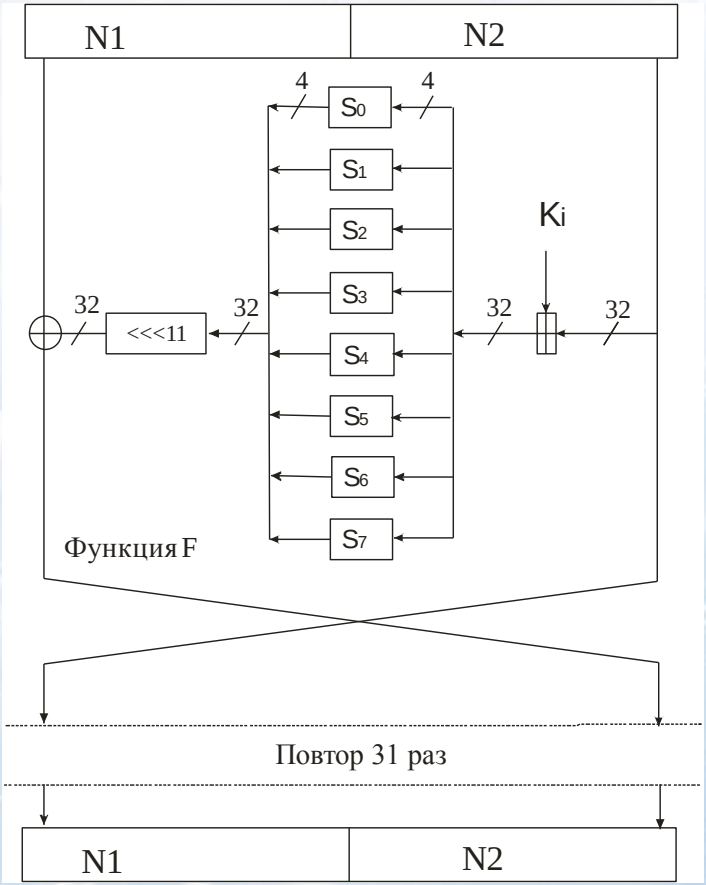
Введение в инфраструктуру открытых ключей

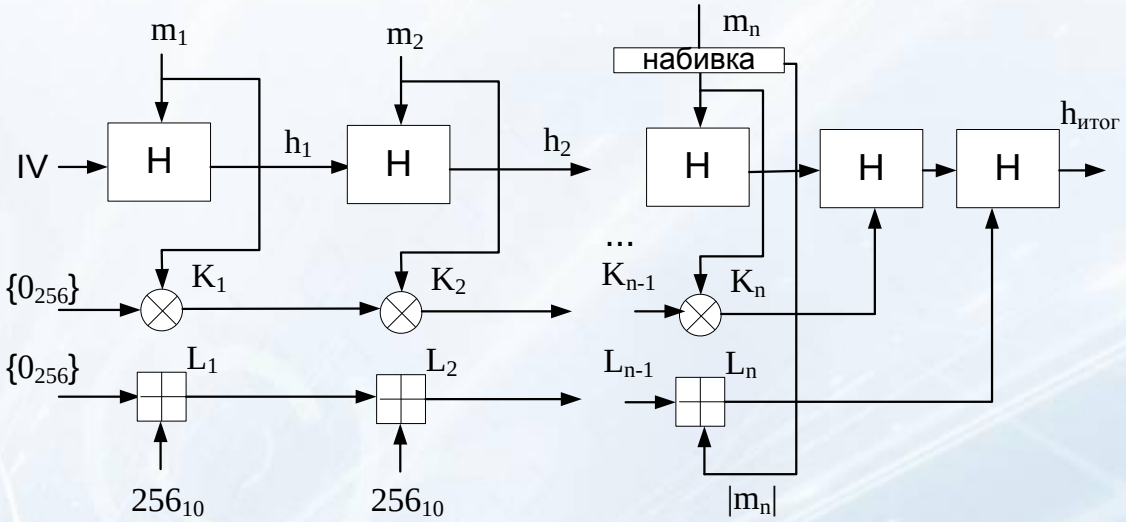
Симметричное шифрование

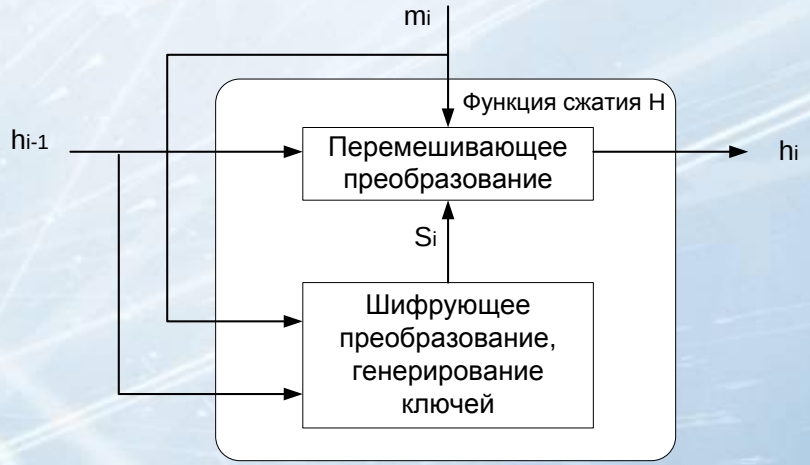
Для обеспечения конфиденциальности данных используется шифрование информации. В России в качестве национального стандарта используется алгоритм шифрования ГОСТ 28147-89.



- сложение по модулю 2^{32}

ХЭШ-функция





ЭЦП

Подписание документа автором:

Проверка подписи получателем:

ФЗ N 63-ФЗ "Об электронной подписи"

от 6 апреля 2011 г.

Федеральный закон от 10 января 2002 года № 1-ФЗ "Об ЭЦП" признать утратившим силу с 1 июля 2012 года.

Типы подписей:

1. Простая (коды, пароли или иных средств для подтверждения факта формирования электронной подписи конкретным лицом)

2. Усиленная

- Неквалифицированная
- Квалифицированная

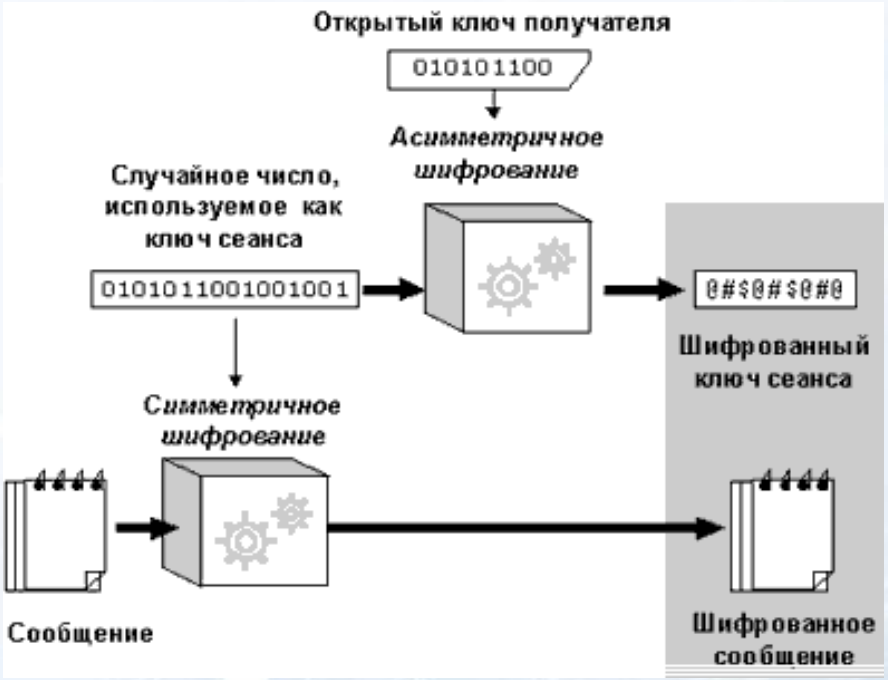
Неквалифицированная эл.подпись

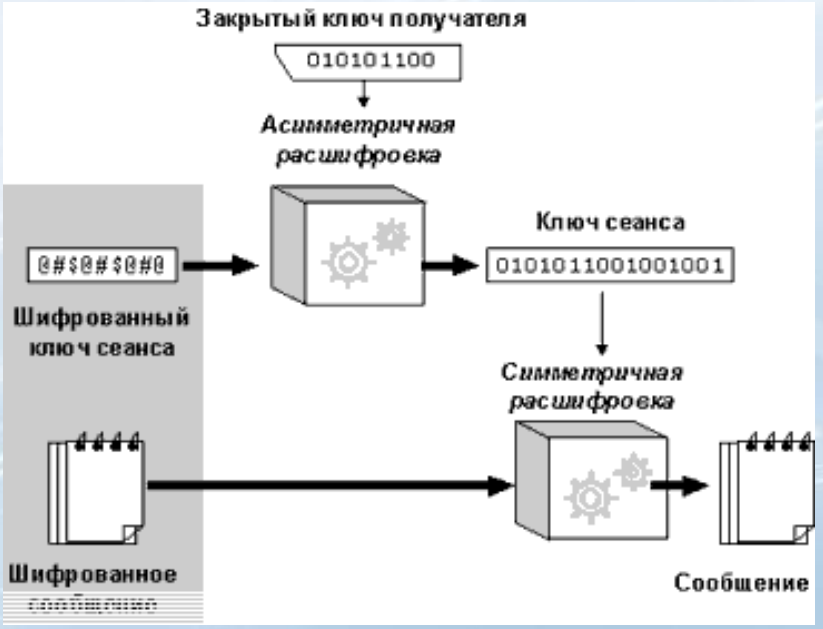
- получена в результате криптографического преобразования информации с использованием ключа электронной подписи
- позволяет определить лицо, подписавшее электронный документ
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Квалифицированная эл.подпись

- все признаки неквалифицированной эл.подписи
- ключ проверки эл.подписи указан в квалифицированном сертификате
- для создания и проверки эл.подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Электронный цифровой конверт





Распределение ключей

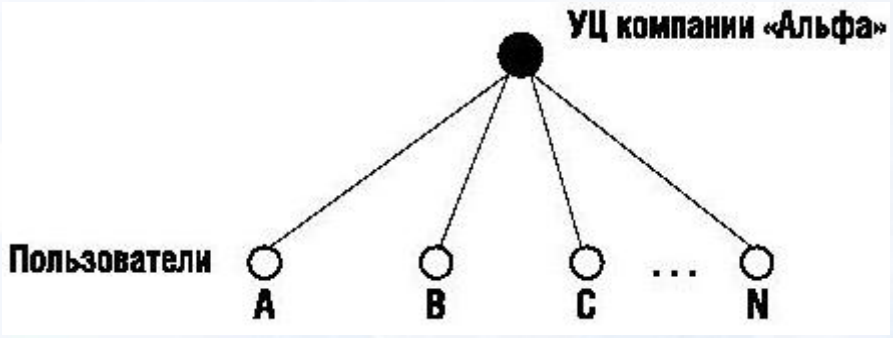
Необходимо исключить подмену на этапе пересылки открытых ключей, а также подтвердить правильность сведений о владельце.

Рассмотрим два варианта обмена :

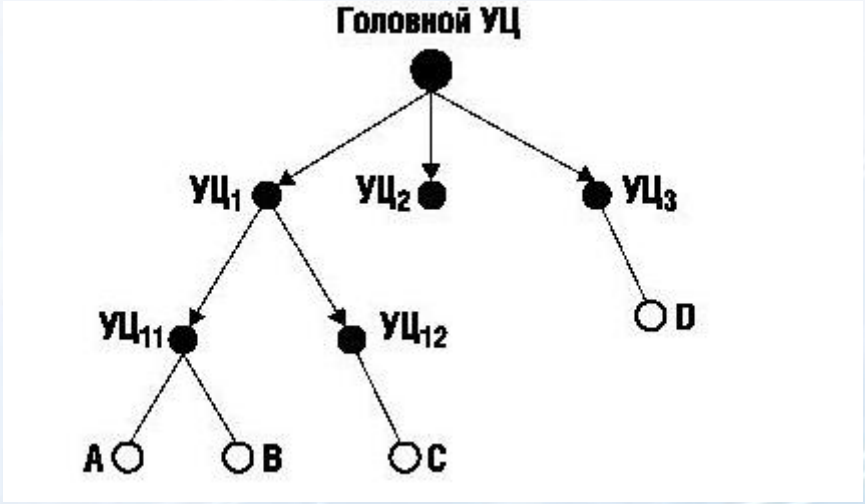
- Прямой обмен открытыми ключами
- Обмен открытыми ключами через удостоверяющий центр.

Архитектуры Public Key Infrastructure

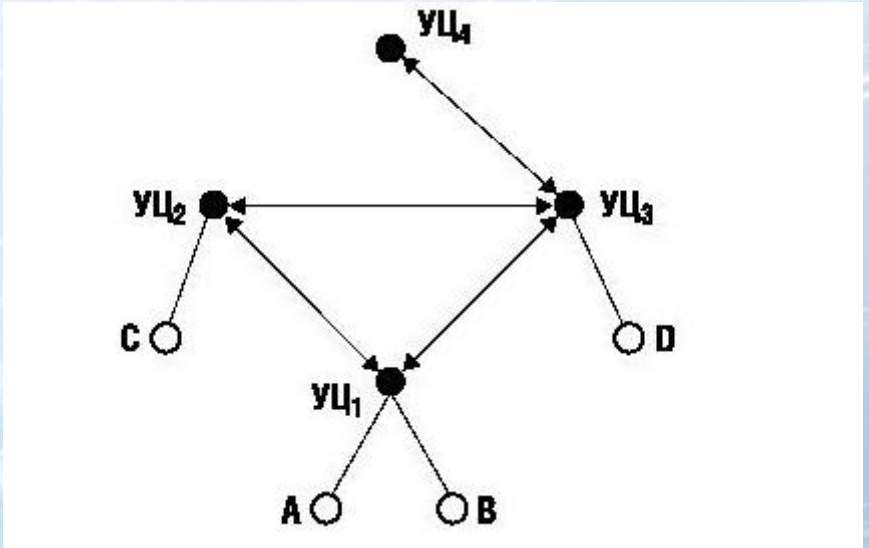
Одиночный УЦ



Иерархическая PKI

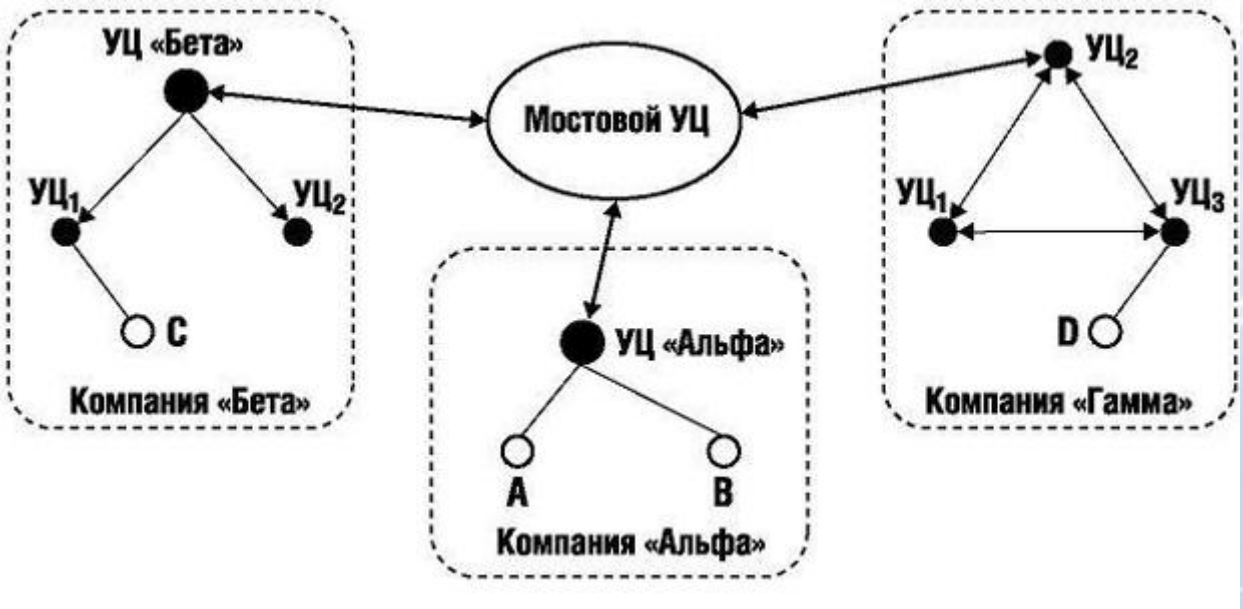


Сетевая PKI



Архитектуры PKI (2)

Архитектура мостового УЦ



Стандарт X.509 версия 3

Version	Версия сертификата	3
Certificate Serial Number	Серийный номер сертификата	40:00:00:00:00:00:00:ab:38:1e:8b:e9:00:31:0c:60
Signature Algorithm Identifier	Идентификатор алгоритма ЭЦП	ГОСТ Р 34.10-94
Issuer X.500 Name	Имя Издателя сертификата	C=RU, ST=Moscow,O=PKI, CN=Certification Authority
Validity Period	Срок действия сертификата	Действителен с : Ноя 2 06:59:00 1999 GMT Действителен по : Ноя 6 06:59:00 2004 GMT
Subject X.500 Name	Имя Владельца сертификата	C=RU, ST=Moscow, O=PKI, CN=Sidorov
Subject Public Key Info	Открытый ключ Владельца	тип ключа: Открытый ключ ГОСТ длина ключа: 1024 значение: AF:ED:80:43.....
Issuer Unique ID version 2	Уникальный идентификатор Издателя	
Subject Unique ID version 2	Уникальный идентификатор Владельца	
type critical value		**дополнения (только версия 3)**
type critical value		
type critical value		
CA Signature ЭЦП Центра Сертификации		

Типы дополнений:

- ограничивающие
- информационные

Программный комплекс «Верба-сертификат - МВ»

Удостоверяющий центр на базе программного комплекса «Верба»

Назначение

- Построение иерархической системы управления сертификатами (PKI)

- Обеспечение конфиденциальности, целостности информации и подтверждение авторства (ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94, ГОСТ 28147-89)

Состав

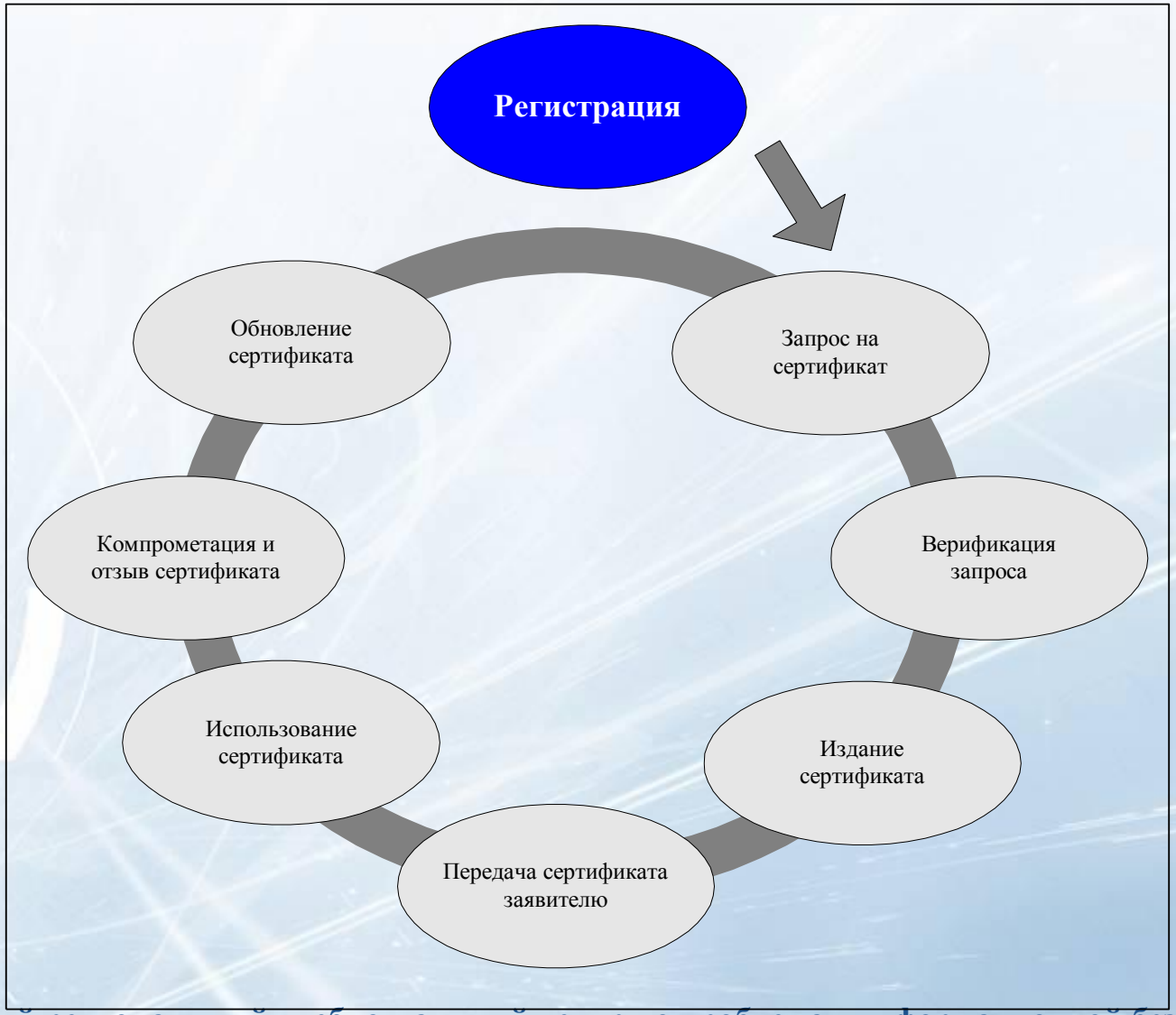
- Удостоверяющий центр:
  - Центры сертификации (ЦС)
  - Центры регистрации (ЦР)
  - АРМ РКС
- Конечные пользователи:
  - «Верба- Сертификат МВ Клиент»
  - ПО «Верба-файл»

Базовые объекты

системы «Верба-Сертификат МВ»

- сертификат (.cer)
- список отозванных сертификатов (СОС) (.crl)
- запрос на сертификат (.pse)
- сертификат регистрации (.cer)
- сообщение о компрометации (.pse)
- упакованные данные (PKCS#7 и PKCS#10)

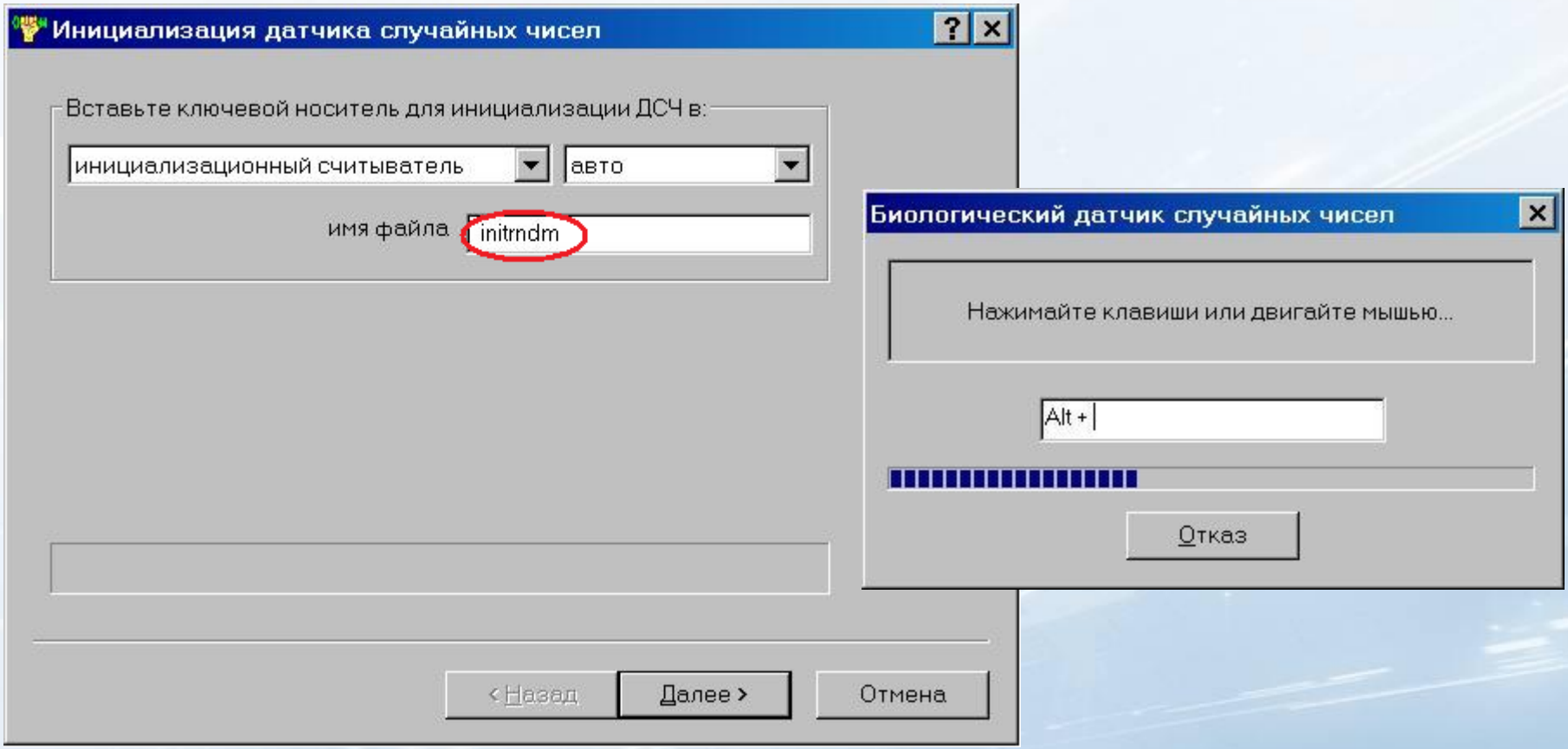
Жизненный цикл объектов



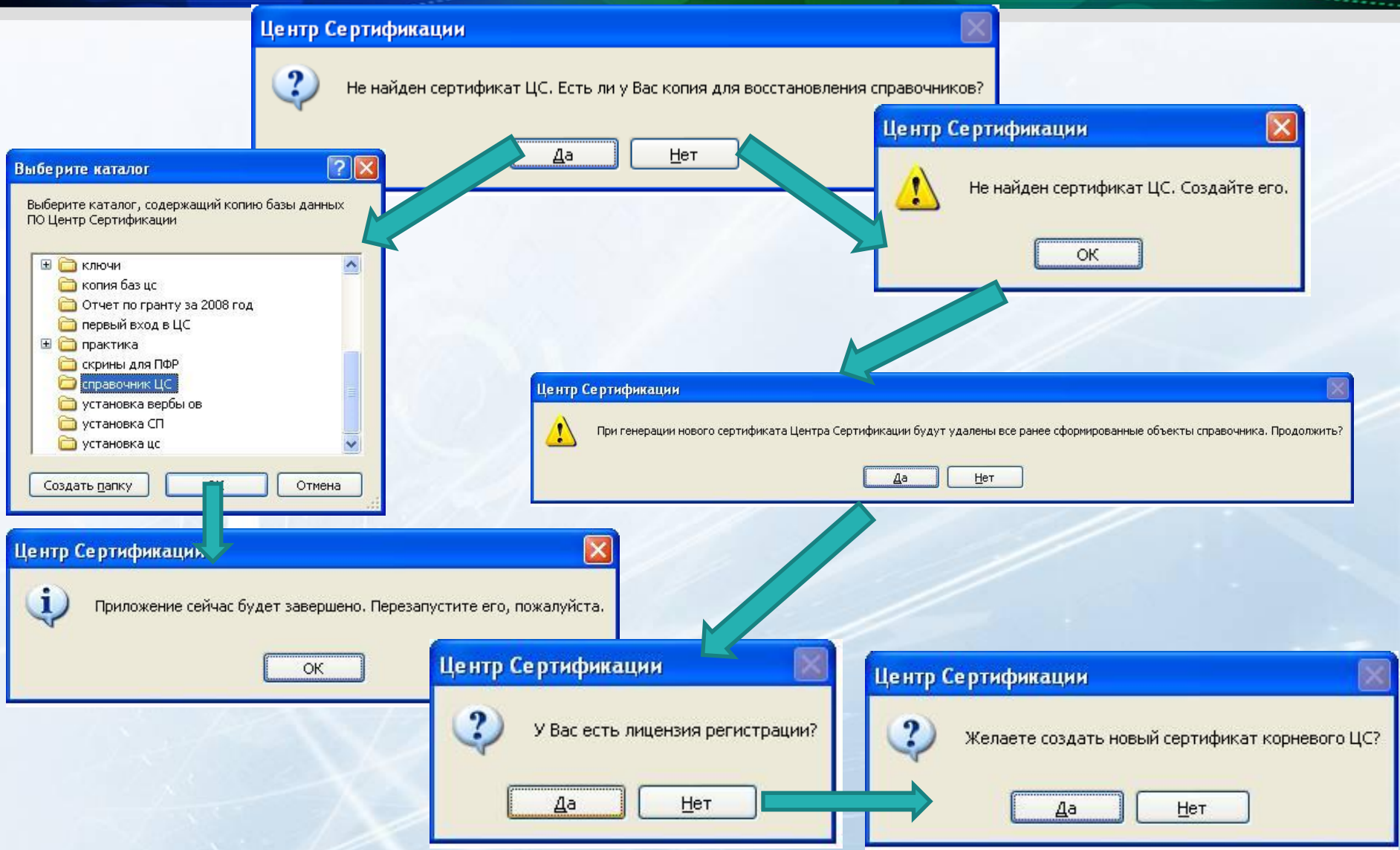
Центр Сертификации

Биологический датчик случайных чисел

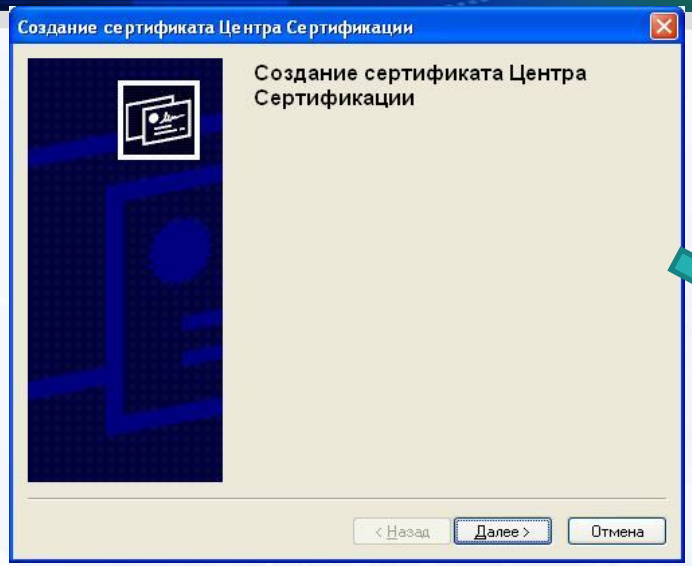
Первоначальная инициализация датчика

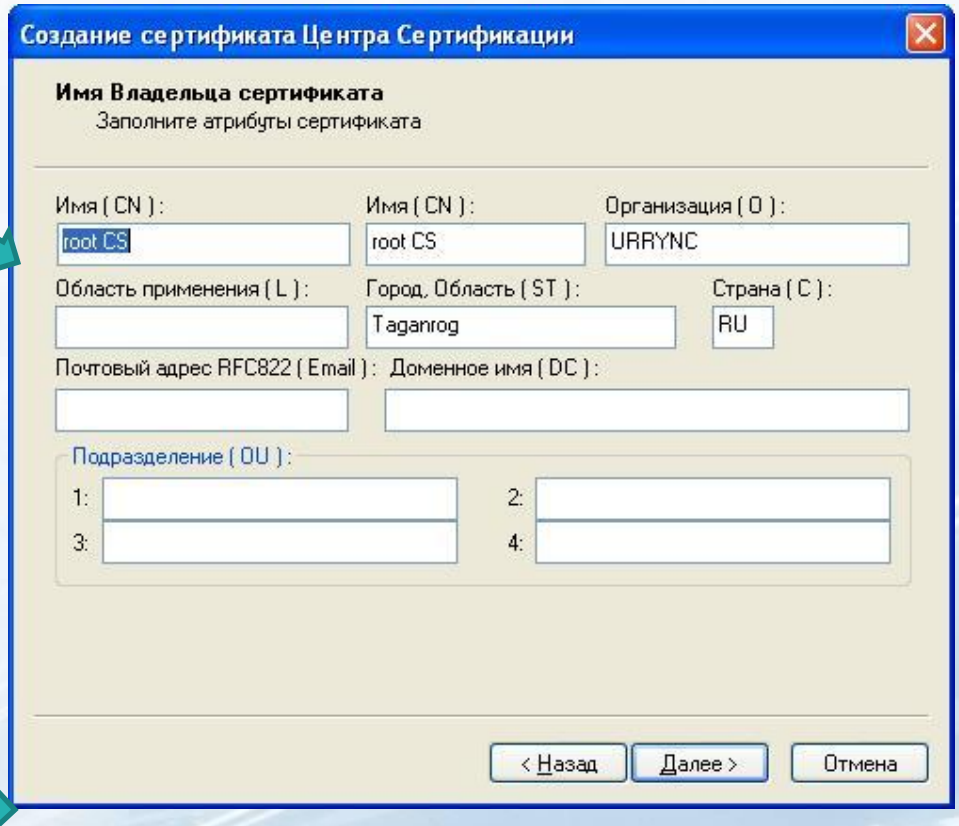


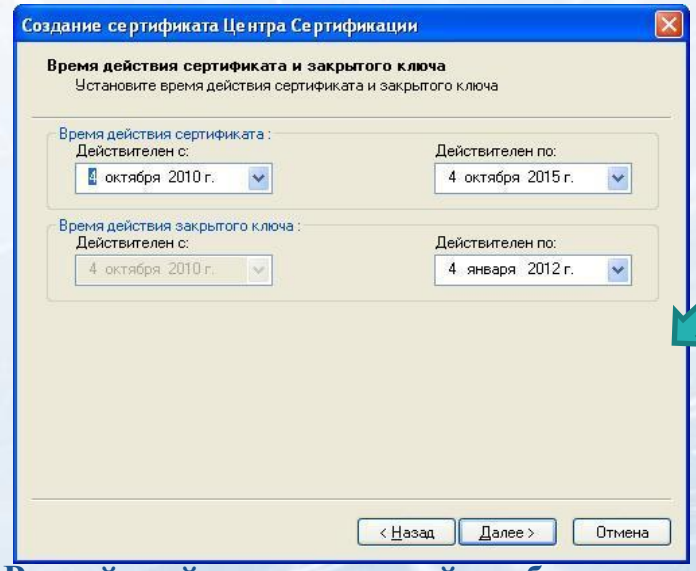
Первый запуск ЦС



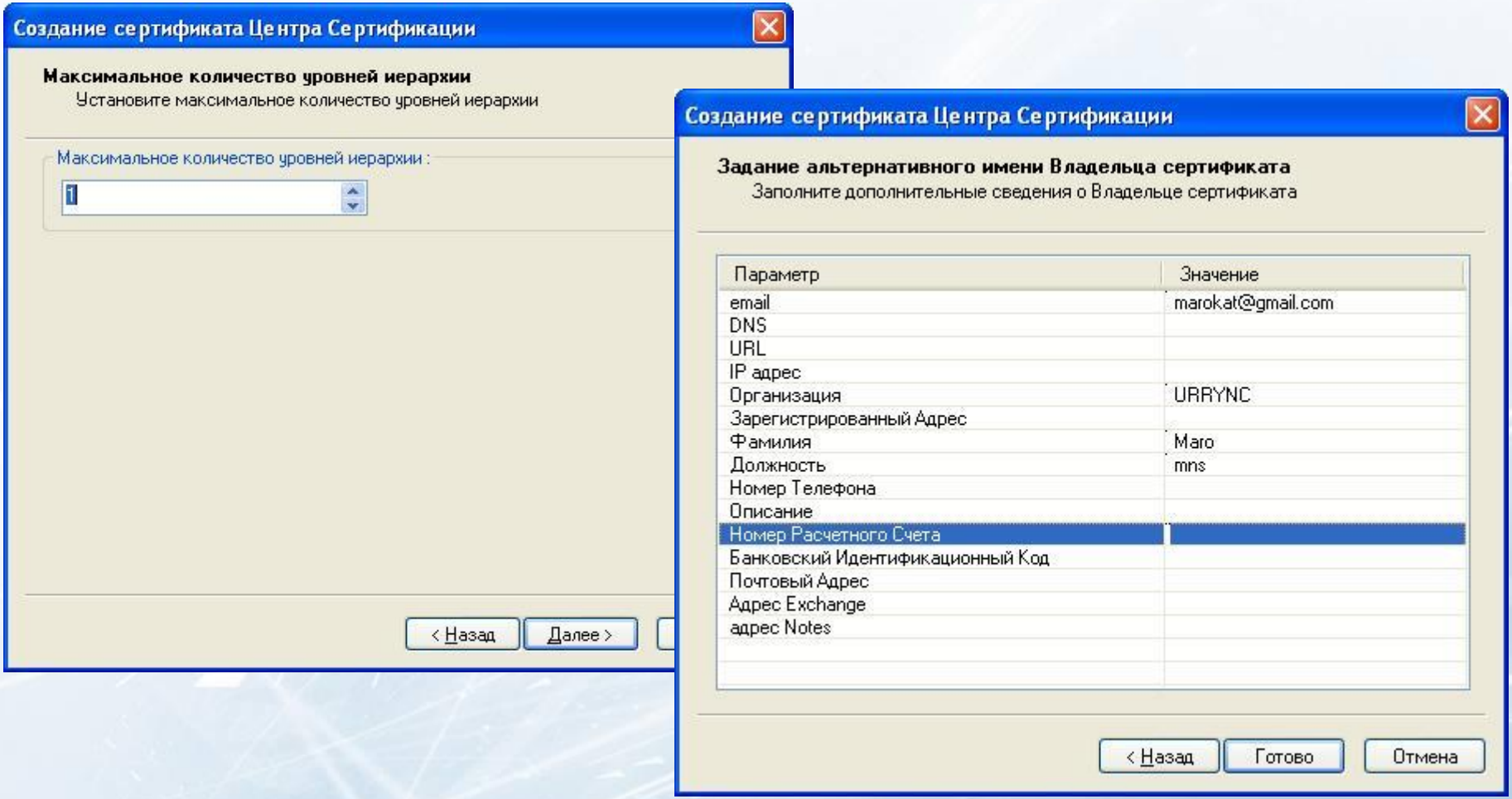
Создание самоподписанного сертификата





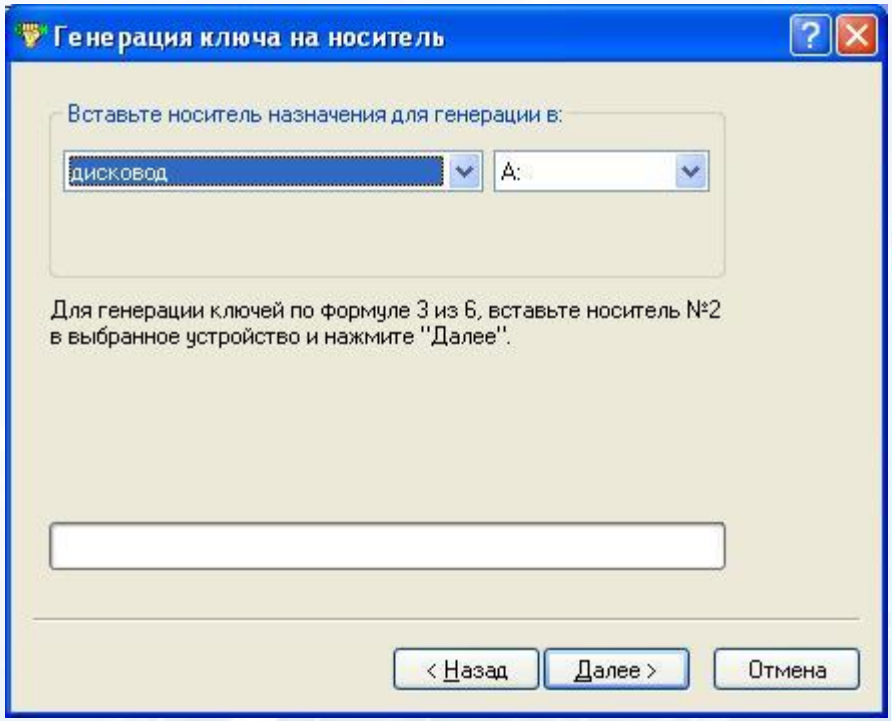


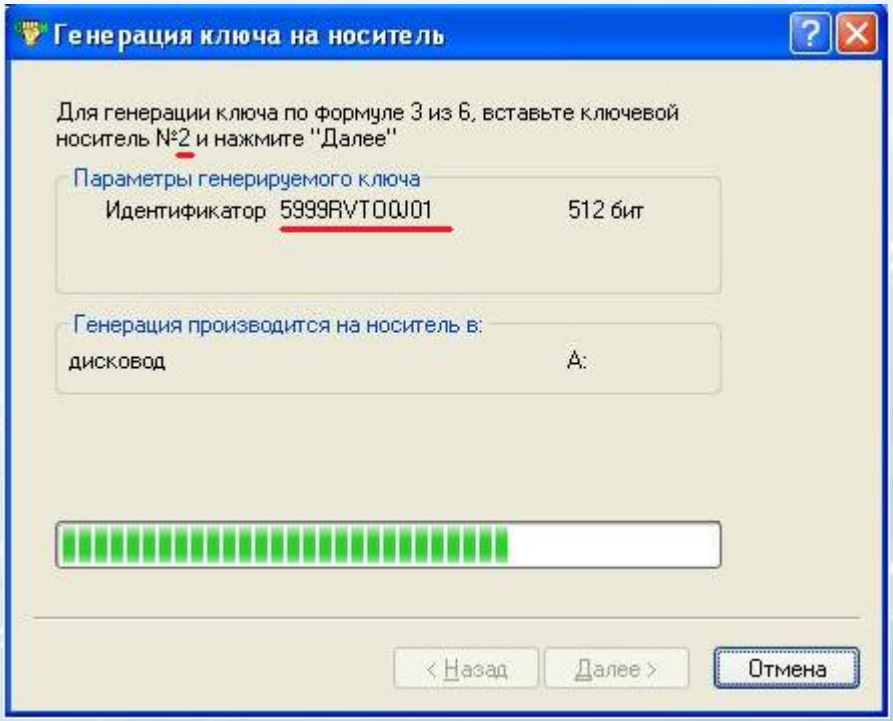
Создание самоподписанного сертификата



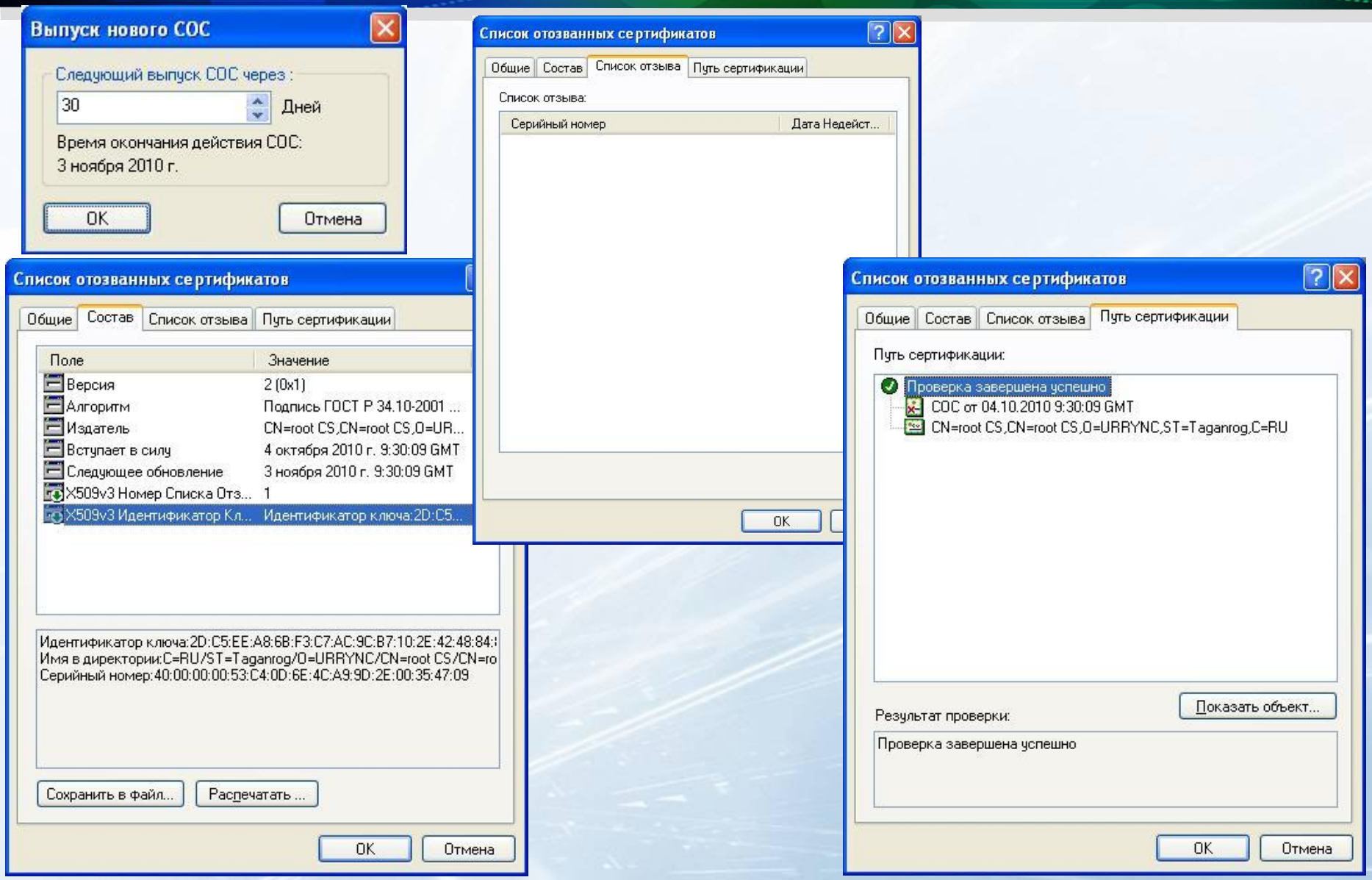
Сертификат ЦС печатается в двух экземплярах

Создание закрытых ключей ЦС

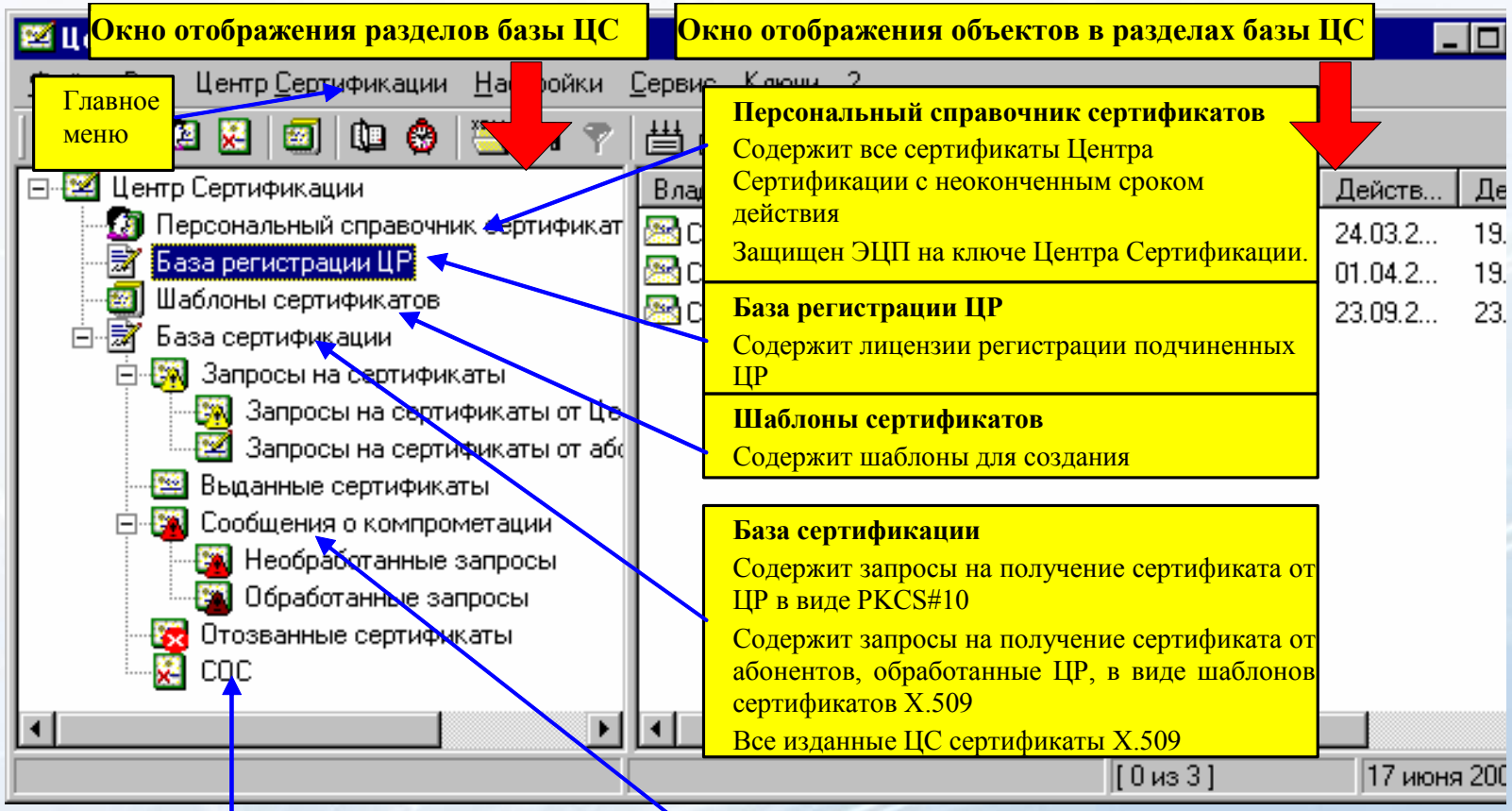




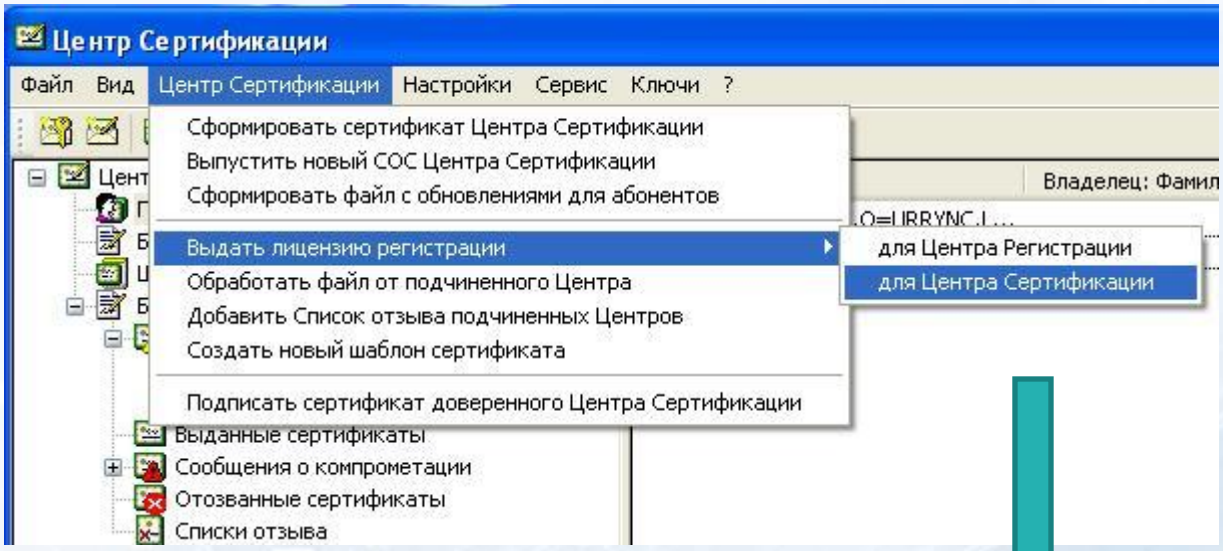
Формирование СОС ЦС

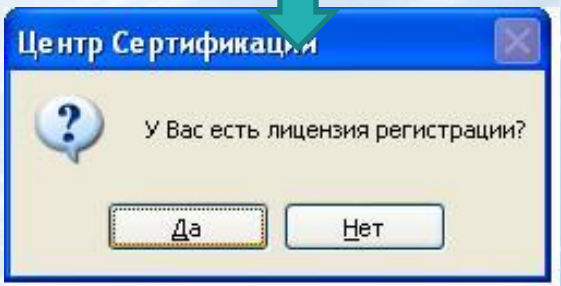


Интерфейс ЦС

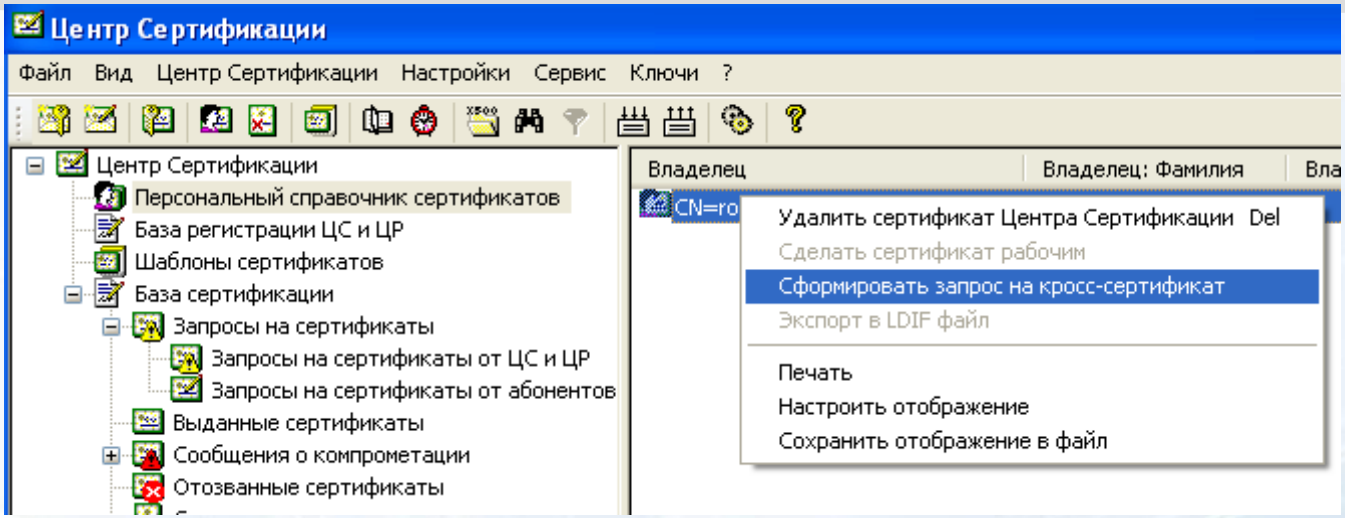


Регистрация подчиненного ЦС



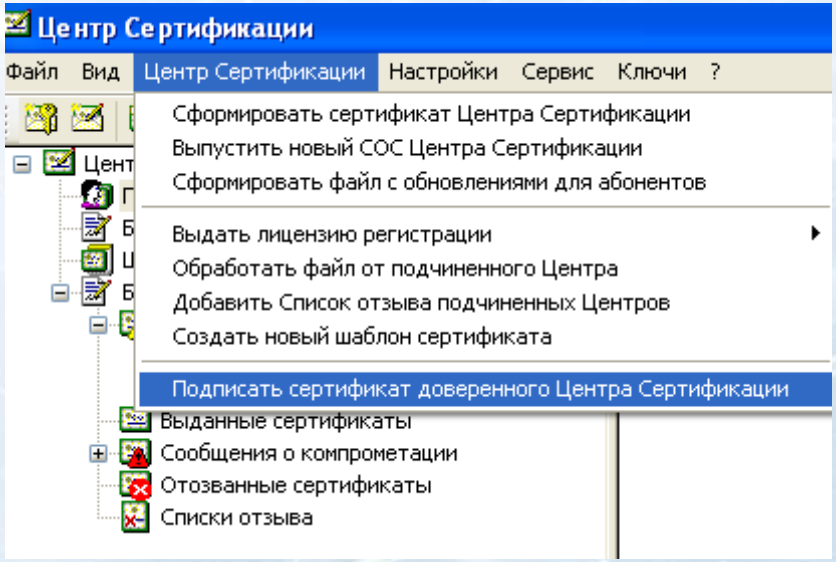


Установление доверия между ЦС



(.req)

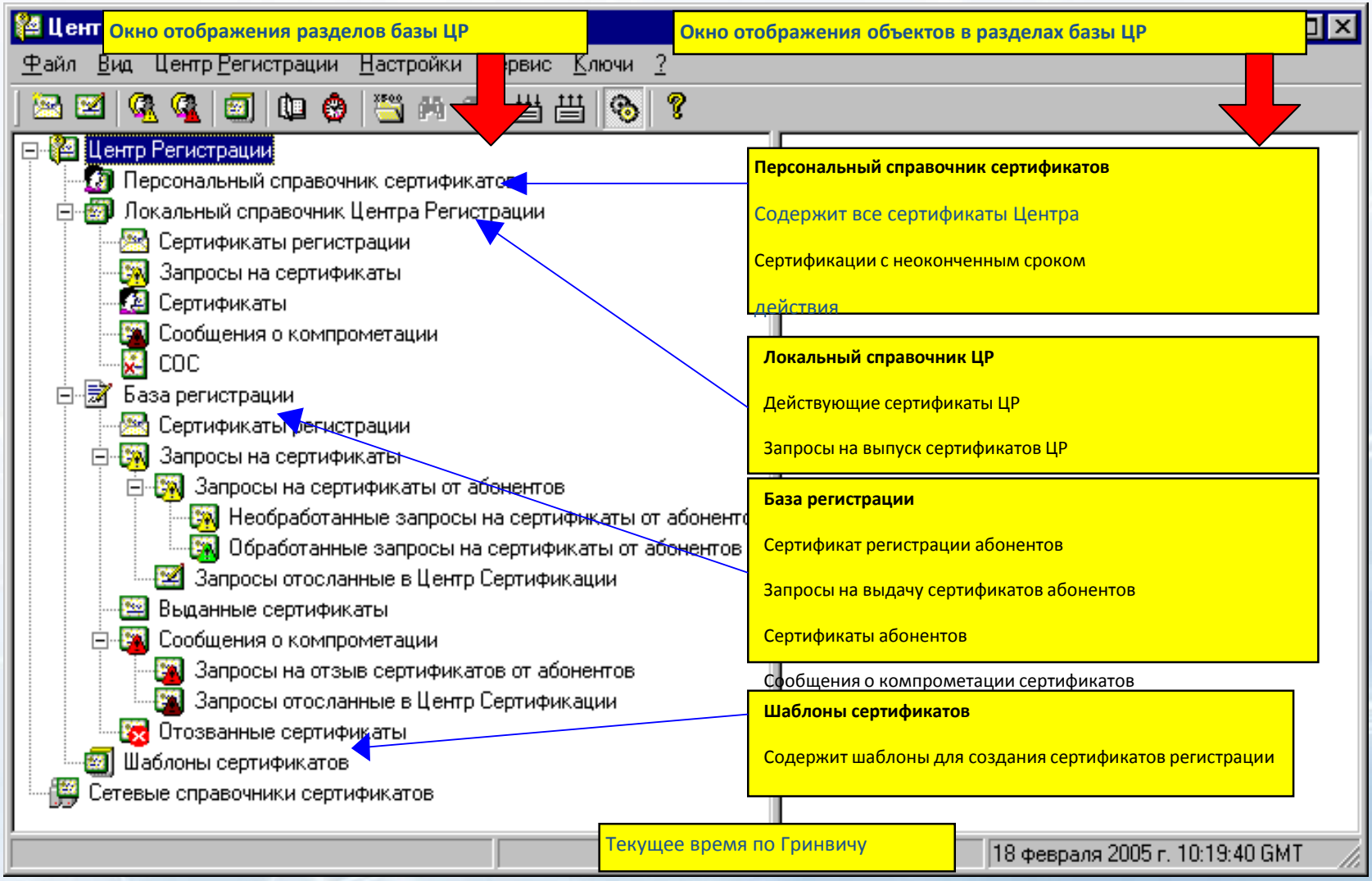
ASN 1 .DER



(.pse) PKCS#7

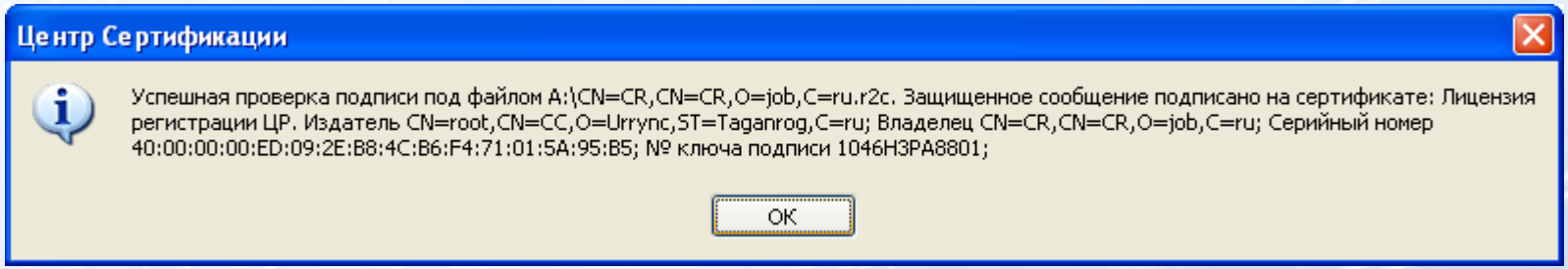
Центр Регистрации

Интерфейс ЦР

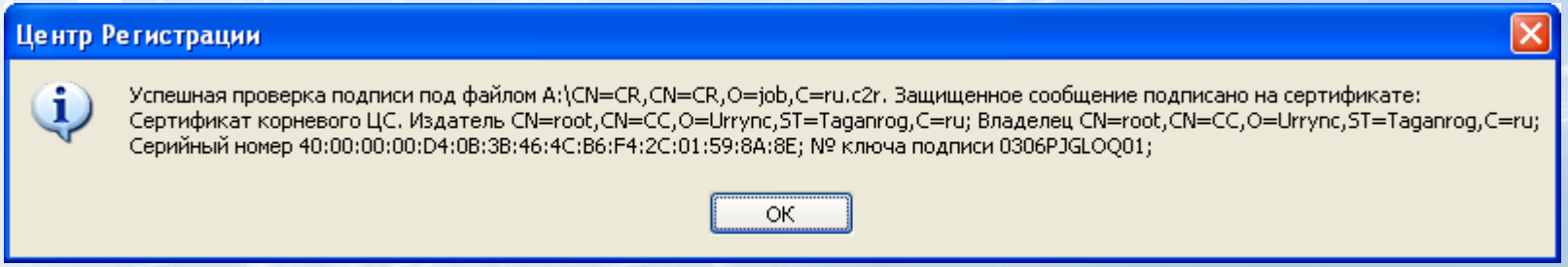


Создание сертификата ЦР

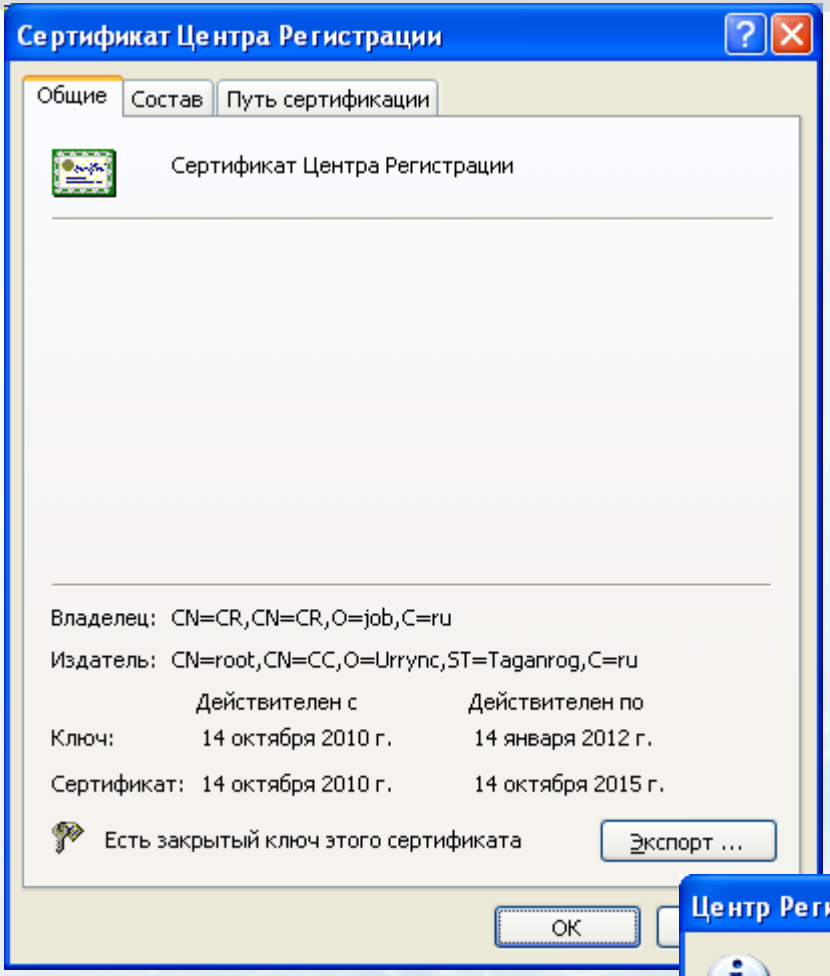
- ЦС: ЦС→Выдать лицензию регистрации →для ЦР
- ЦР: Вход по лицензии регистрации
- ЦР: ЦР →Сформировать запрос на сертификат ЦР (.r2c)
- ЦС: ЦС →Обработать файл от подчиненного центра

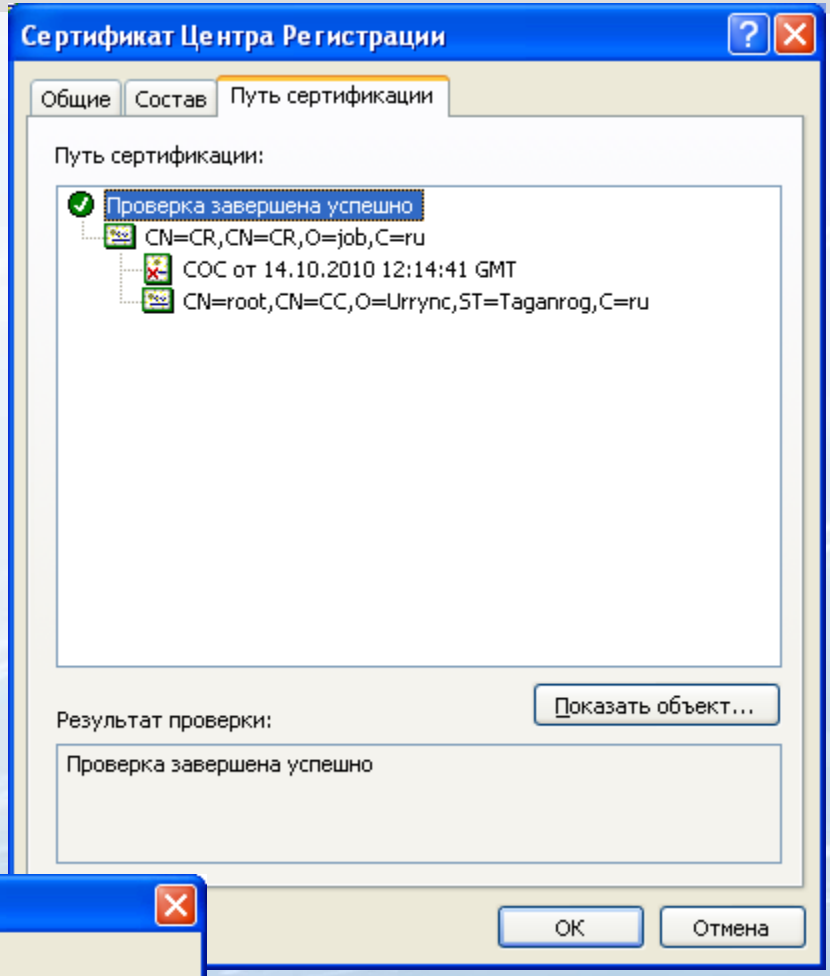


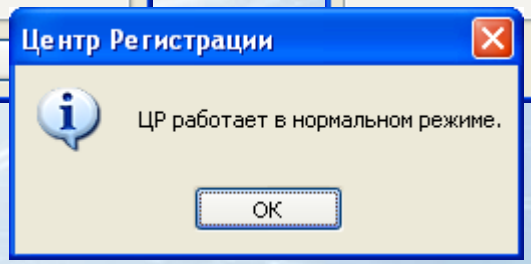
- ЦС: Создание сертификата и сохранение для ЦР (.c2r)
- ЦР: ЦР → Обработать файл из ЦС



Создание сертификата ЦР

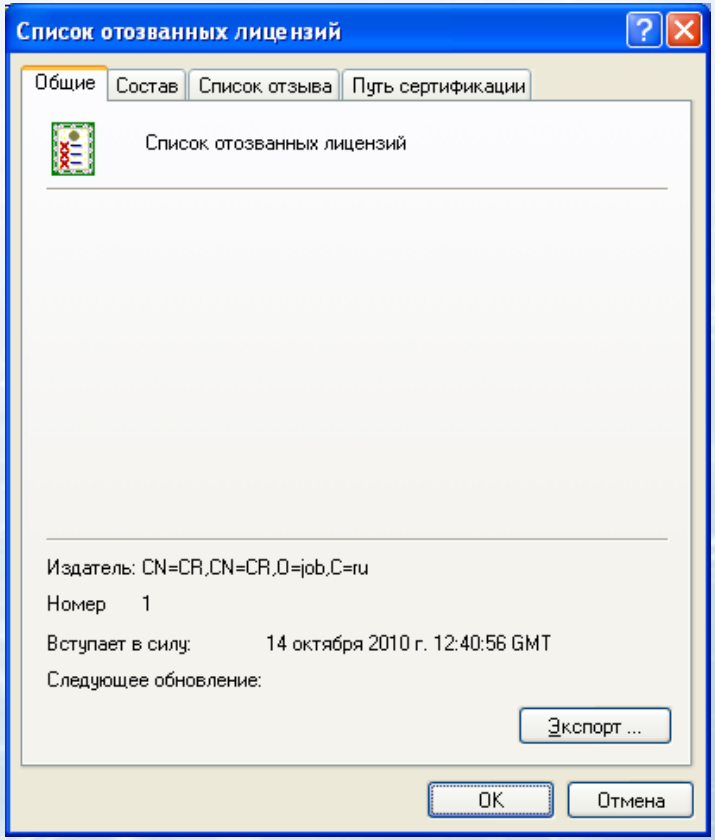


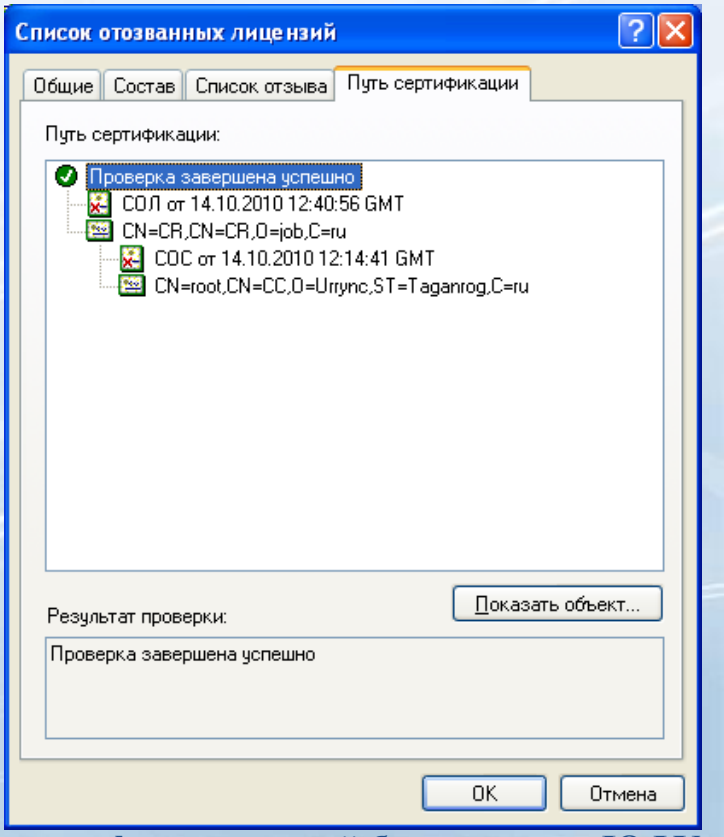




Импорт СОЛ ЦР в ЦС

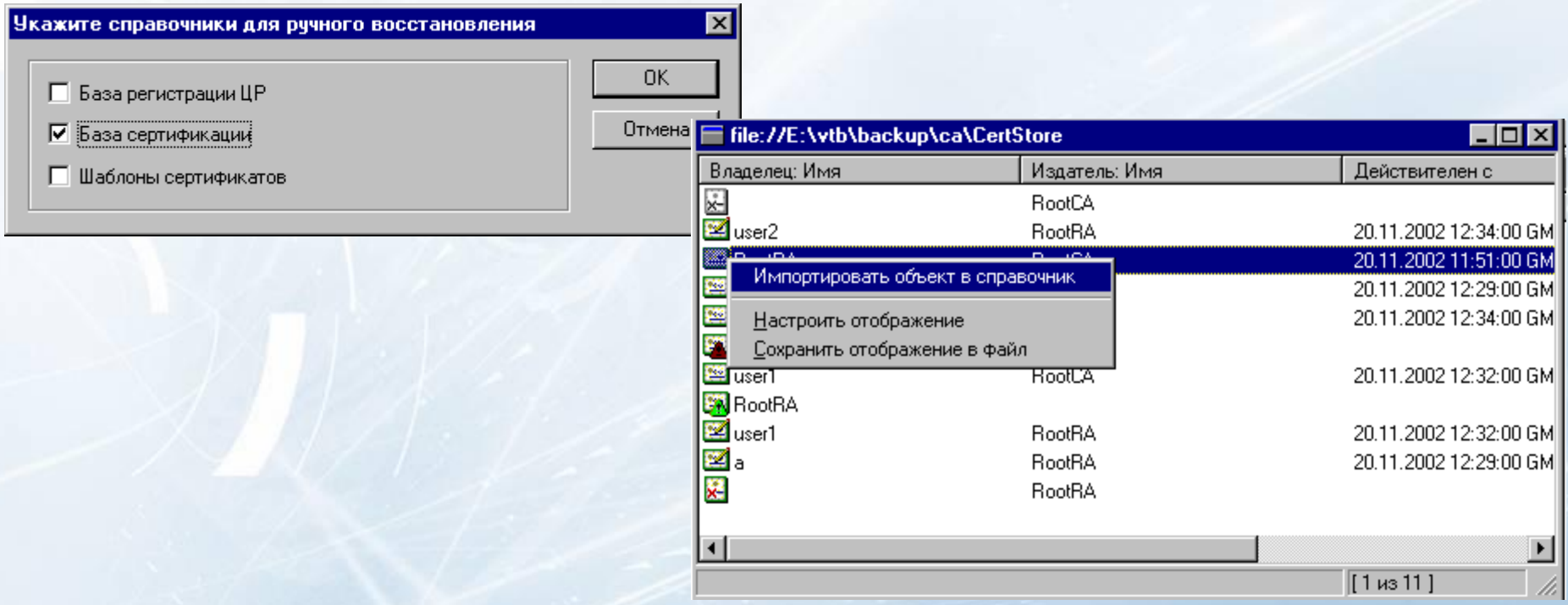
- ЦР: Списки отзыва→Экспорт в файл в DER кодировке (.crl)
- ЦС: ЦС→Добавить Список отзыва подчиненных Центров





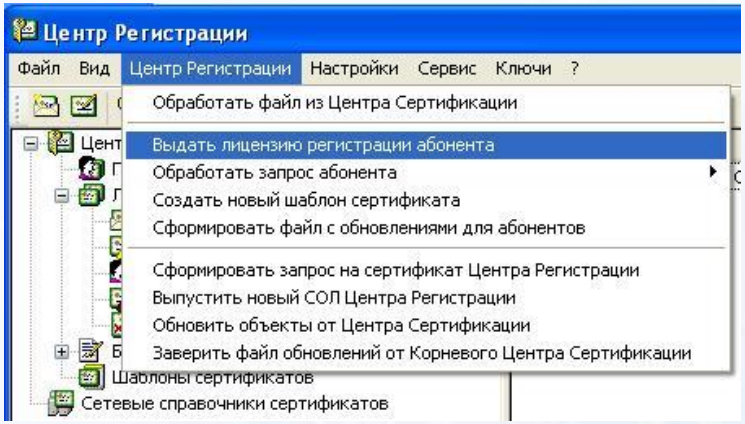
Восстановление баз

Сервис→Восстановление справочников
Сервис→Ручное восстановление справочников



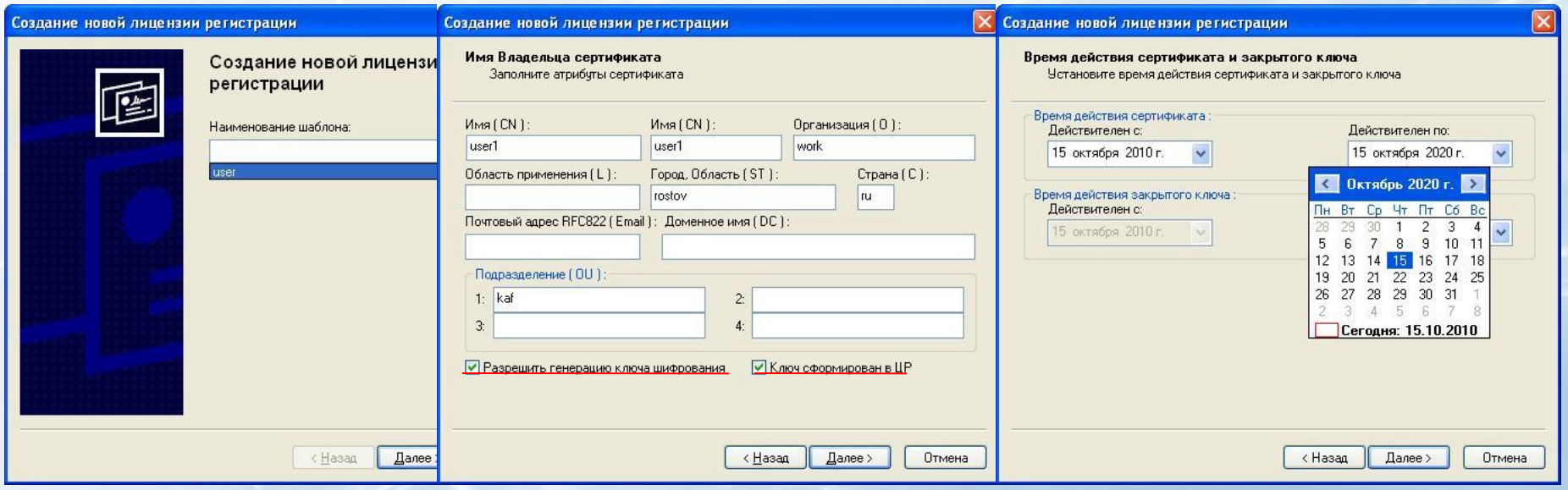
Создание сертификатов пользователей

Регистрация пользователя



Пользователь предоставляет:

- лист с образцами печати и личной подписи руководителя организации
- копию Договора с администрацией системы
- выписку из приказа о назначении администратора информационной безопасности организации



Генерация ключей пользователем

Пользователь получает в ЦР:

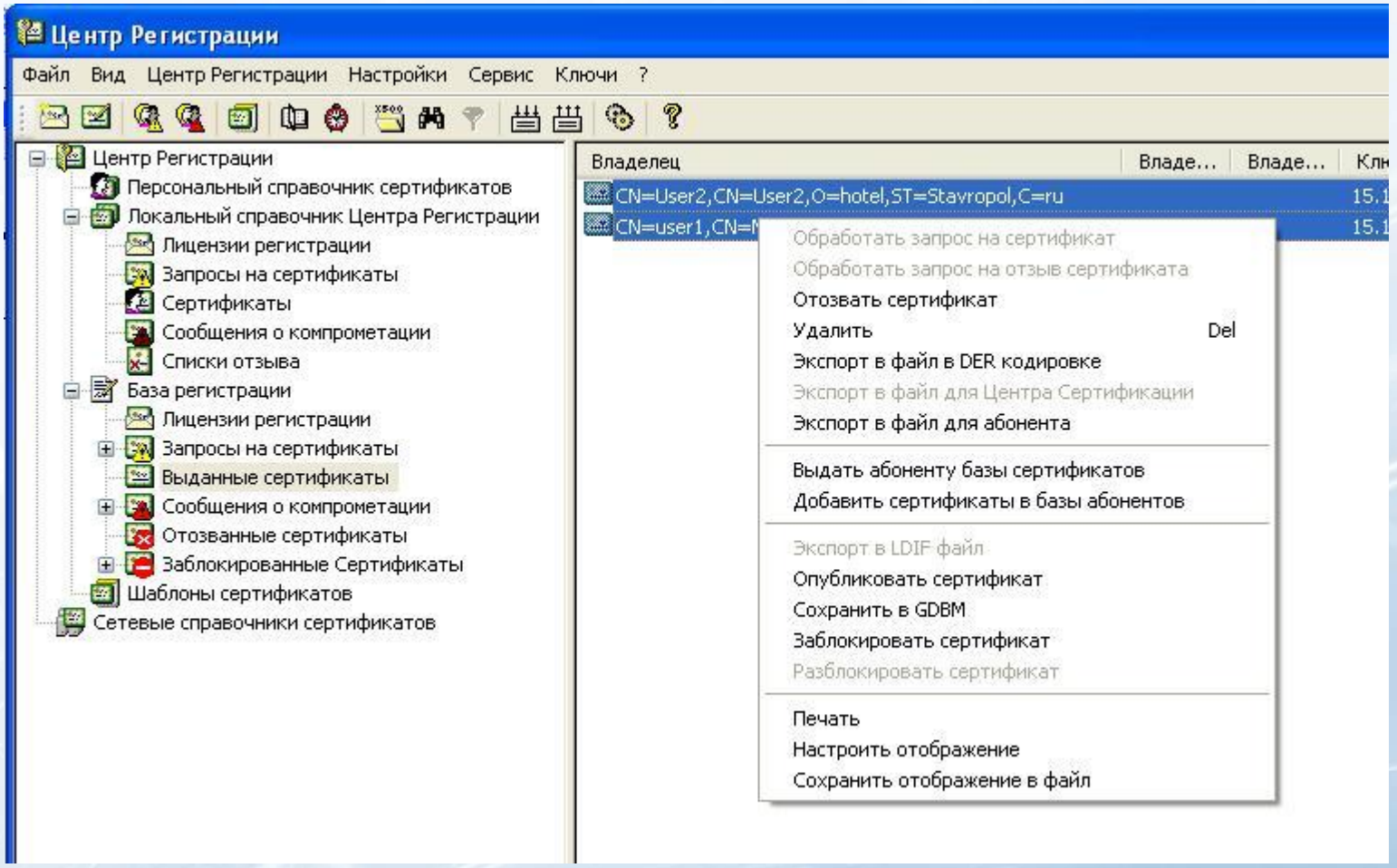
- Ключ регистрации
- Сертификат регистрации (сертификаты ЦС, ЦР и действующие СОС)
- Карточку оповещения о компрометации
- Копию заверенного бланка сертификата регистрации пользователя
- Копии заверенных бланков сертификатов ЦС и ЦР

Генерация ключей в ЦР

Пользователь получает:

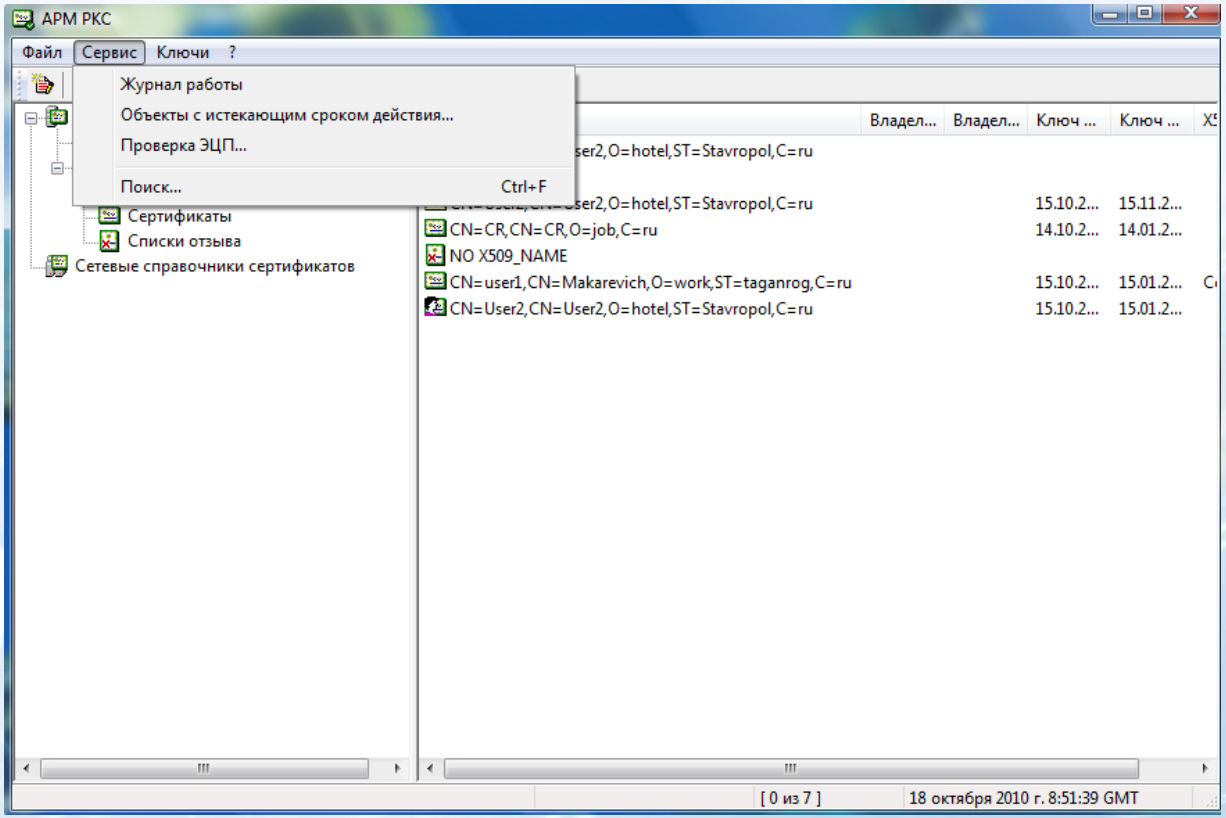
- Закрытый ключ
- Сертификат открытого ключа
- Копии справочника
- Карточку оповещения о компрометации
- Копию заверенного бланка сертификата открытого ключа
- Копии заверенных бланков сертификатов ЦС и ЦР

Создание обновлений для пользователей

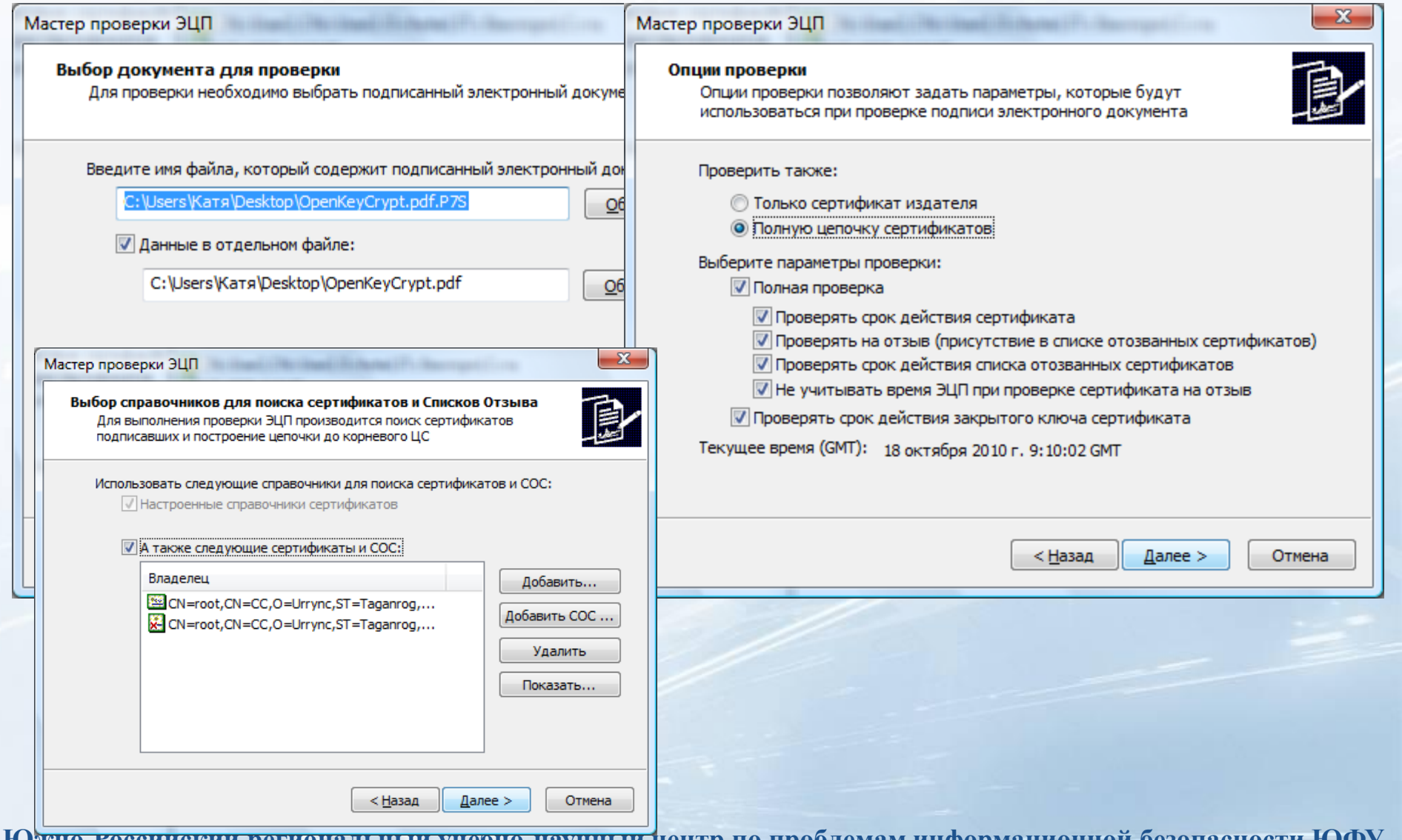


АРМ «Разбора конфликтных ситуаций»

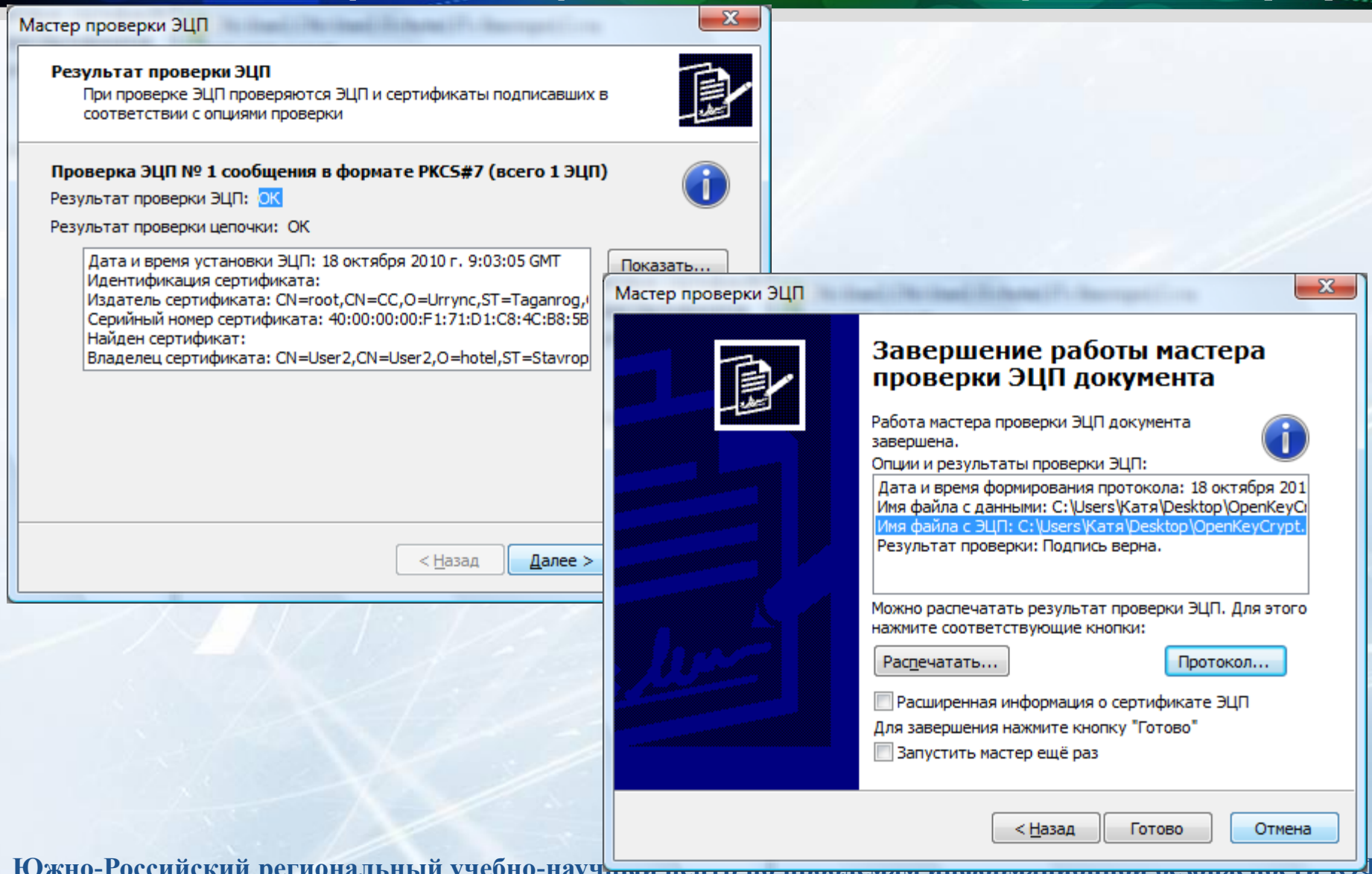
Интерфейс


АРМ РКС
Файл
Сервис
Ключи
?
Журнал работы
Объекты с истекающим сроком действия...
Проверка ЭЦП...
Поиск... Ctrl+F
Сертификаты
Списки отзыва
Сетевые справочники сертификатов
Владел...
Владел...
Ключ ...
Ключ ...
ser2,O=hotel,ST=Stavropol,C=ru
ser2,O=hotel,ST=Stavropol,C=ru
15.10.2...
15.11.2...
CN=CR,CN=CR,O=job,C=ru
14.10.2...
14.01.2...
NO X509_NAME
CN=user1,CN=Makarevich,O=work,ST=taganrog,C=ru
15.10.2...
15.01.2...
CN=User2,CN=User2,O=hotel,ST=Stavropol,C=ru
15.10.2...
15.01.2...
[0 из 7]
18 октября 2010 г. 8:51:39 GMT

Разбор конфликтной ситуации (1)



Разбор конфликтной ситуации (2)



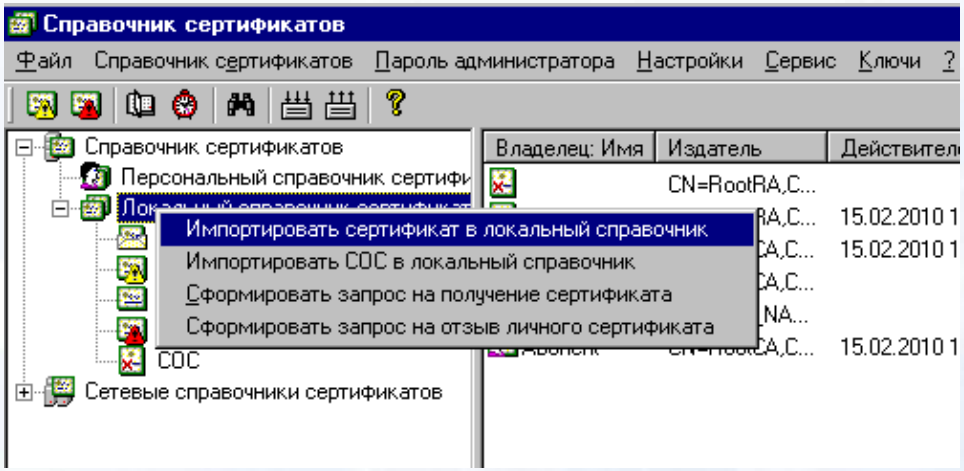
Верба-сертификат МВ Клиент

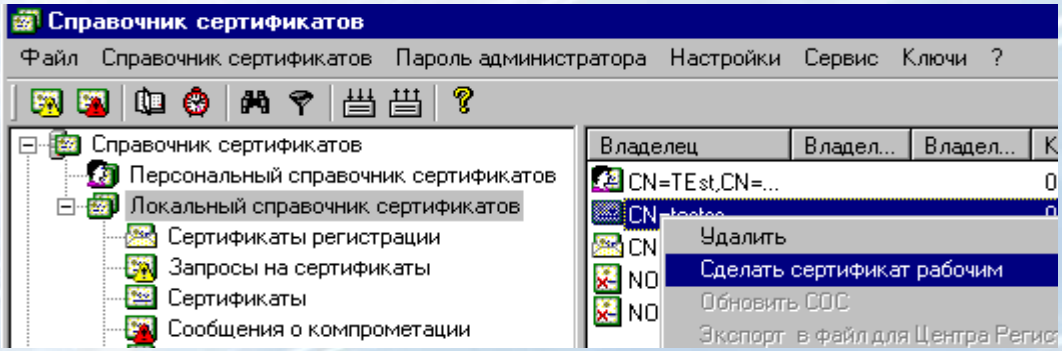
Поднятие справочника сертификатов

При первом запуске возможна настройка справочника сертификатов:

- По лицензии регистрации
- По копии баз справочника

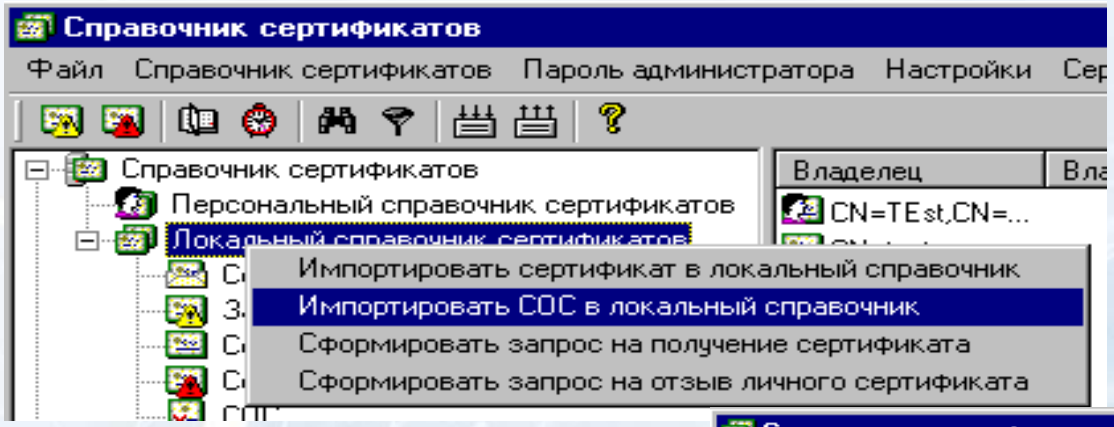
Добавление сертификата

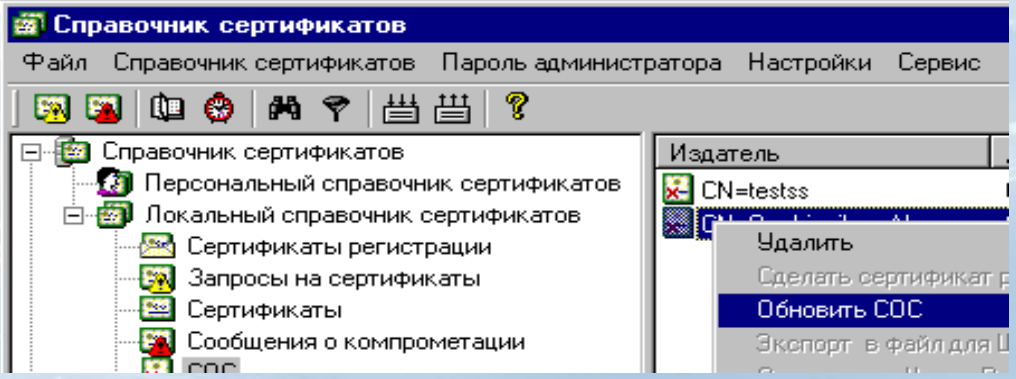




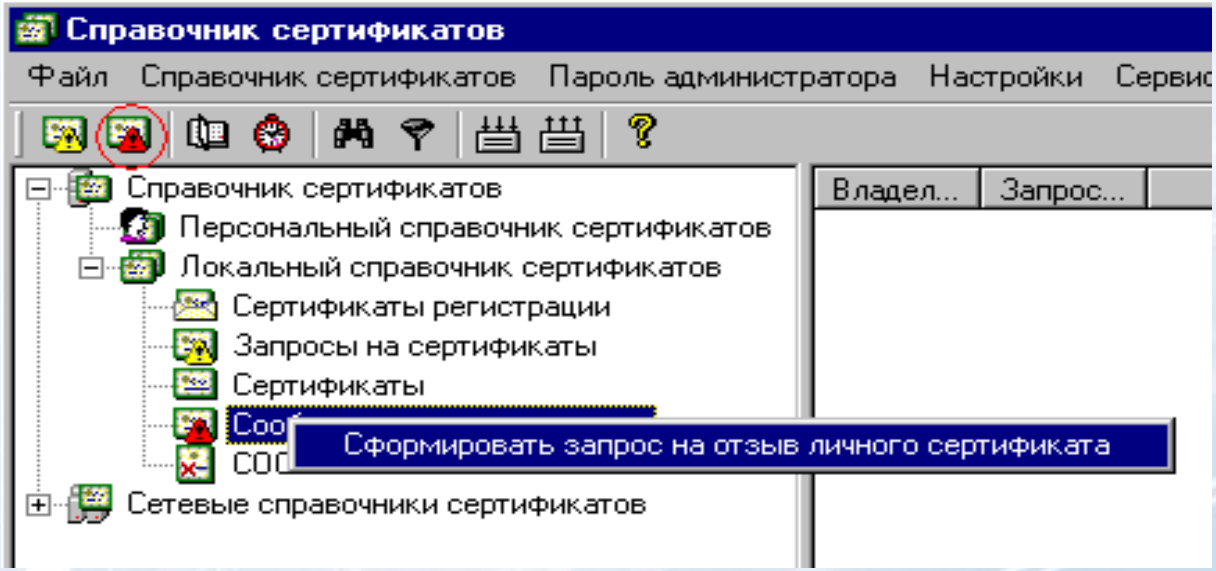
Обновление СОС

Добавление СОС из файла на внешнем носителе;
Обновление через файл с обновлениями;
Обновление СОС по сети, с использованием дополнения "**Точка распространения СОС**".



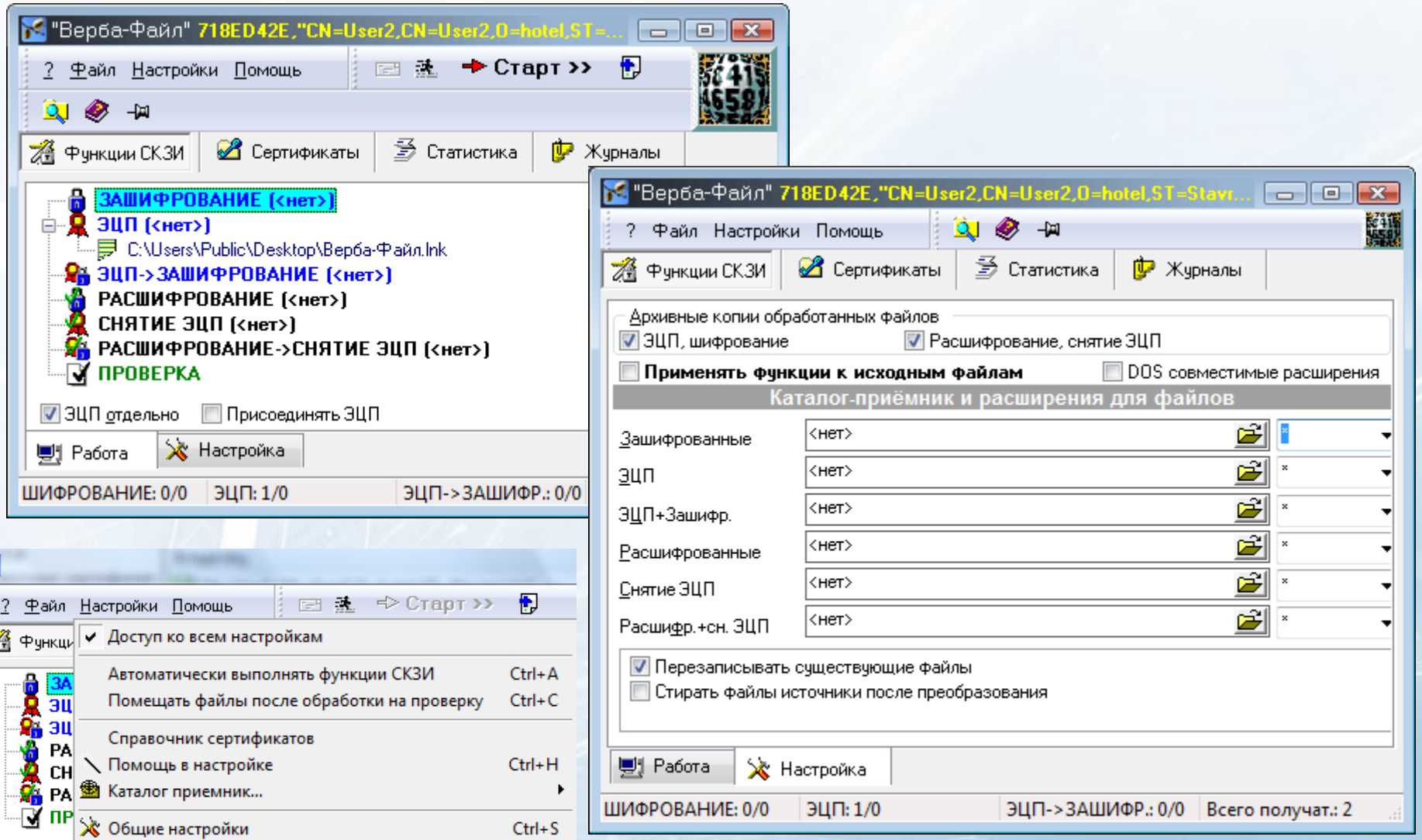


Отзыв сертификата

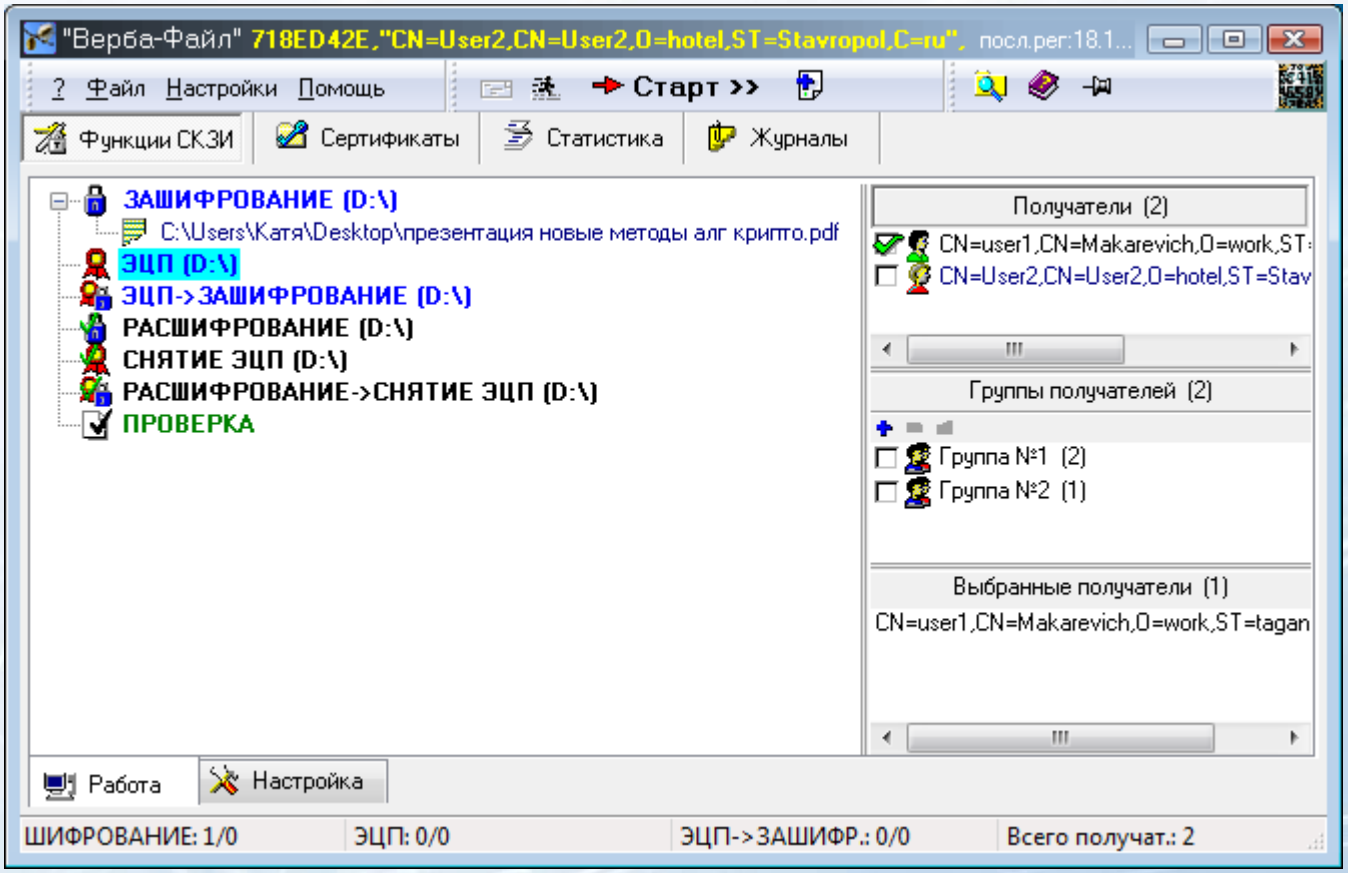


Верба-Файл

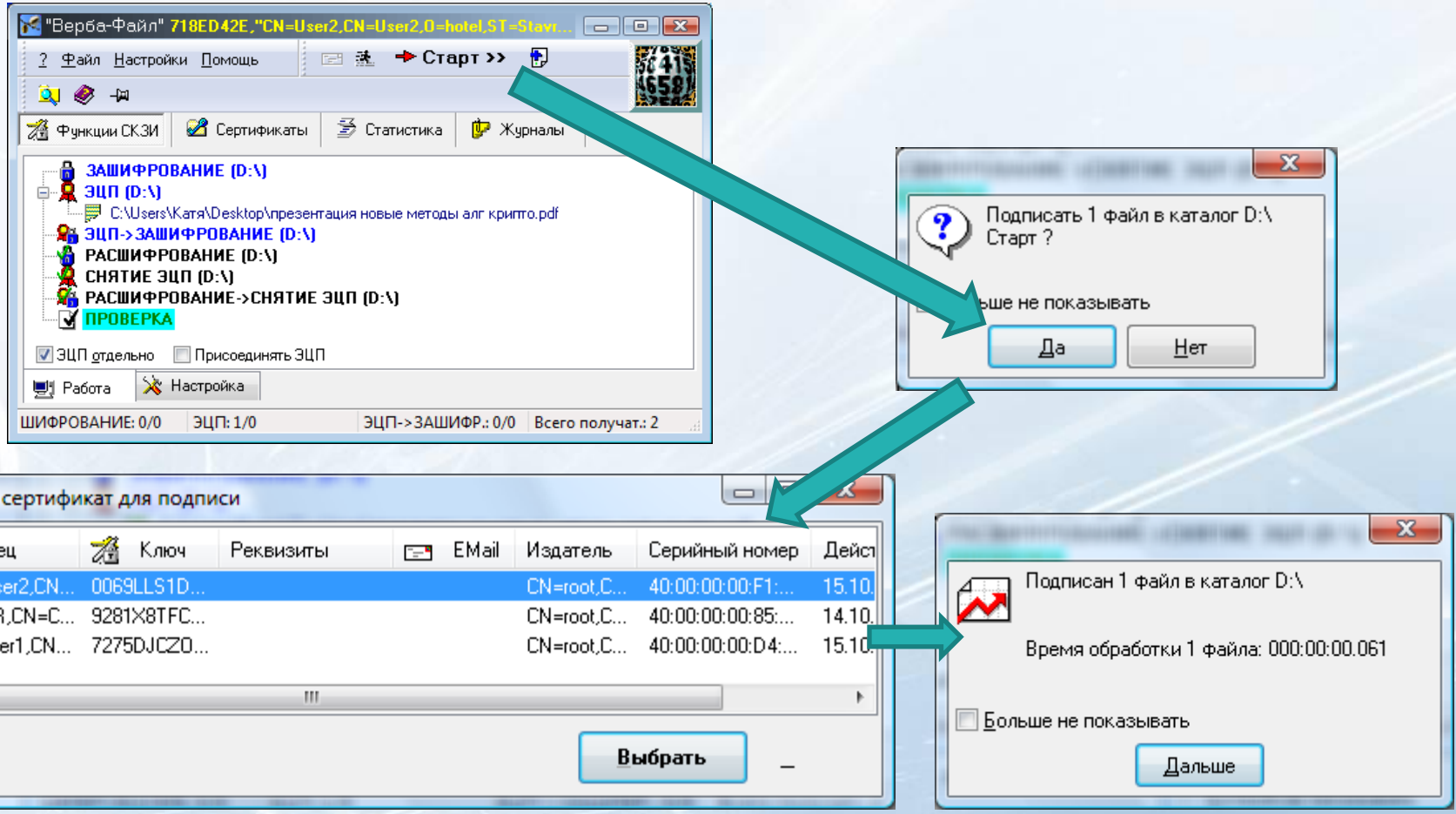
Интерфейс


"Верба-Файл" 718ED42E,"CN=User2,CN=User2,O=hotel,ST=...
Файл Настройки Помощь
Старт >>
Функции СКЗИ
Сертификаты
Статистика
Журналы
ЗАШИФРОВАНИЕ (<нет>)
ЭЦП (<нет>)
C:\Users\Public\Desktop\Верба-Файл.lnk
ЭЦП->ЗАШИФРОВАНИЕ (<нет>)
РАСШИФРОВАНИЕ (<нет>)
СНЯТИЕ ЭЦП (<нет>)
РАСШИФРОВАНИЕ->СНЯТИЕ ЭЦП (<нет>)
ПРОВЕРКА
ЭЦП отдельно
Присоединять ЭЦП
Работа
Настройка
ШИФРОВАНИЕ: 0/0
ЭЦП: 1/0
ЭЦП->ЗАШИФР.: 0/0
"Верба-Файл" 718ED42E,"CN=User2,CN=User2,O=hotel,ST=Stavr...
Архивные копии обработанных файлов
ЭЦП, шифрование
Расшифрование, снятие ЭЦП
Применять функции к исходным файлам
DOS совместимые расширения
Каталог-приёмник и расширения для файлов
Зашифрованные
ЭЦП
ЭЦП+Зашифр.
Расшифрованные
Снятие ЭЦП
Расшифр.+сн. ЭЦП
<нет>
Перезаписывать существующие файлы
Стирать файлы источники после преобразования
Всего получат.: 2
Доступ ко всем настройкам
Автоматически выполнять функции СКЗИ Ctrl+A
Помещать файлы после обработки на проверку Ctrl+C
Справочник сертификатов
Помощь в настройке Ctrl+H
Каталог приемник...
Общие настройки Ctrl+S

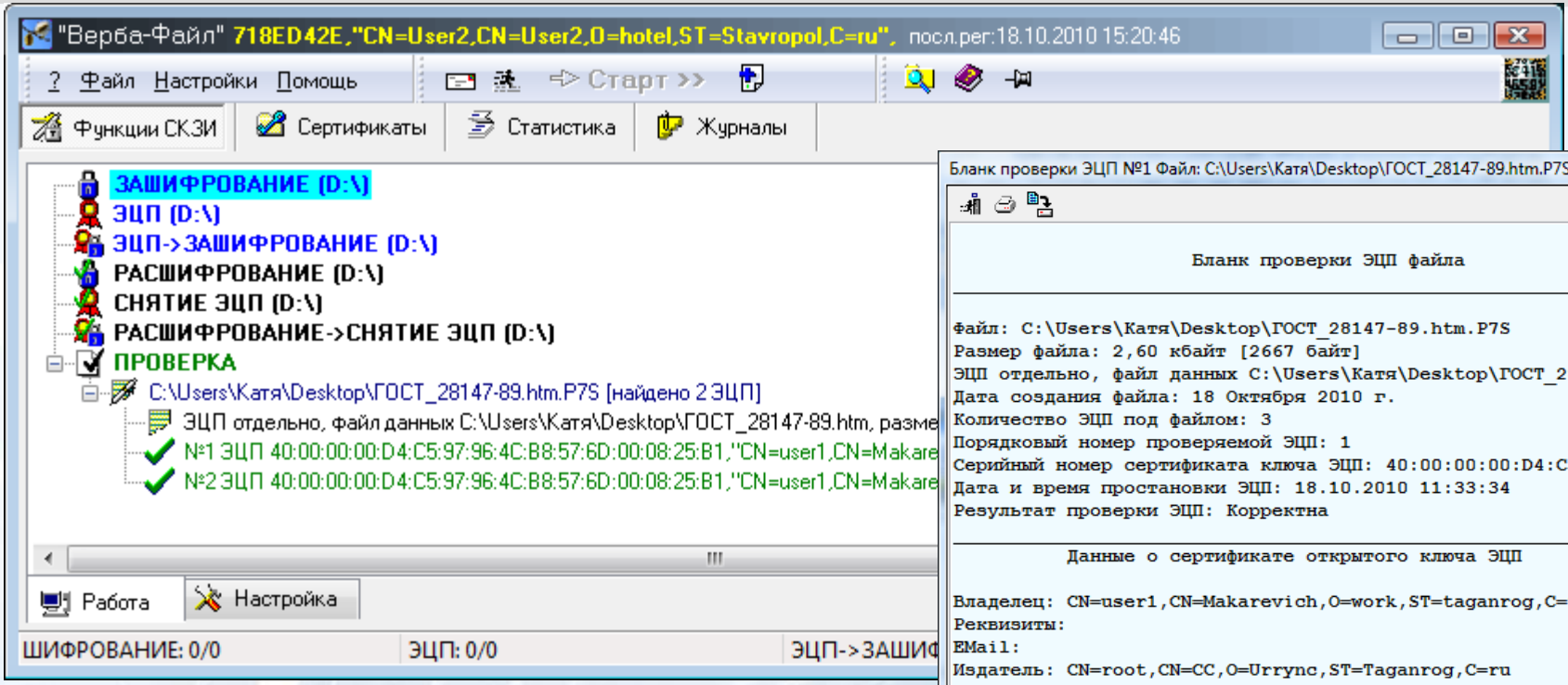
Зашифрование

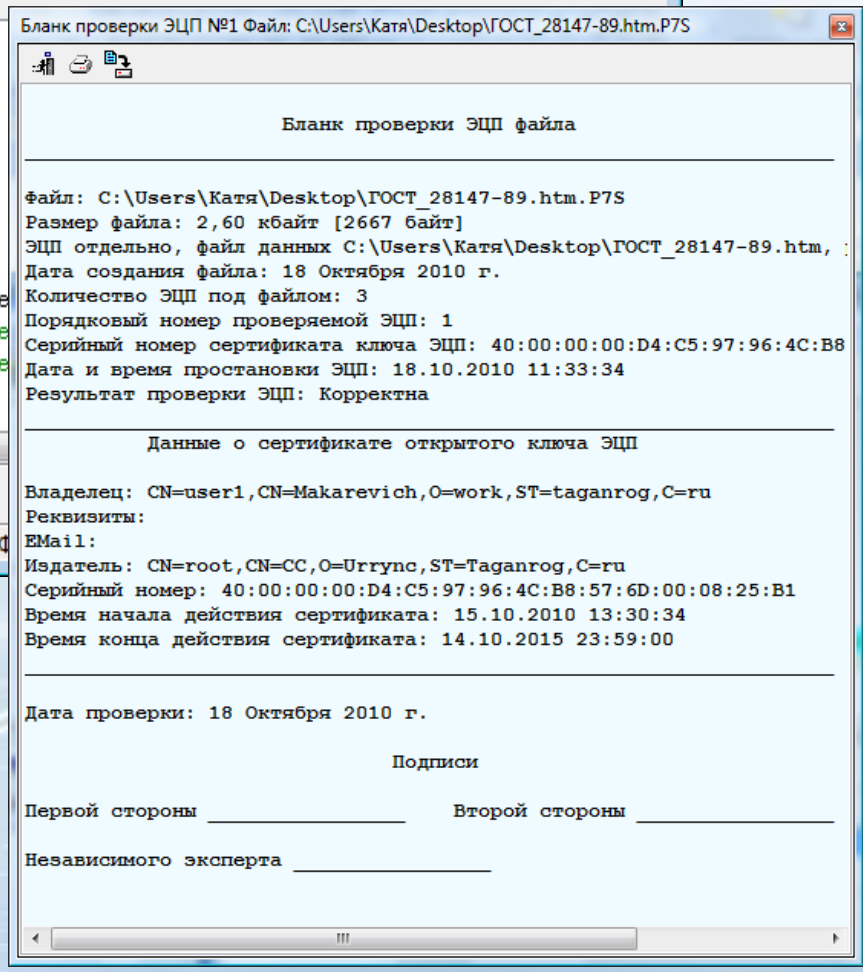


ЭЦП

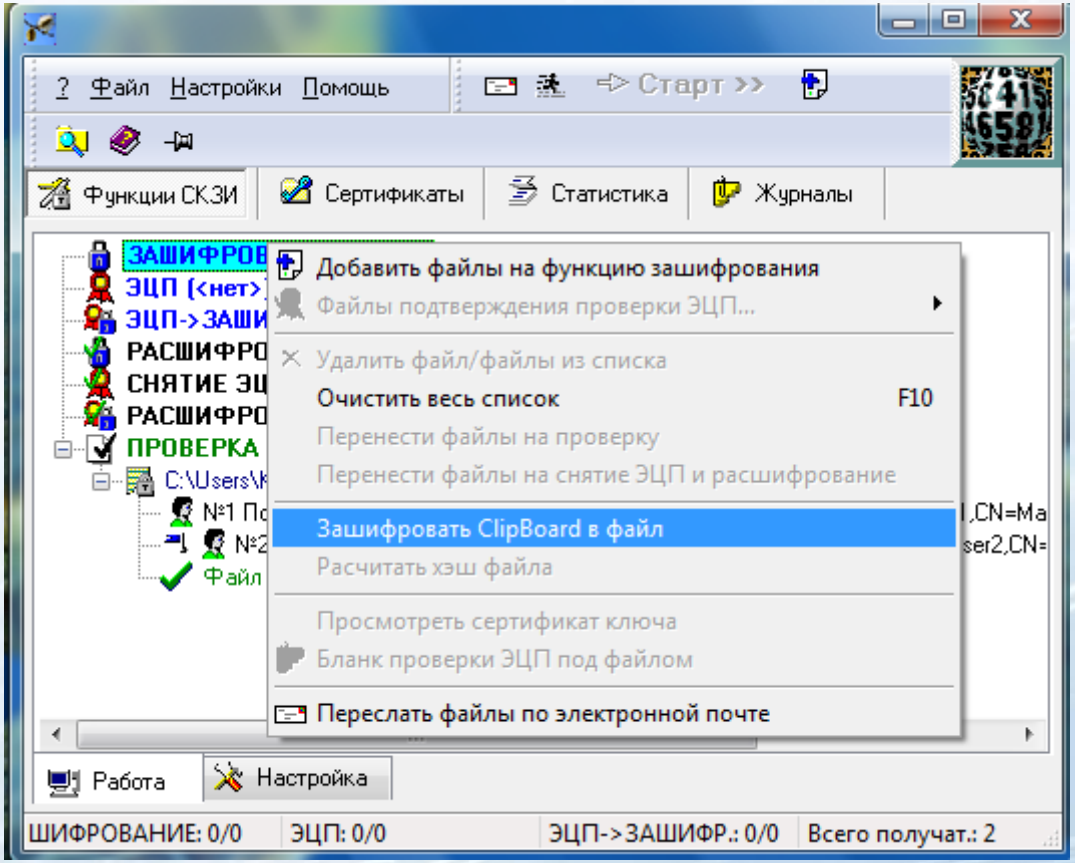

"Верба-Файл" 718ED42E,"CN=User2,CN=User2,O=hotel,ST=Stavr...
Файл Настройки Помощь
Старт >>
Функции СКЗИ
Сертификаты
Статистика
Журналы
ЗАШИФРОВАНИЕ (D:\)
ЭЦП (D:\)
C:\Users\Катя\Desktop\презентация новые методы алг крипто.pdf
ЭЦП->ЗАШИФРОВАНИЕ (D:\)
РАСШИФРОВАНИЕ (D:\)
СНЯТИЕ ЭЦП (D:\)
РАСШИФРОВАНИЕ->СНЯТИЕ ЭЦП (D:\)
ПРОВЕРКА
ЭЦП отдельно
Присоединять ЭЦП
Работа
Настройка
ШИФРОВАНИЕ: 0/0
ЭЦП: 1/0
ЭЦП->ЗАШИФР.: 0/0
Всего получат.: 2
Подписать 1 файл в каталог D:\
Старт ?
ьше не показывать
Да
Нет
Выберите сертификат для подписи
Владелец
Ключ
Реквизиты
EMail
Издатель
Серийный номер
Дейст
CN=User2,CN...
0069LLS1D...
CN=root,C...
40:00:00:00:F1:...
15.10.
CN=CR,CN=C...
9281X8TFC...
CN=root,C...
40:00:00:00:85:...
14.10.
CN=user1,CN...
7275DJCZO...
CN=root,C...
40:00:00:00:D4:...
15.10.
Выбрать
Подписан 1 файл в каталог D:\
Время обработки 1 файла: 000:00:00.061
Больше не показывать
Дальше

Проверка


"Верба-Файл" 718ED42E,"CN=User2,CN=User2,O=hotel,ST=Stavropol,C=ru", посл.рег:18.10.2010 15:20:46
Файл Настройки Помощь
Старт >>
Функции СКЗИ
Сертификаты
Статистика
Журналы
ЗАШИФРОВАНИЕ (D:\)
ЭЦП (D:\)
ЭЦП->ЗАШИФРОВАНИЕ (D:\)
РАСШИФРОВАНИЕ (D:\)
СНЯТИЕ ЭЦП (D:\)
РАСШИФРОВАНИЕ->СНЯТИЕ ЭЦП (D:\)
ПРОВЕРКА
C:\Users\Катя\Desktop\ГОСТ_28147-89.htm.P7S [найдено 2 ЭЦП]
ЭЦП отдельно, файл данных C:\Users\Катя\Desktop\ГОСТ_28147-89.htm, разме
№1 ЭЦП 40:00:00:00:D4:C5:97:96:4C:B8:57:6D:00:08:25:B1,"CN=user1,CN=Makare
№2 ЭЦП 40:00:00:00:D4:C5:97:96:4C:B8:57:6D:00:08:25:B1,"CN=user1,CN=Makare
Работа
Настройка
ШИФРОВАНИЕ: 0/0
ЭЦП: 0/0
ЭЦП->ЗАШИФ

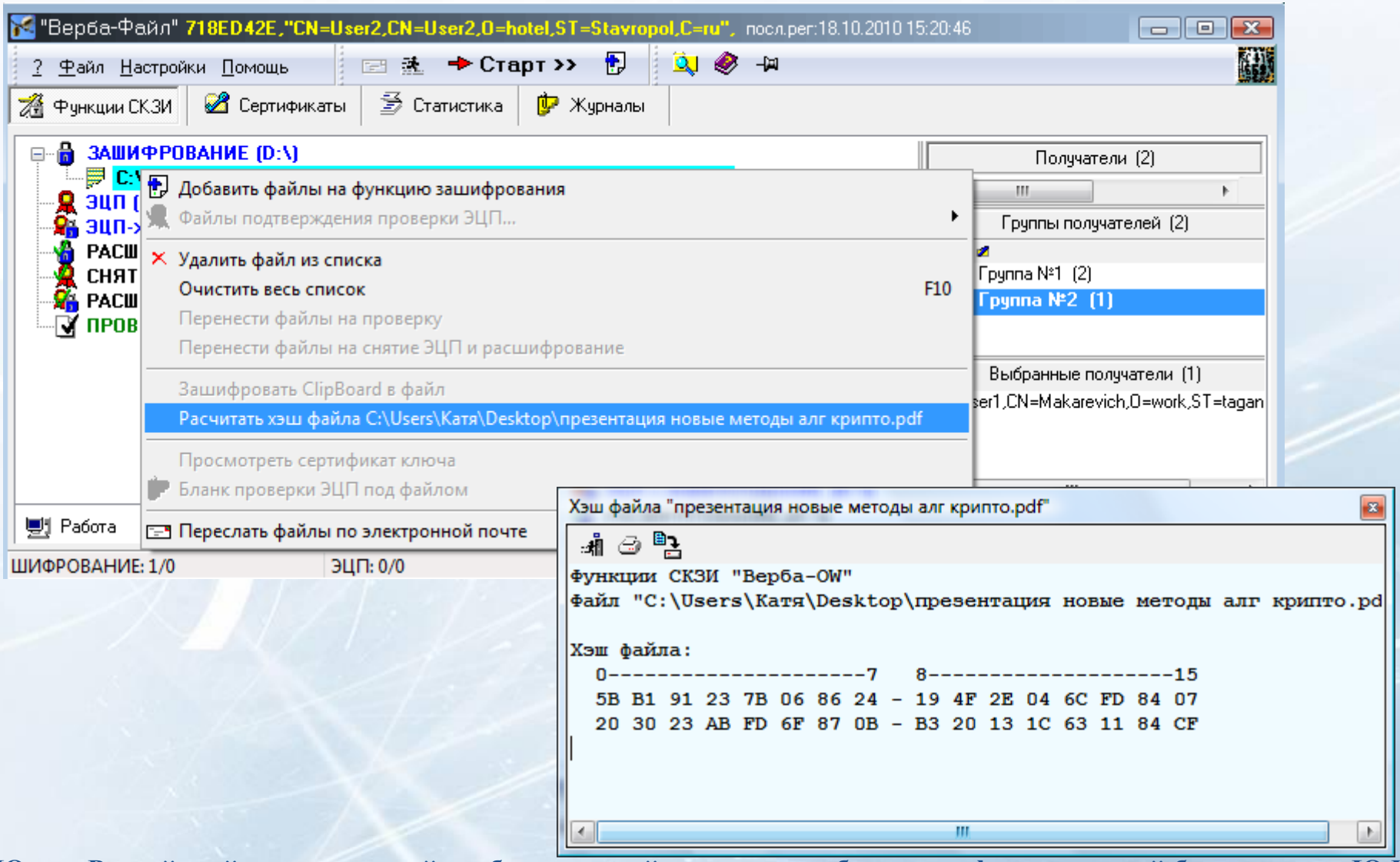

Бланк проверки ЭЦП №1 Файл: C:\Users\Катя\Desktop\ГОСТ_28147-89.htm.P7S
Бланк проверки ЭЦП файла
Файл: C:\Users\Катя\Desktop\ГОСТ_28147-89.htm.P7S
Размер файла: 2,60 кбайт [2667 байт]
ЭЦП отдельно, файл данных C:\Users\Катя\Desktop\ГОСТ_28147-89.htm,
Дата создания файла: 18 Октября 2010 г.
Количество ЭЦП под файлом: 3
Порядковый номер проверяемой ЭЦП: 1
Серийный номер сертификата ключа ЭЦП: 40:00:00:00:D4:C5:97:96:4C:B8
Дата и время простановки ЭЦП: 18.10.2010 11:33:34
Результат проверки ЭЦП: Корректна
Данные о сертификате открытого ключа ЭЦП
Владелец: CN=user1,CN=Makarevich,O=work,ST=taganrog,C=ru
Реквизиты:
EMail:
Издатель: CN=root,CN=CC,O=Urrync,ST=Taganrog,C=ru
Серийный номер: 40:00:00:00:D4:C5:97:96:4C:B8:57:6D:00:08:25:B1
Время начала действия сертификата: 15.10.2010 13:30:34
Время конца действия сертификата: 14.10.2015 23:59:00
Дата проверки: 18 Октября 2010 г.
Подписи
Первой стороны _____ Второй стороны _____
Независимого эксперта _____

Шифрование содержимого буфера

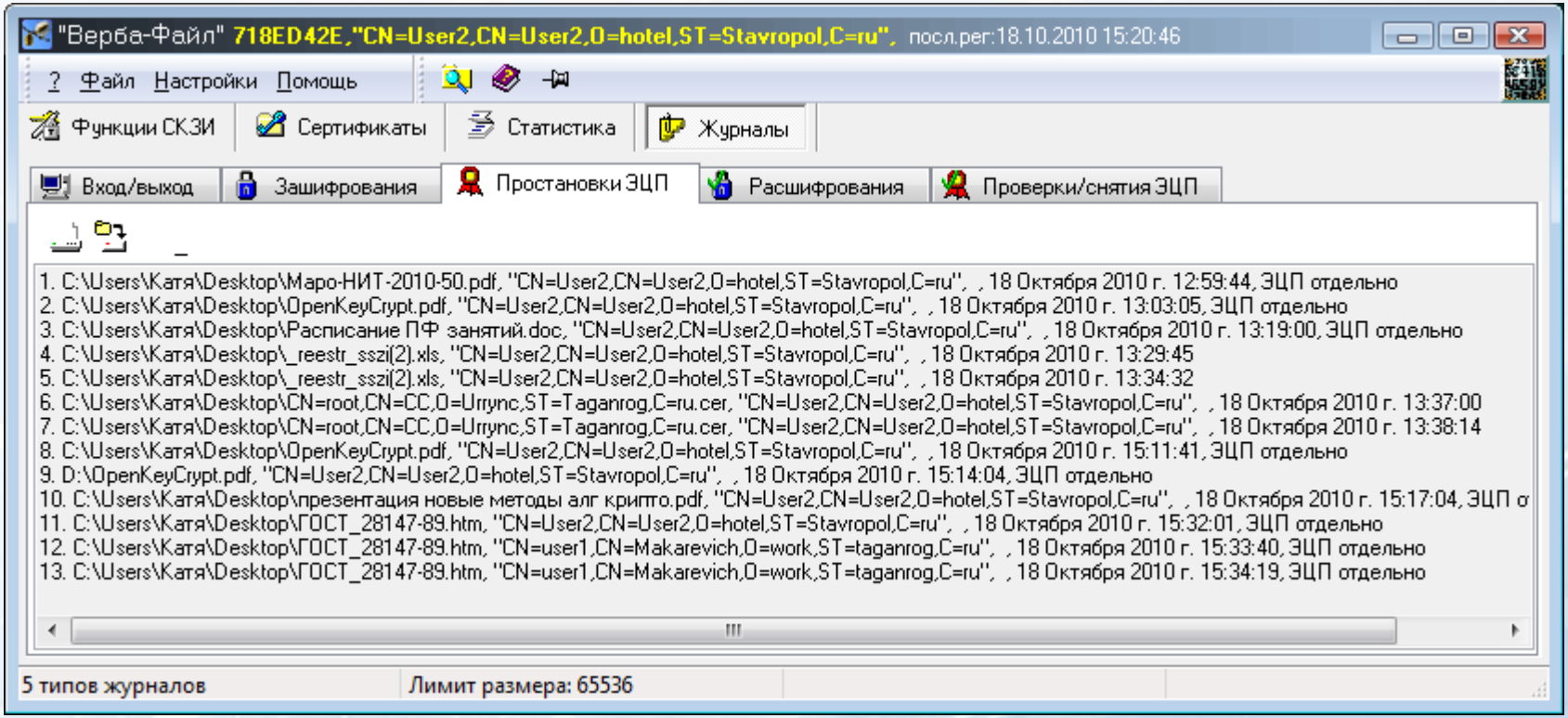


ClipBoard.clp

Вычисление ХЭШ



Протоколирование



C:\«пользователь»\AppData\Roaming\MDPREI\Verba-File\JOU

Обработка командных скриптов

Команды:

TO <список ключей> — установить получателей зашифрованного файла

CRYPT <имя файла> или **ENCRYPT <имя файла>** — зашифровать файл

SIGN <имя файла> — подписать файл;

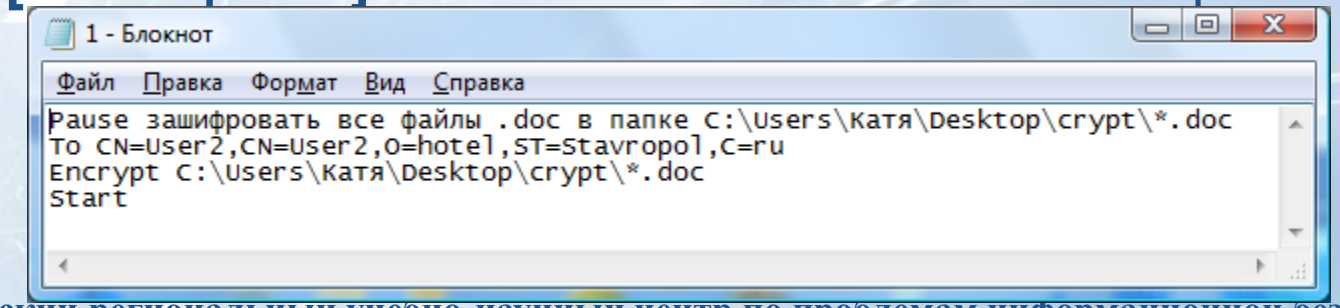
UNCRYPT <имя файла> или **DECRYPT <имя файла>** — расшифровать файл

UNSIGN <имя файла> — снять ЭЦП с файла с проверкой

START или **BEGIN** — начать процесс обработки

EXIT или **CLOSE** — закрыть программу

PAUSE [сообщение] — остановить выполнение скрипта



Вопросы?

Южно-Российский региональный учебно-научный центр по проблемам информационной безопасности ЮФУ