



Работа с контейнерами ключей в ПО Крипто-Про CSP 3.6

Данное руководство содержит в себе три раздела:

Раздел 1. Копирование ключевых контейнеров. ([стр. 2](#))

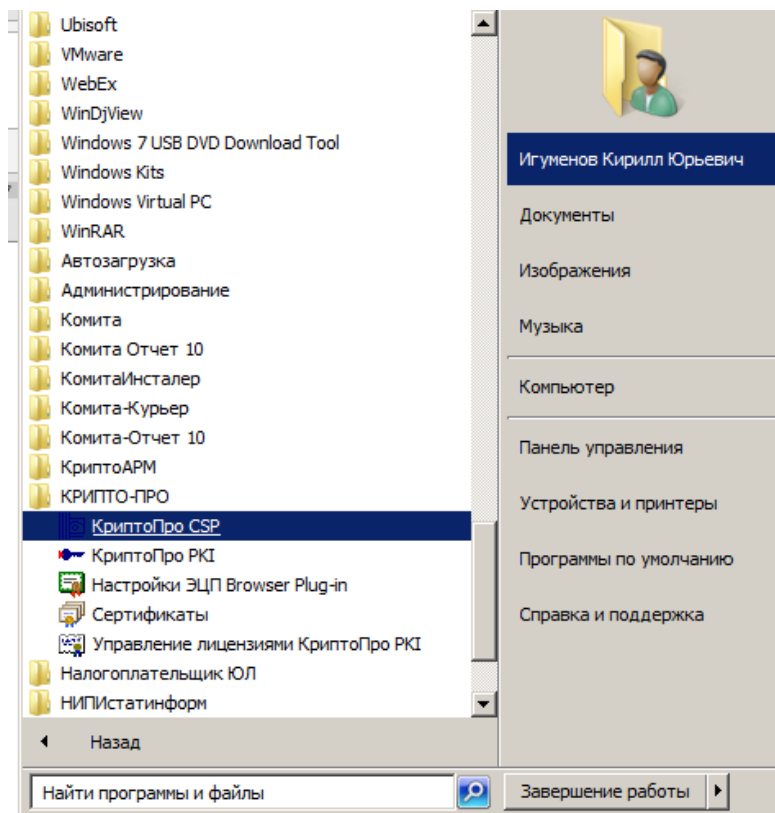
Раздел 2. Установка сертификата открытого ключа шифрования из контейнера. ([стр. 8](#))

Раздел 3. Рекомендации и пояснения по использованию контейнеров ключей шифрования в работе с программными комплексами «Комита-Отчет 10» и «Комита Курьер JE» ([стр. 11](#))

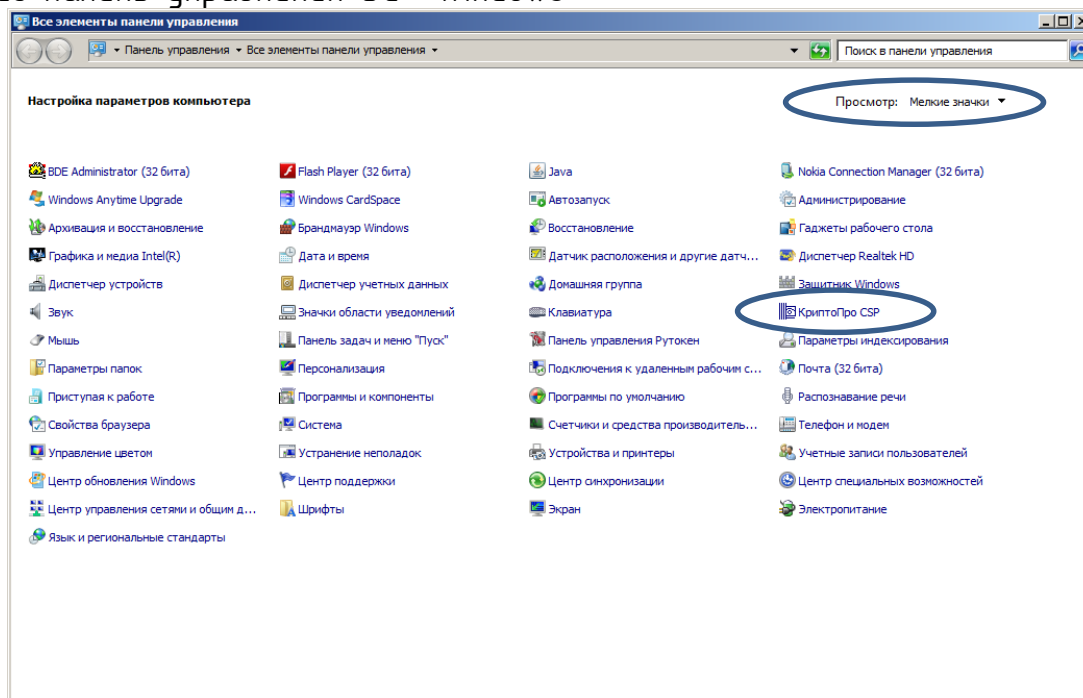
Раздел 1. Копирование ключевых контейнеров.

1. Запускаем Крипто-Про CSP 3.6 Сделать это можно несколькими способами:

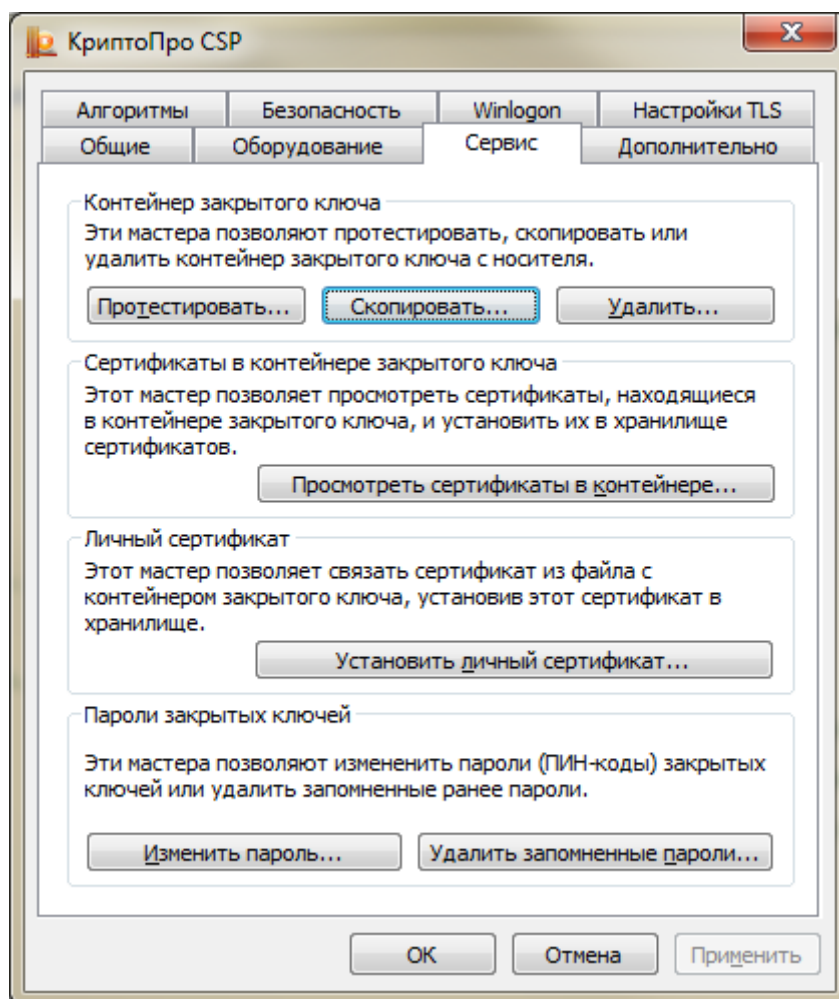
А) Через меню «Все программы» ОС Windows



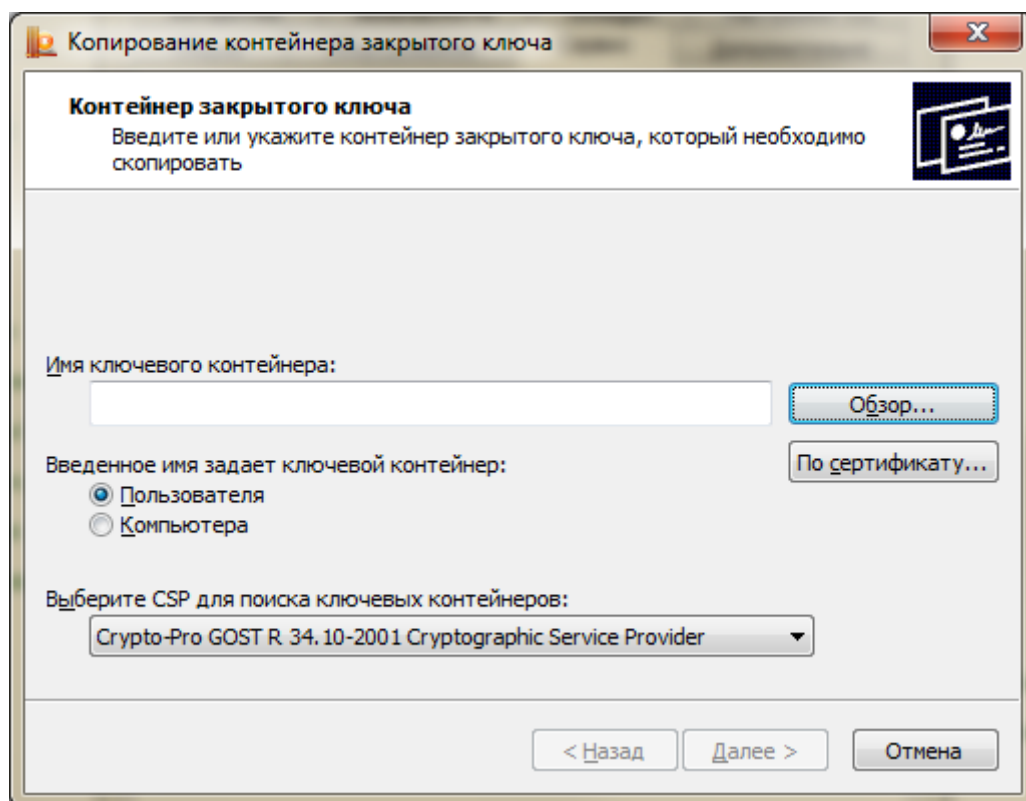
Б) Через панель управления ОС «Windows»



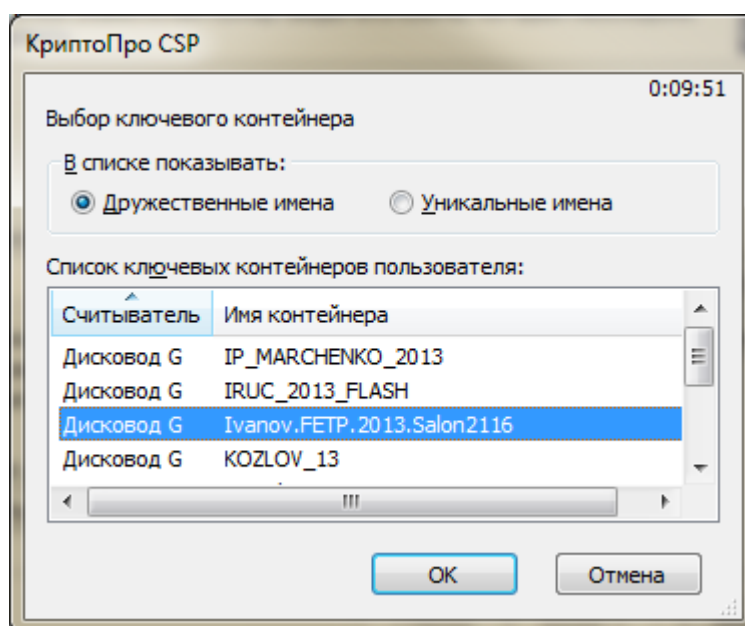
2. Для копирования контейнеров переходим на вкладку «Сервис» и нажимаем кнопку «Скопировать» (название и вид кнопок может отличаться в разных версиях)



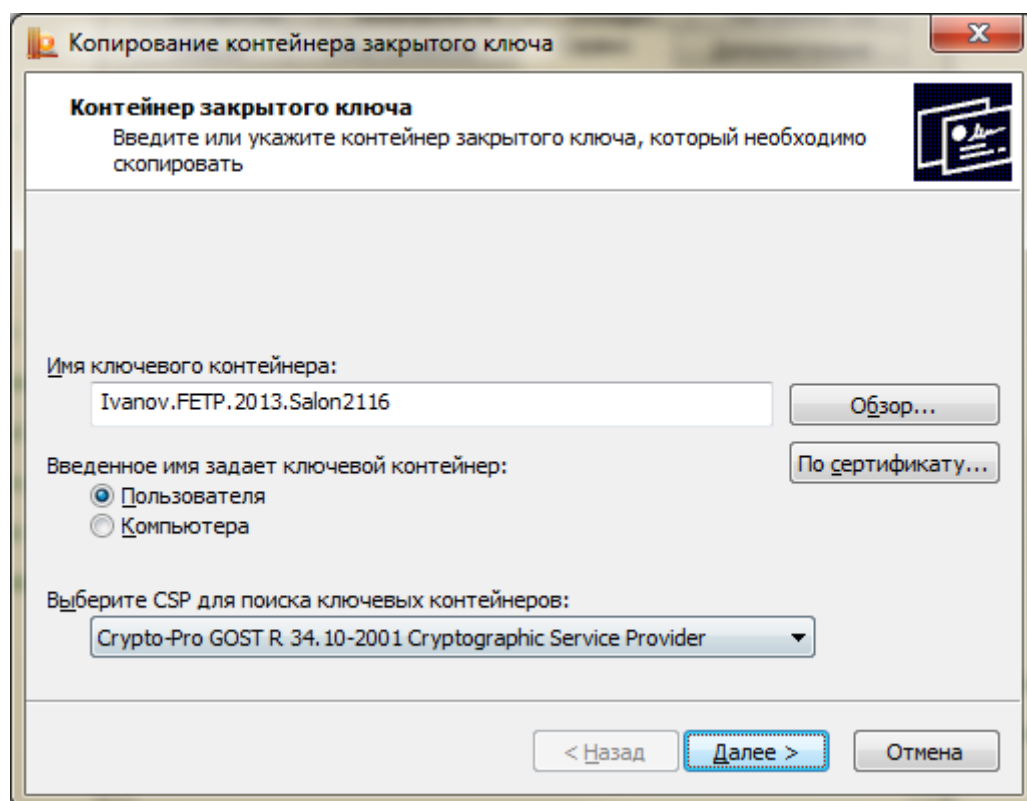
3. Открывается диалоговое окно «Копирование контейнера закрытого ключа».



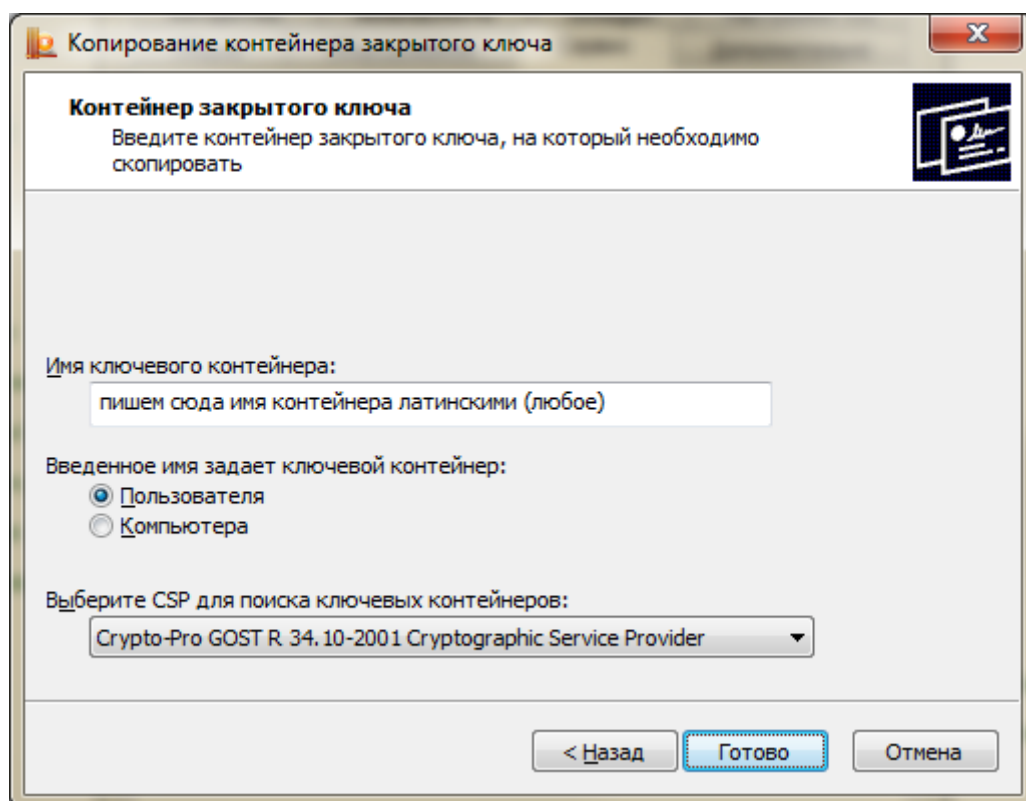
4. Нажимаем кнопку «Обзор» и выбираем контейнер, который хотим скопировать



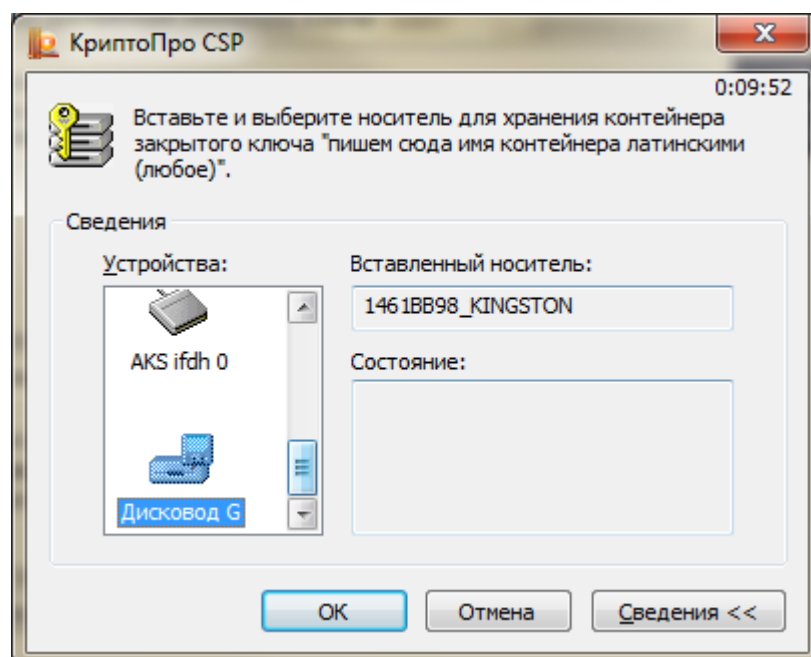
5. Выделяем контейнер и нажимаем кнопку «ОК», после этого заполняется имя ключевого контейнера в окне «Копирование закрытого ключа». Нажимаем кнопку «Далее»



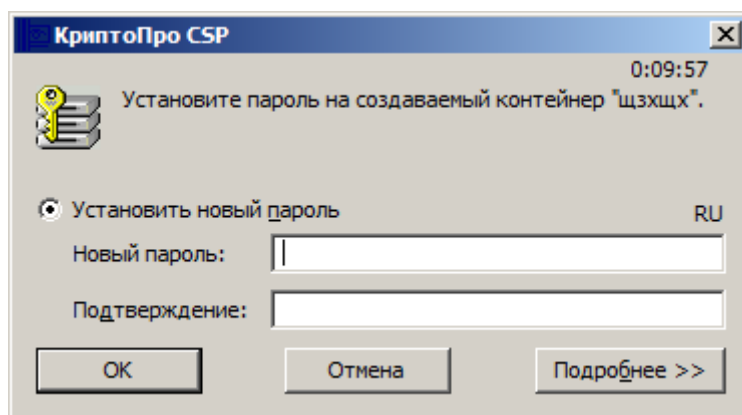
6. В следующем окне вводим имя, под которым будет создан новый ключевой контейнер. Имя может состоять из символов русского и английского алфавитов, а также цифр и специальных знаков. После ввода имени нажимаем кнопку «Готово»



7. Появляется окно выбора носителя для хранения контейнера. Для копирования контейнера «на компьютер», выбираем носитель «Реестр» (должен быть установлен в считывателях). После выбора носителя, нажимаем кнопку «OK»

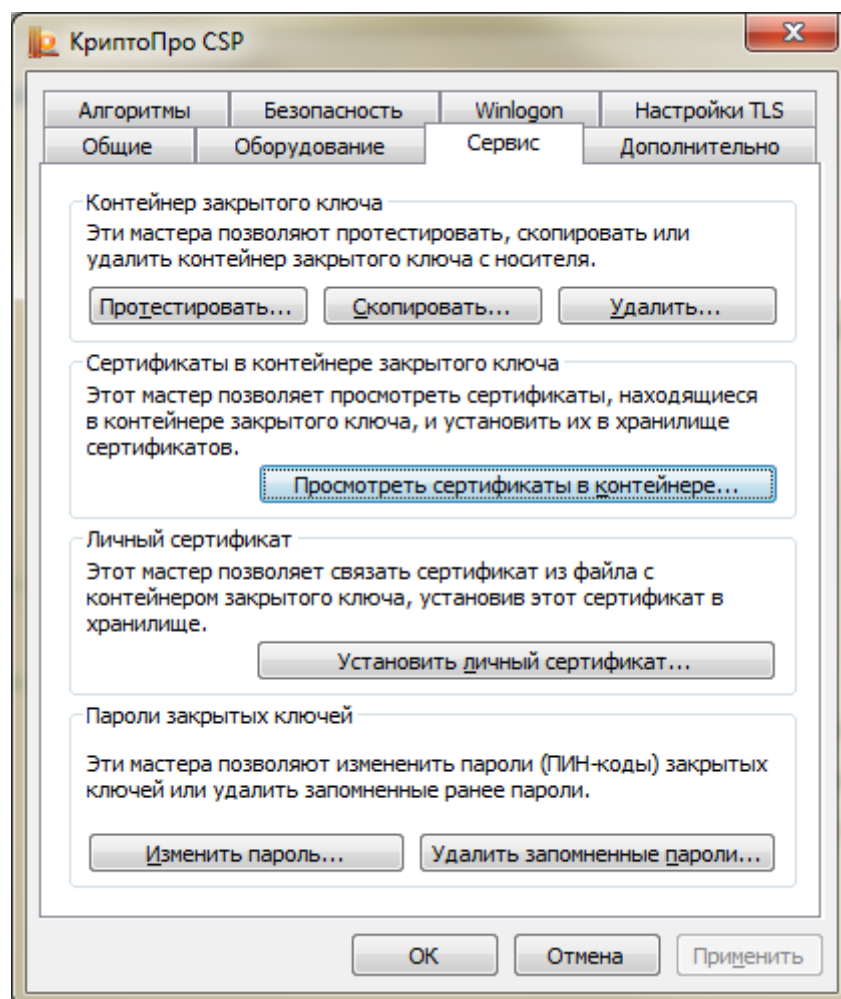


8. Появляется окно с предложением установить пароль на контейнер. При создании пароля, во время каждого обращения к контейнеру будет запрашиваться его ввод. Если создавать пароль не нужно, оставляем все поля пустыми и нажимаем кнопку «OK»

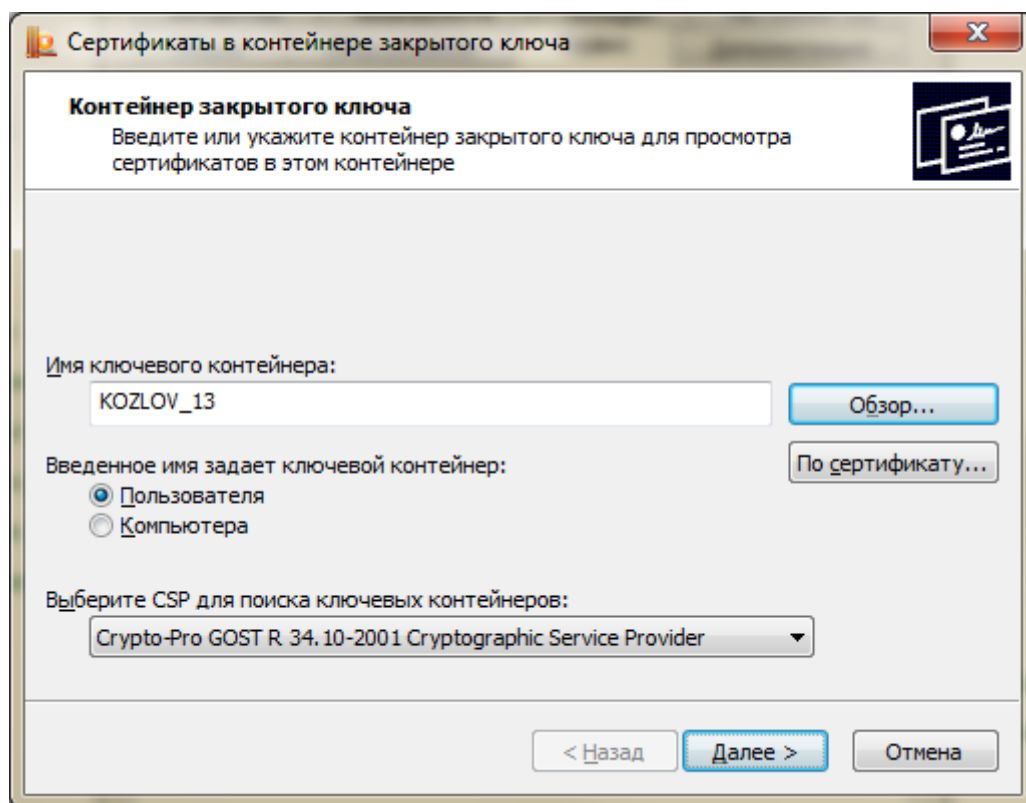


Раздел 2. Установка сертификата открытого ключа шифрования из контейнера.

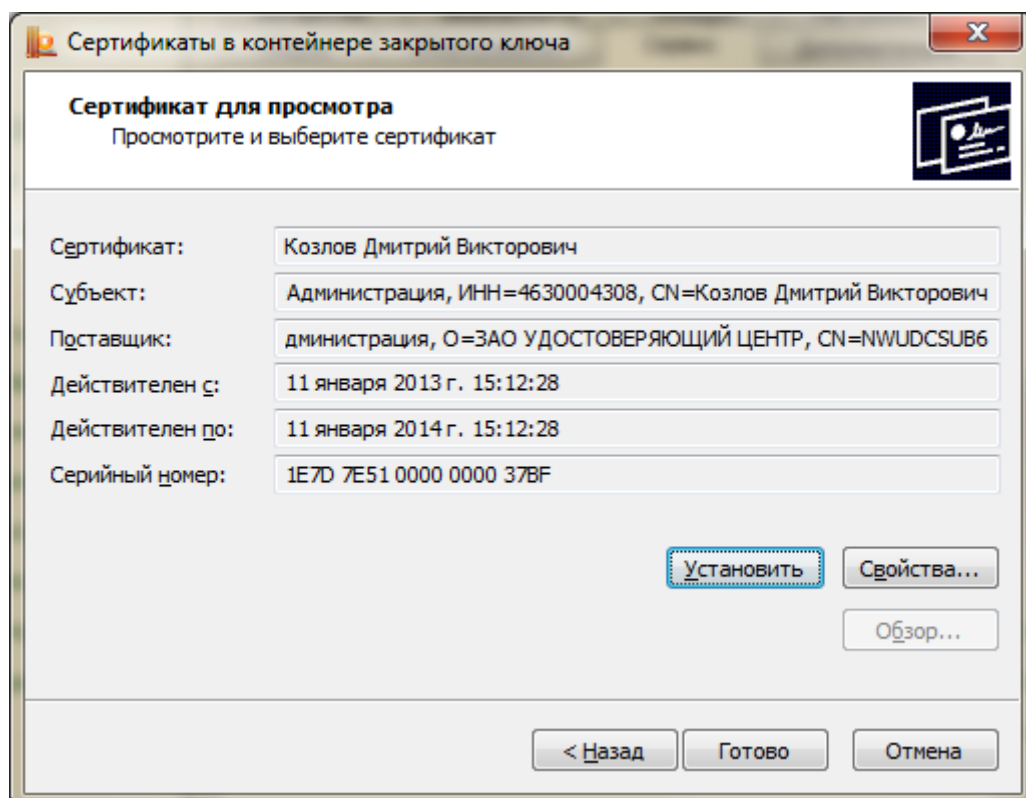
1. Запускаем Крипто-Про CSP 3.6 (см стр. №1)
2. Переходим на вкладку «Сервис», нажимаем кнопку «Просмотреть сертификаты в контейнере. . .»



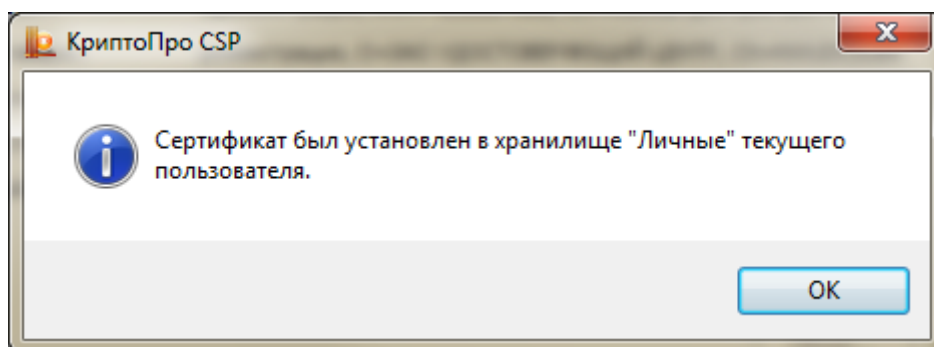
3. Нажимаем кнопку «Обзор» и выбираем необходимый нам контейнер. Нажимаем кнопку «Далее»



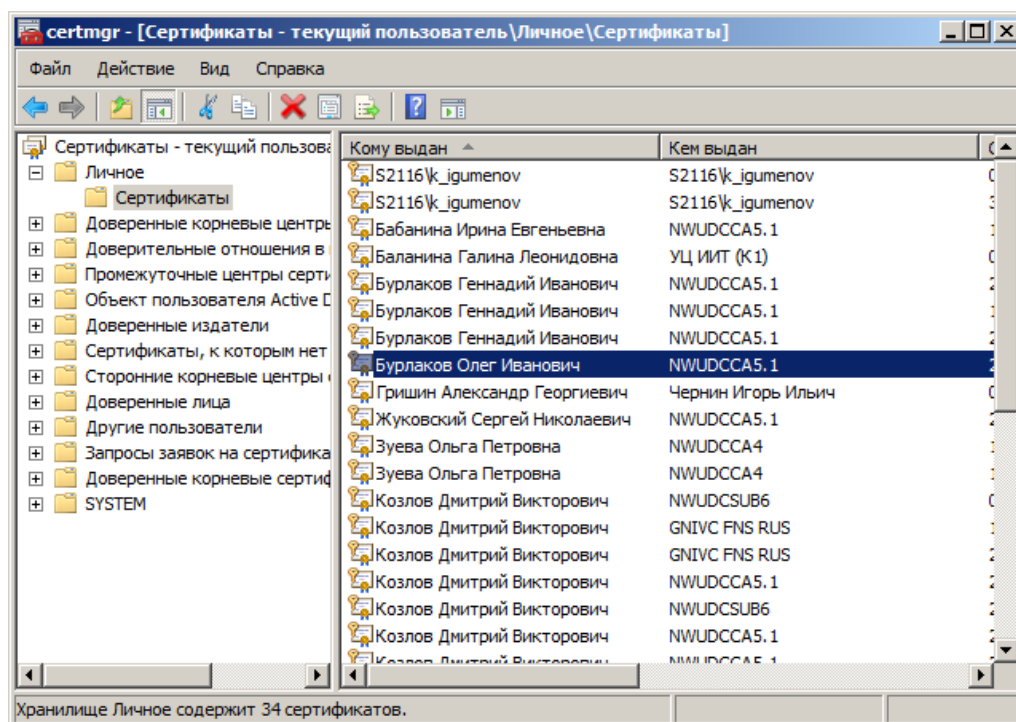
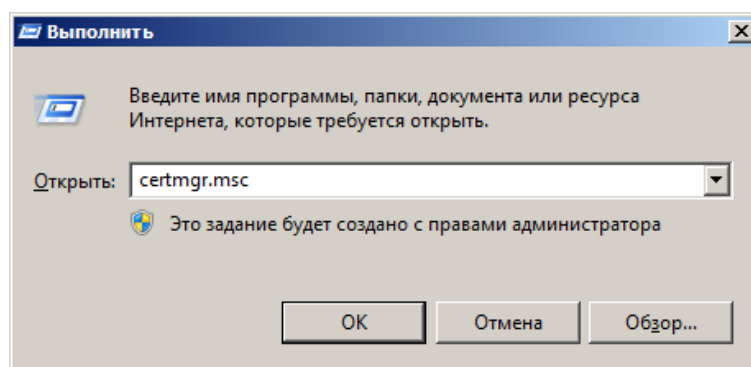
4. Появляется окно с предварительной информацией о сертификате. Нажимаем кнопку «Установить».



5. Появляется следующее окно, говорящее об установке сертификата в хранилище «Личные»



6. Хранилище сертификатов в ОС «Windows» можно просмотреть, запустив оснастку консоли MMC «Менеджер сертификатов». Для этого запускаем программу «Выполнить» (комбинация клавиш  + «R») и вводим там команду certmgr.msc



Раздел 3. Рекомендации и пояснения по использованию контейнеров ключей шифрования в работе с программными комплексами «Комита-Отчет 10» и «Комита Курьер JE»

Для работы процедур шифрования и подписи в ПК «Комита-Отчет 10» и ПК «Комита Курьер JE» в хранилище сертификатов «Личные» ОС «Windows» должен быть установлен сертификат пользователя со ссылкой на закрытый ключ. Иными словами, он должен быть установлен из ключевого носителя, с помощью которого будут производиться эти процедуры. Появляются два варианта использования носителей: «Внешний» и «Внутренний».

Под «внешним» носителем подразумеваются физические устройства (флешки, eToken, РуToken, магнитные диски). Соответственно, во время процессов шифрования и подписи этот носитель должен быть подключен к компьютеру.

Под «внутренним» носителем подразумевается реестр компьютера. Этот носитель будет всегда подключен к компьютеру, так как является неотъемлемой частью ОС «Windows». Выбор способа организации работы программных комплексов остается у пользователя.

Следует помнить: **НЕОБХОДИМО ХРАНИТЬ КОПИЮ КОНТЕЙНЕРА КЛЮЧЕЙ ШИФРОВАНИЯ НА ФИЗИЧЕСКОМ НОСИТЕЛЕ!** В случае переустановки ОС или иных ситуаций, влекущих за собой удаление контейнеров с компьютера, ключевую информацию можно будет легко восстановить. ООО «Салон 2116 – электронный почтамт» не хранит у себя закрытые ключи! Ответственность за сохранность лежит на владельце ключа. Так же, для обеспечения надежной защиты контейнеров ключей, ООО «Салон 2116 – электронный почтамт» рекомендует использовать специализированные устройства РуToken или EToken.

Для получения подробной информации о принципах работы используемой криптосистемы с открытым ключом, можно перейти по следующей ссылке:

http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC