя с маркерным доступом;
- установить выпущенный сертификат;





- закрыть страницу на АРМ зарегистрированного пользователя с маркерным доступом;
- открыть страницу по умолчанию web-интерфейса ЦР;
- перейти на АРМ зарегистрированного пользователя с ключевым доступом;



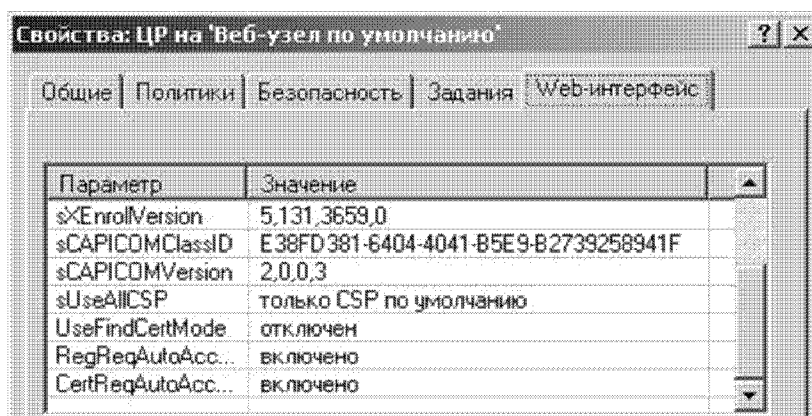


- сформировать запрос на сертификат и установить выпущенный сертификат.

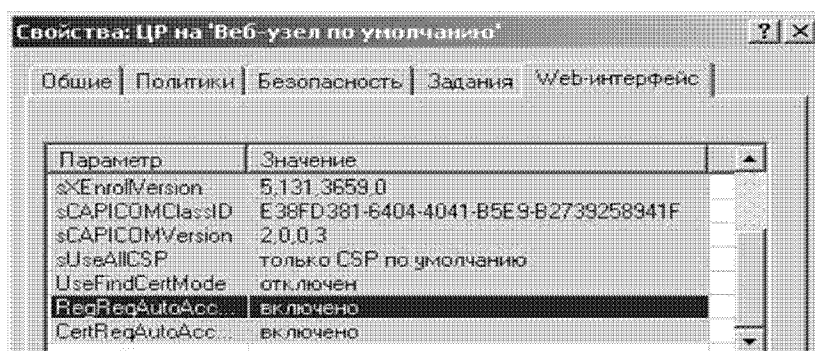
Регистрация пользователей, изготовление и управление сертификатами в распределенном режиме с ручным принятием запросов

В распределенном режиме управление пользователями и их сертификатами осуществляется удаленно с использованием web-интерфейса ЦР. Запросы на регистрацию пользователя, выпуск и управление сертификатами принимаются на АРМ администратора ЦР оператором или администратором.

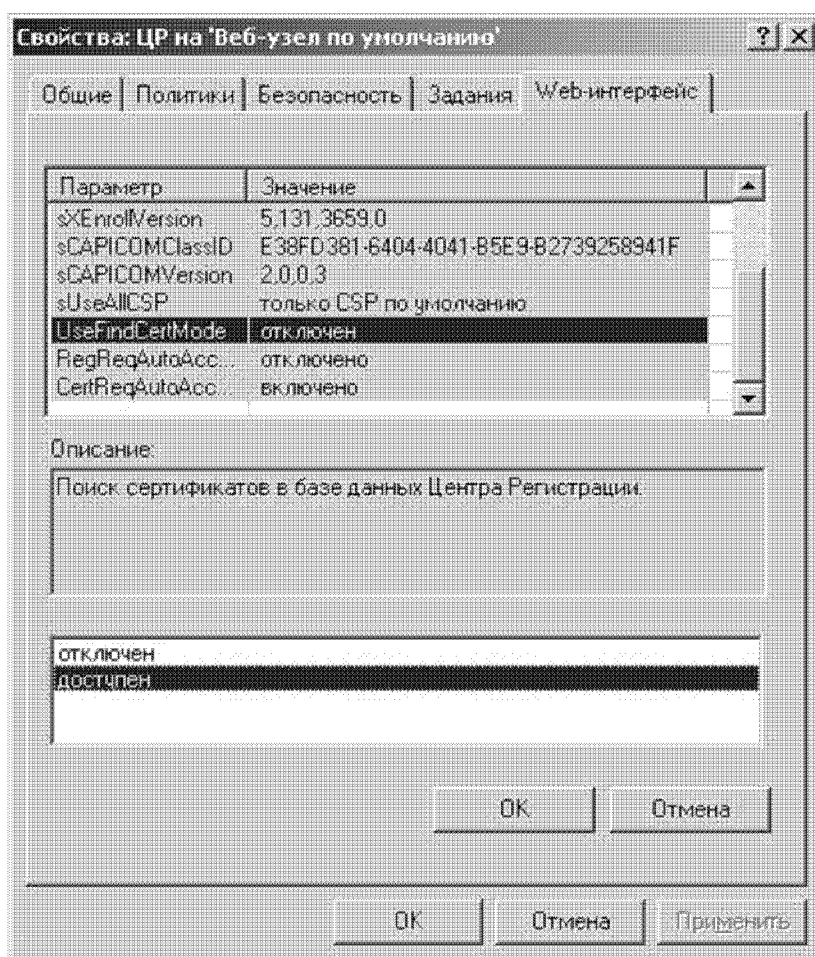
- запустить приложение «Параметры центра регистрации» и открыть окно свойств модуля доступа центра регистрации;



- отключить автоматическое принятие запросов на регистрацию и выпуск сертификата в настройках web-интерфейса;



- включить режим разрешения поиска сертификатов в настройках web-интерфейса;



- открыть страницу по умолчанию web-интерфейса центра регистрации (запомнить маркер временного доступа);
- сформировать запрос на регистрацию и поставить в очередь;
- на АРМ администратора активизировать подключение с ролью «оператор» и принять запрос на регистрацию пользователя;

- обновить страницу по умолчанию web-интерфейса ЦР;
- закрыть страницу по умолчанию web-интерфейса ЦР;
- открыть страницу по умолчанию web-интерфейса ЦР;
- перейти на АРМ зарегистрированного пользователя с маркерным доступом;
- сформировать запрос на сертификат и поставить в очередь;
- на АРМ администратора активизировать подключение с ролью «администратор» и принять запрос на сертификат пользователя;
- обновить страницу на АРМ зарегистрированного пользователя с маркерным доступом;
- установить выпущенный сертификат;
- закрыть страницу на АРМ зарегистрированного пользователя с маркерным доступом;
- открыть страницу по умолчанию web-интерфейса ЦР;
- перейти на АРМ зарегистрированного пользователя с ключевым доступом;
- изготовить новый сертификат пользователя;
- перейти в режим поиска сертификатов и найти сертификат администратора центра регистрации с ролью «администратор».

Поиск сертификатов в Реестре

Пожалуйста, выберите параметр по которому Вы собираетесь искать необходимый сертификат, введите искомое значение, если необходимо укажите условия сортировки и параметры вывода списка отобранных сертификатов.

Параметр сертификата:

Значение параметра:

Искать среди:

ЛАБОРАТОРНАЯ РАБОТА № 7

Тема лабораторной работы

Использование сертификатов в системах защищенного электронного документооборота

Цель работы

Изучить особенности использования ключей и сертификатов в системах защищенного электронного документооборота

ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

Защищенный документооборот

Современный защищенный электронный документооборот немислим без технологии PKI. PKI применяется там, где необходима единая устойчивая система безопасности, включающая в себя надежную аутентификацию, конфиденциальность, интеграцию технологий и обеспечение достоверности источника электронных сообщений.

Технология PKI может использоваться в различных информационных системах:

- обмена финансовой информацией с гарантией того, что все стороны, выполняющие финансовые операции, не будут в состоянии опровергнуть свое участие;
- для организации удаленного доступа с гарантией конфиденциальности передаваемой информации и уверенностью в том, что ее получит только тот, для кого она предназначена;
- в прикладных защищенных системах различного уровня (юридически значимый электронный документооборот, Интернет-банкинг, биллинговые системы, электронная коммерция, Интернет-процессинг и др.)

PKI обеспечивает программным обеспечением всю систему защиты внутри организации. Все логины, средства аутентификации, авторизации и другой сервис по обеспечению безопасности может быть обеспечен для приложений внутри

одной логической схемы, что позволит значительно уменьшить расходы.

Для того чтобы в полной мере использовать преимущества технологии PKI, необходимо одновременно обеспечить как доступность открытых ключей, так и их защиту от подделки и искажений при передаче по линиям связи. Для решения этих проблем и предназначены цифровые сертификаты. Удостоверяющие центры (УЦ), в свою очередь, дают механизмы доставки и администрирования цифровых сертификатов.

УЦ проектируется как доверенная, замкнутая, не модифицируемая автоматизированная система. УЦ построен по модульному принципу и содержит в своем составе следующие компоненты:

- Центры Сертификации (Certificate Authority (CA)) предназначены для выпуска и отзыва сертификатов открытых ключей;
- Центры Регистрации (Registration Authority (RA)) проверяют связь между открытыми ключами и местом, где они хранятся, перед тем как Центр Сертификации издаст сертификат. RA действует как вход для всех запросов, посылаемых к Центру Сертификации (CA);
- HSM-модуль позволяет повысить сохранность секретного ключа удостоверяющего центра путём разбиения его на несколько частей;
- Держатели сертификатов (для конечных пользователей) - люди, компьютеры или программные агенты, для которых были выпущены сертификаты и которые могут подписывать документы цифровой подписью.
- Клиенты проверяют подлинность цифровых подписей и соответствующих путей сертификации известных открытых ключей на доверяемых Центрах Сертификации.
- Хранилища являются трехсторонними базами данных, которые хранятся в директориях и делают доступными сертификаты, списки отзыва сертификатов (certificate revocation lists (CRLs));
- Политика безопасности определяет направление информационной безопасности для организации на самом верхнем уровне

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В каких системах может использоваться технология PKI
2. Какие компоненты входят в состав УЦ

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

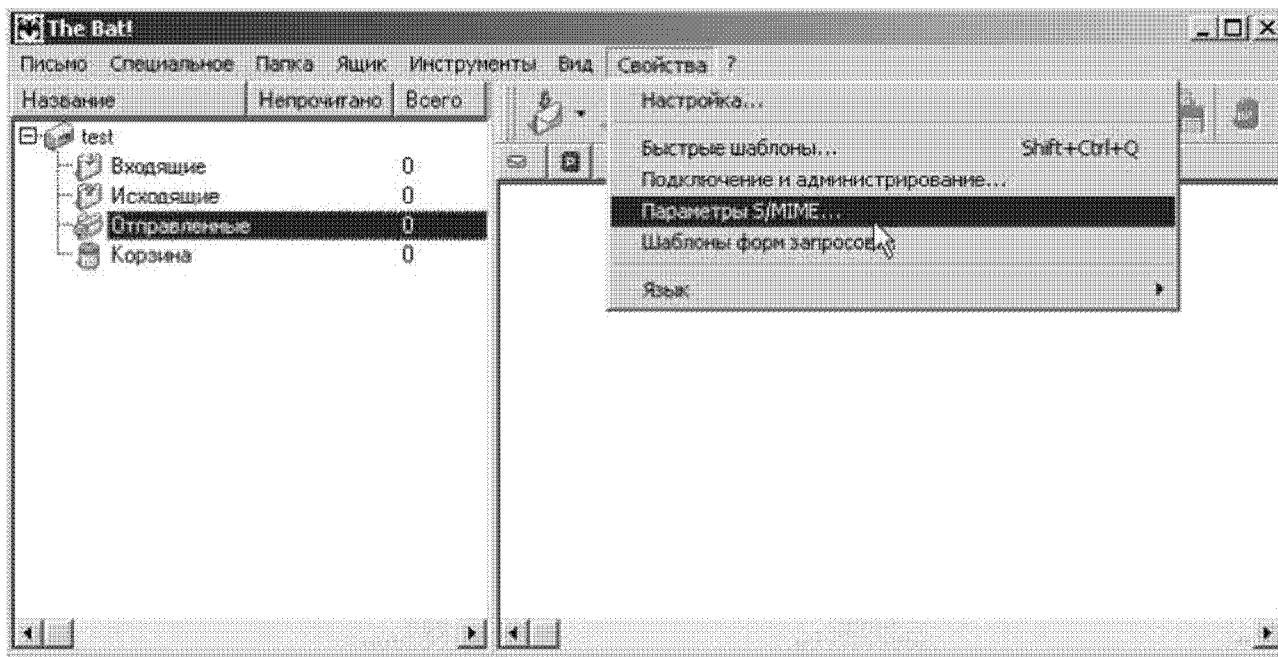
Изучить использование сертификатов в системах защищенного электронного документа оборота

Использование КриптоПро CSP в the Bat

Настройка параметров The Bat!

Для использования протокола S/MIME в почтовой программе The Bat! необходимо, прежде всего, настроить его параметры.

Для этого выполните следующие действия:



1. Выберите пункт меню Свойства -> Параметры S/MIME:
2. В появившемся окне настройки выберите следующие параметры:

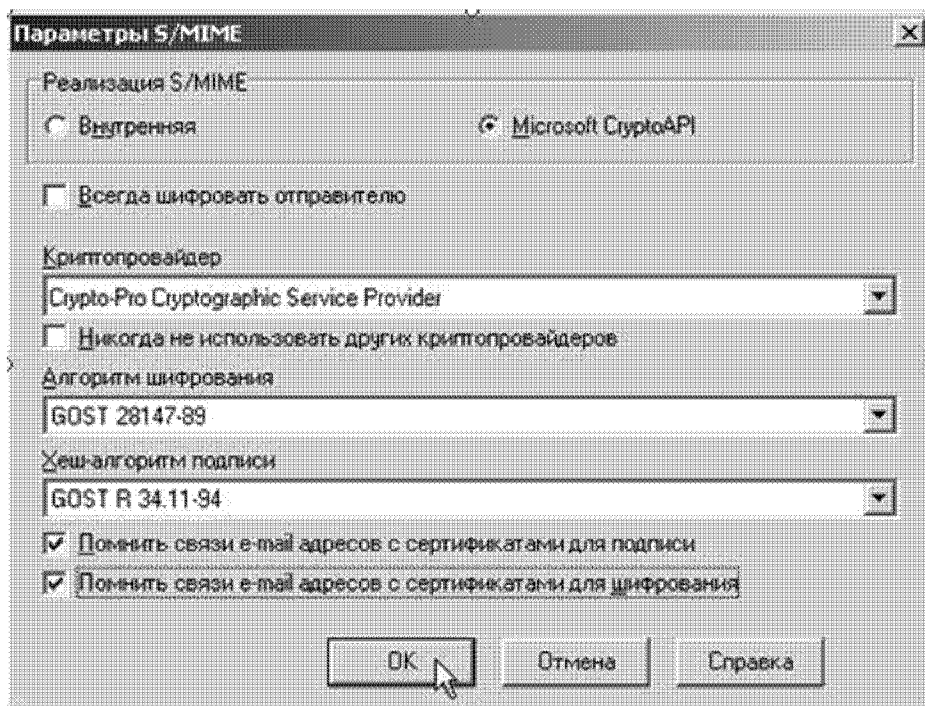
- Реализация S/MIME –> Microsoft CryptoAP

Если вы хотите, чтобы все письма перед отправкой шифровались на закрытом ключе получателя, отметьте пункт Всегда шифровать отправителю.

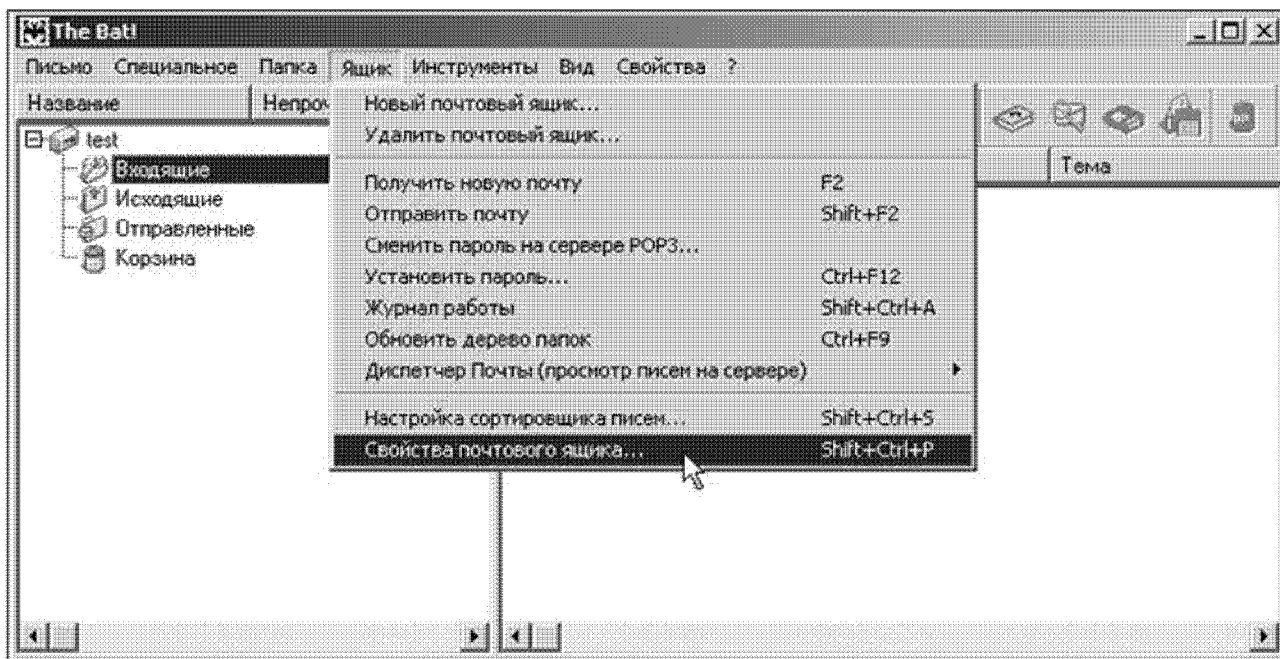
- Криптопровайдеры –> Crypto-Pro Cryptographic Service Provider.

Если вы не хотите использовать сертификаты и ключевые пары на других криптопровайдерах, пометьте пункт Никогда не использовать других криптопровайдеров.

- Алгоритм шифрования (выберите из списка или оставьте по умолчанию)
- Хеш-алгоритм подписи (выберите из списка или оставьте по умолчанию)
- Включите опции Помнить связь e-mail адресов с сертификатами для подписи и Помнить связь e-mail адресов с сертификатами для шифрования. Это избавит Вас от необходимости каждый раз выбирать нужный сертификат из списка.



3. Выберите пункт меню Ящик -> Свойства почтового ящика:



4. В дереве настроек Свойства почтового ящика выберите вкладку Параметры.

•В области Редактор писем можно выбрать опцию Подписать перед отправкой и Зашифровать перед отправкой. Это позволит автоматически при отправке подписывать и зашифровывать сообщения. Обязательно должна быть отмечена опция Авто – S/MIME:

