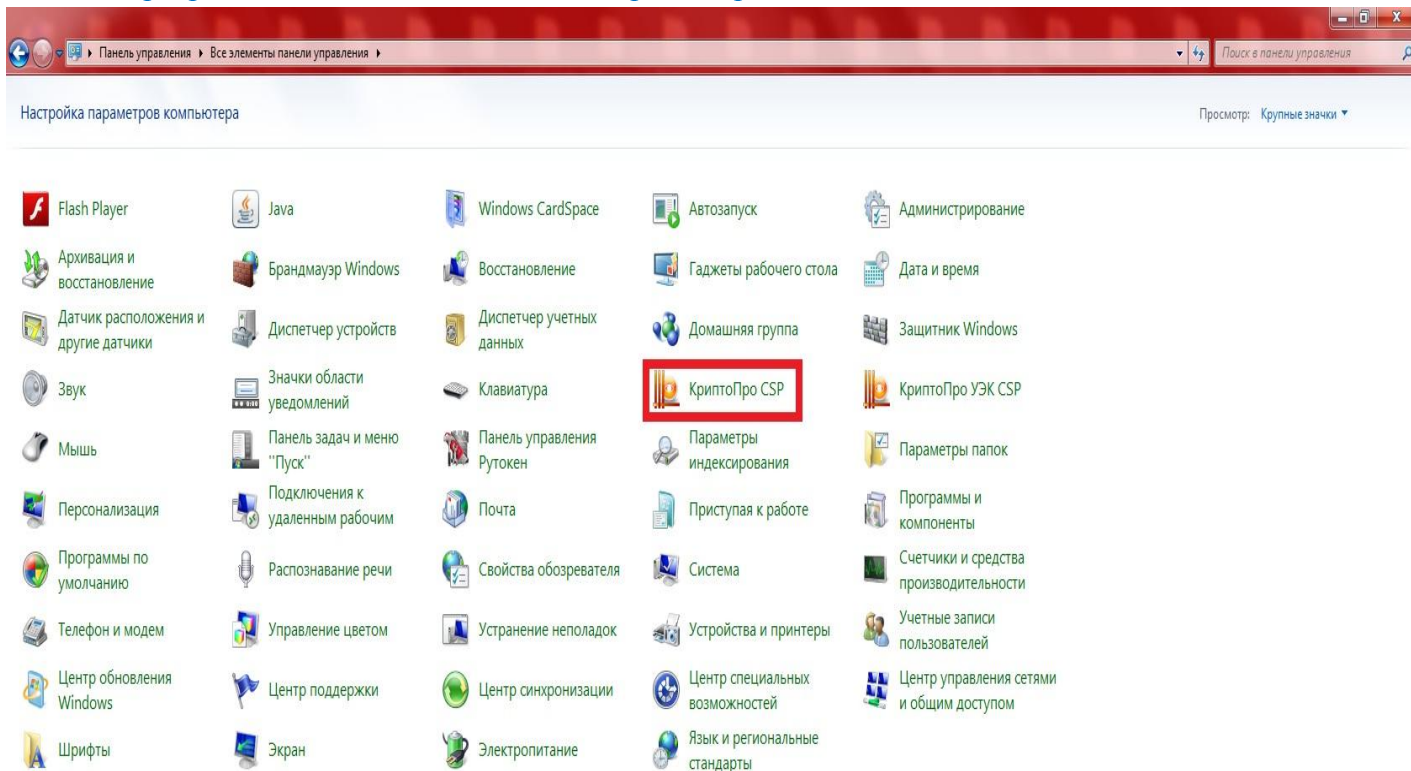
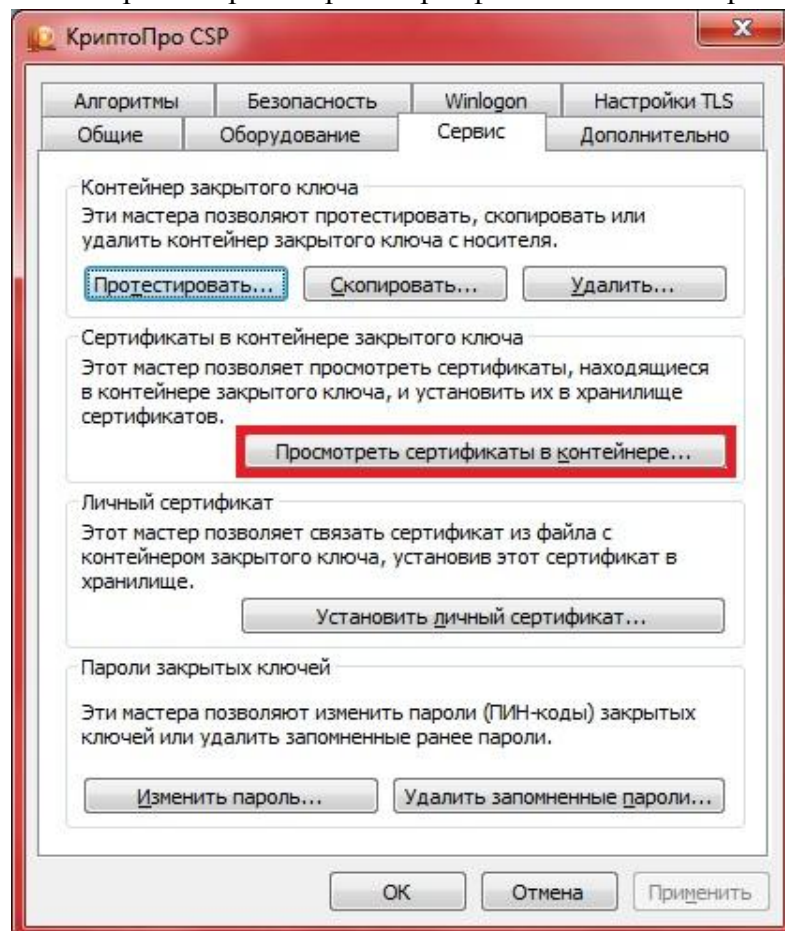


Для экспорта сертификата ключа проверки электронной подписи (далее сертификат КПЭП) с ключевого носителя (Rutoken, e-Token, «Флешка») в формате «*.cer» необходимо:

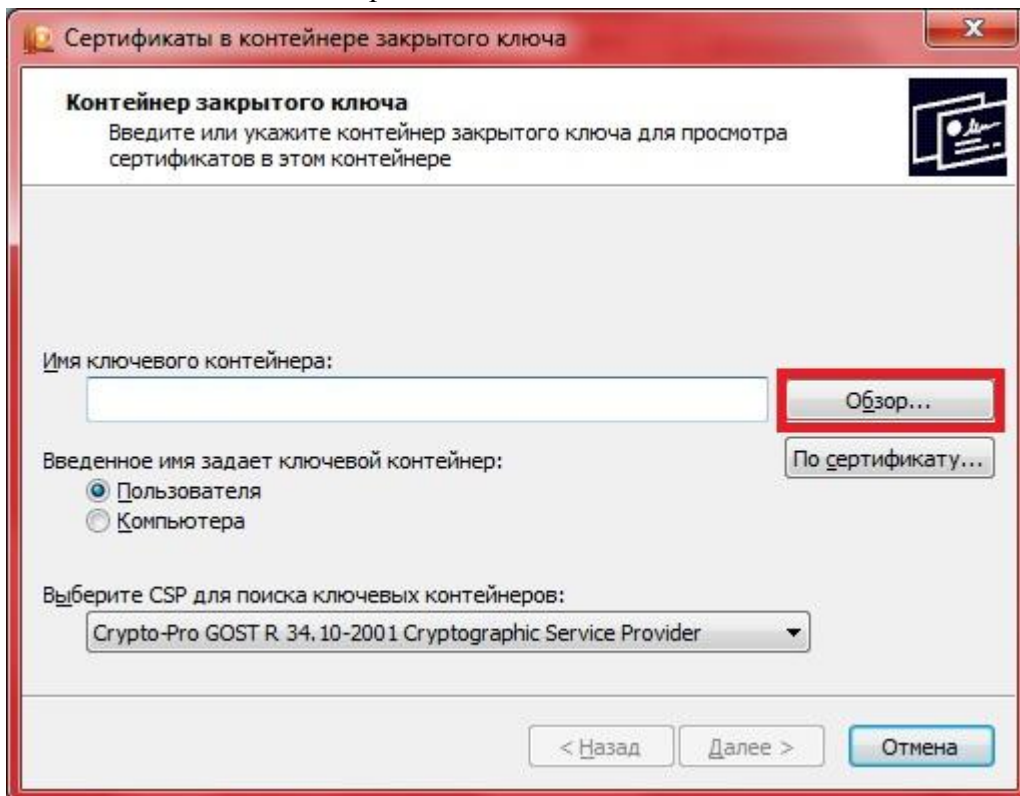
- 1) Открыть КриптоПро CSP: <Пуск> - <Панель управления> - <КриптоПро CSP> либо <Пуск> - <Все программы> - <КРИПТО-ПРО> - <КриптоПро CSP>:



- 2) Во вкладке «Сервис» выбрать «Просмотреть сертификаты в контейнере...»:

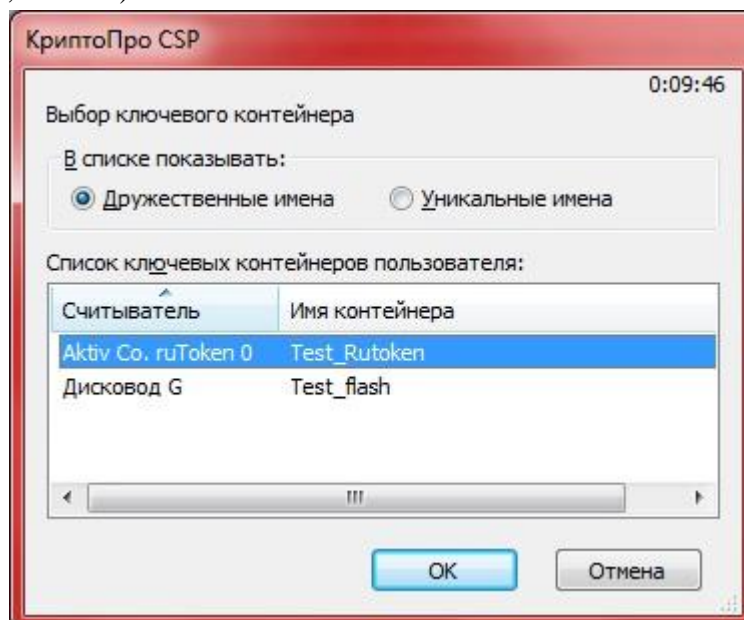


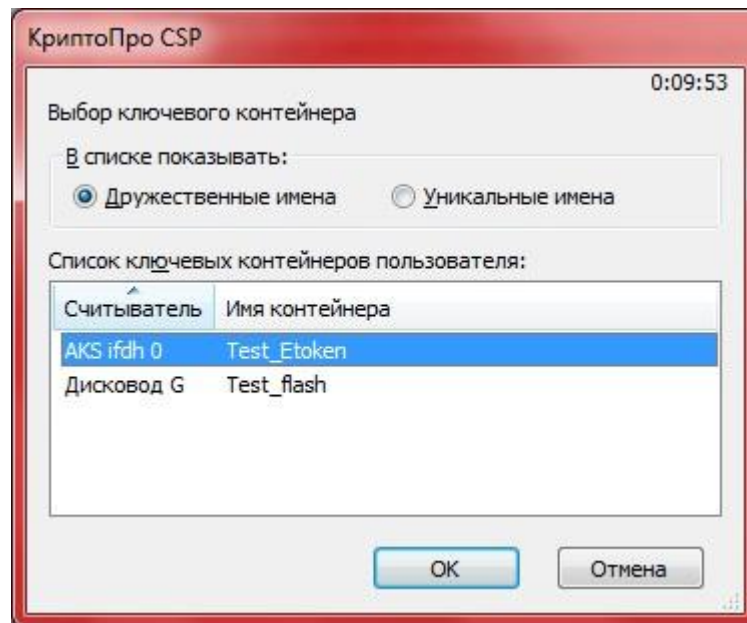
3) В открывшемся окне нажать «Обзор...»:



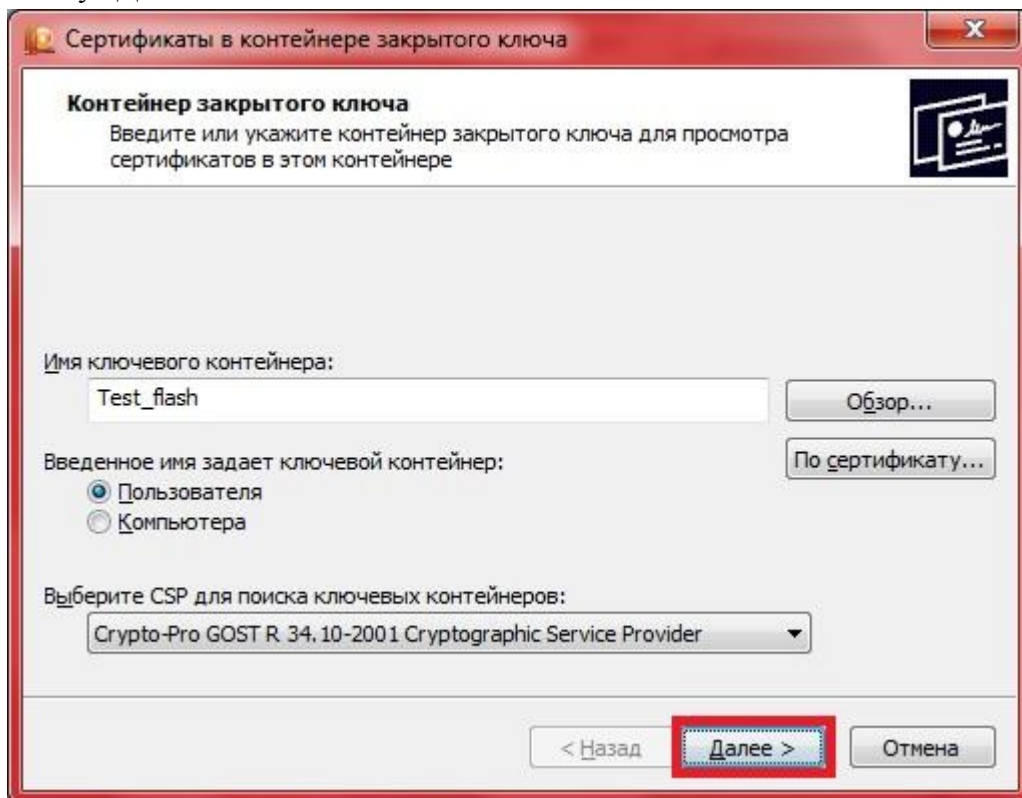
4) В списке ключевых контейнеров пользователя необходимо выбрать контейнер, соответствующий устанавливаемому сертификату КПЭП и нажать «ОК». В списке ключевых контейнеров указывается считыватель и имя контейнера. Считыватели:

- «Дисковод G (H, F и т.п.)» - «Флешка»;
- «Aktiv Co. ruToken 0 (1, 2, 3 и т.п.)» - носители Rutoken;
- «AKS ifdh 0 (1, 2, 3 и т.п.)» - носители e-Token.

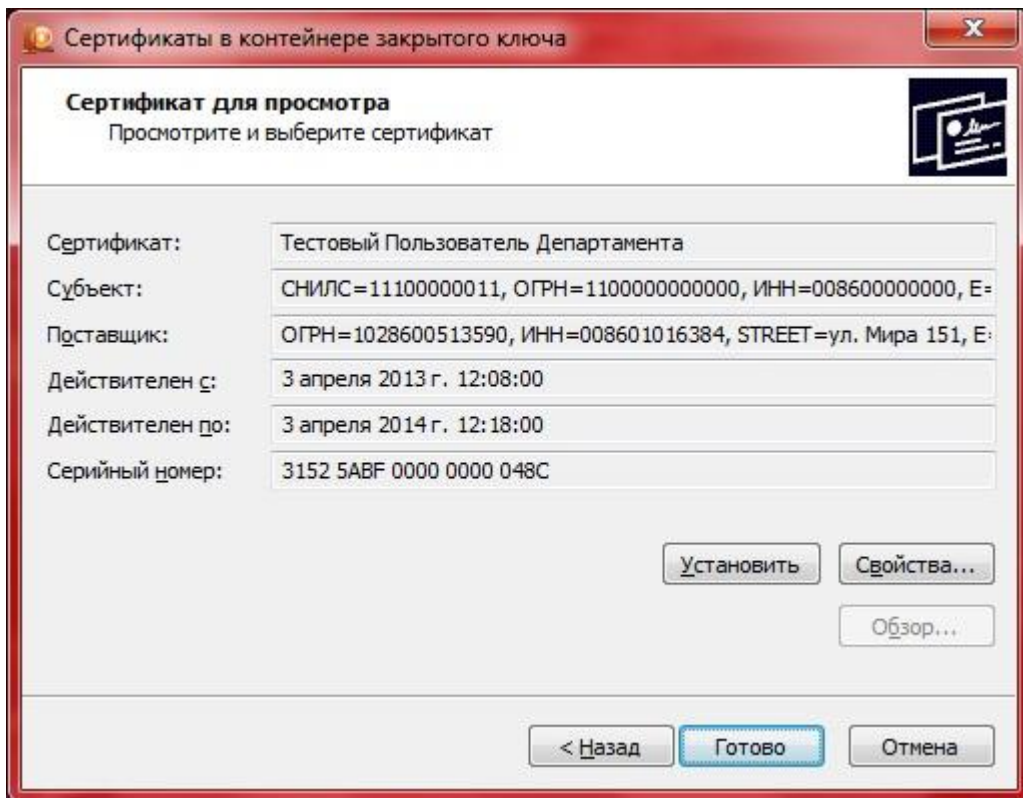




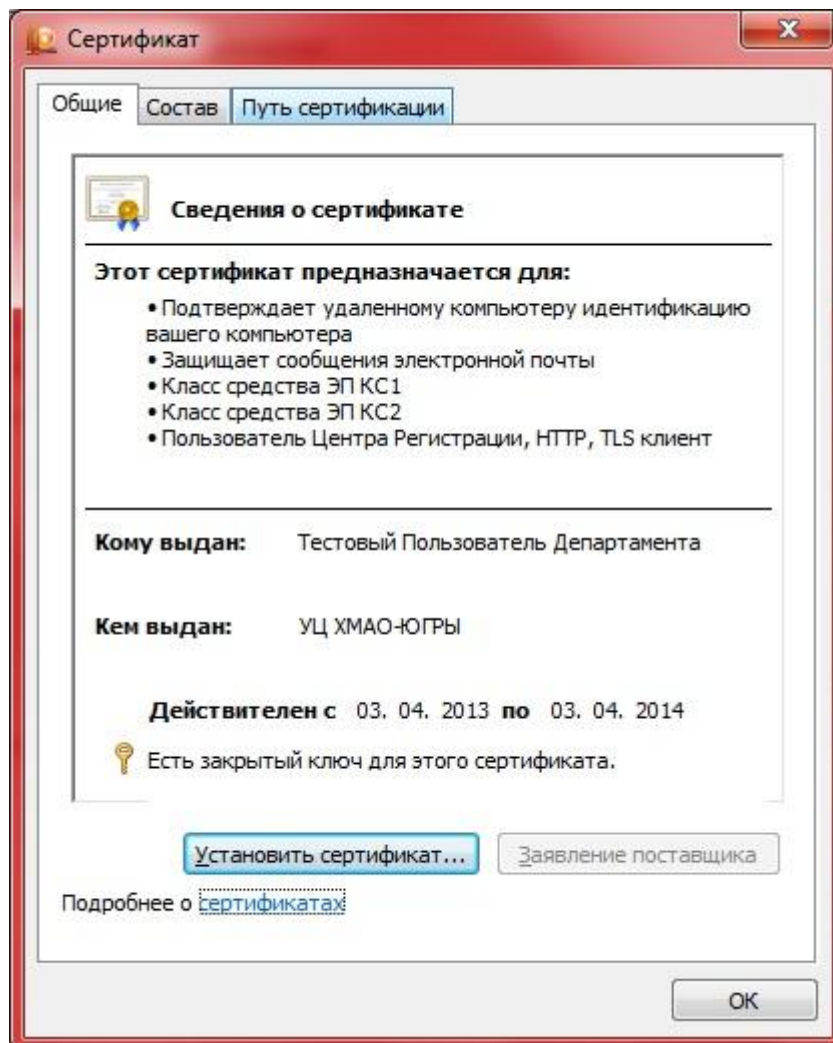
5) Нажать кнопку «Далее»:



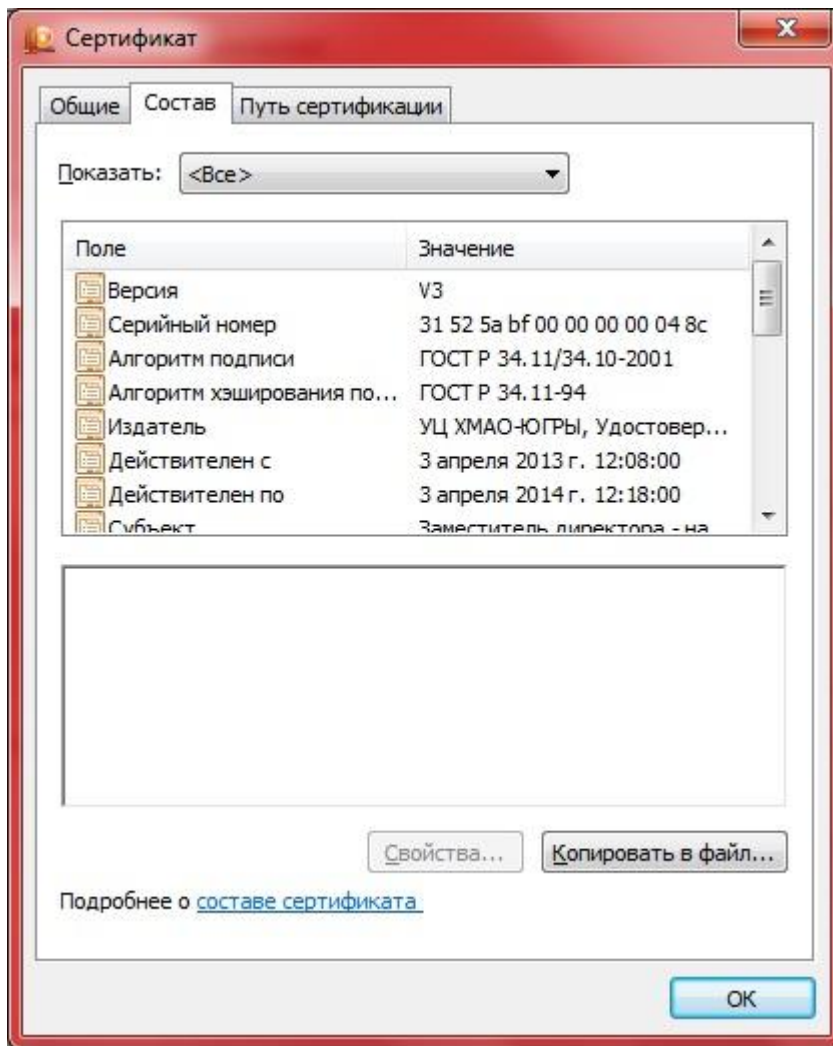
6) КриптоПро CSP отобразит данные сертификата, соответствующего выбранному ключевому контейнеру:



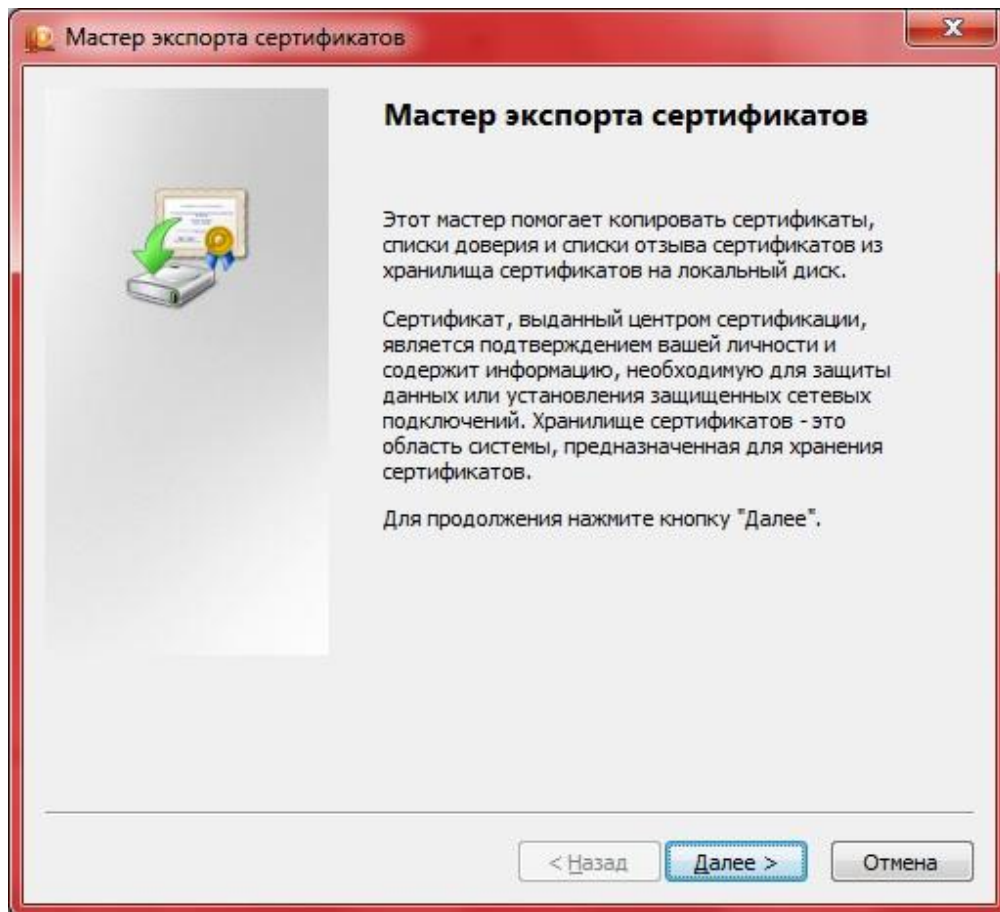
7) Нажать кнопку «Свойства...», после чего откроется следующее окно:



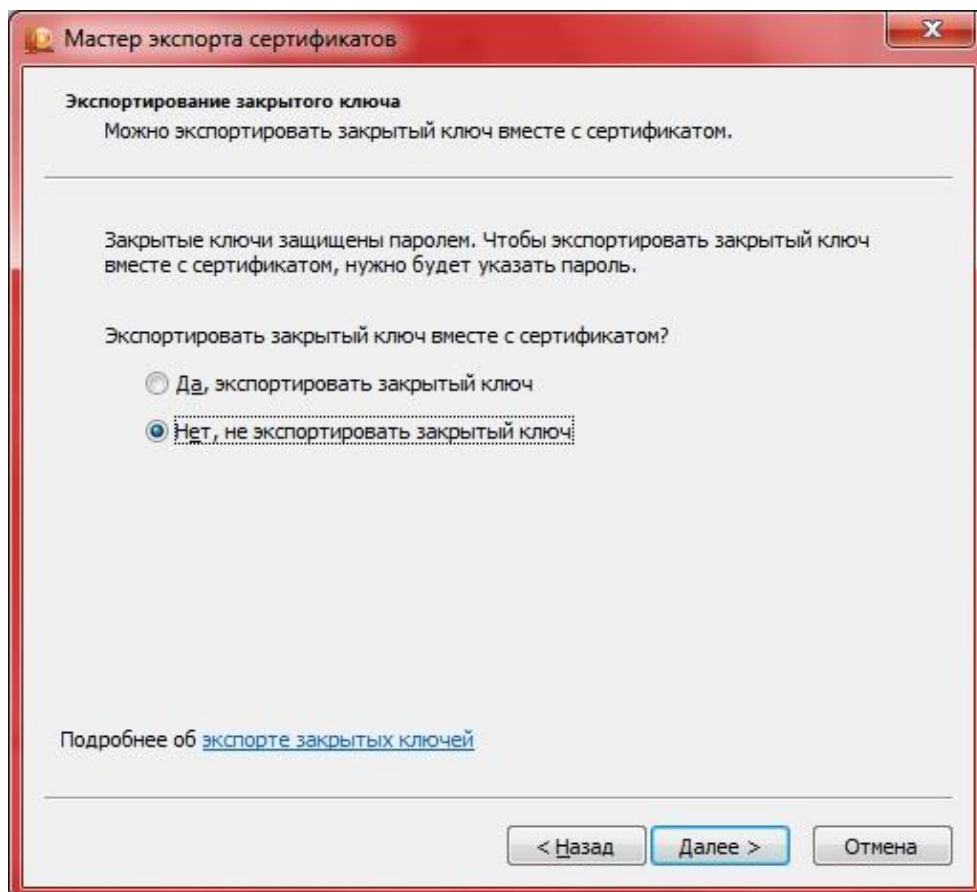
8) В открывшемся окне перейти во вкладку «Состав» (сверху):



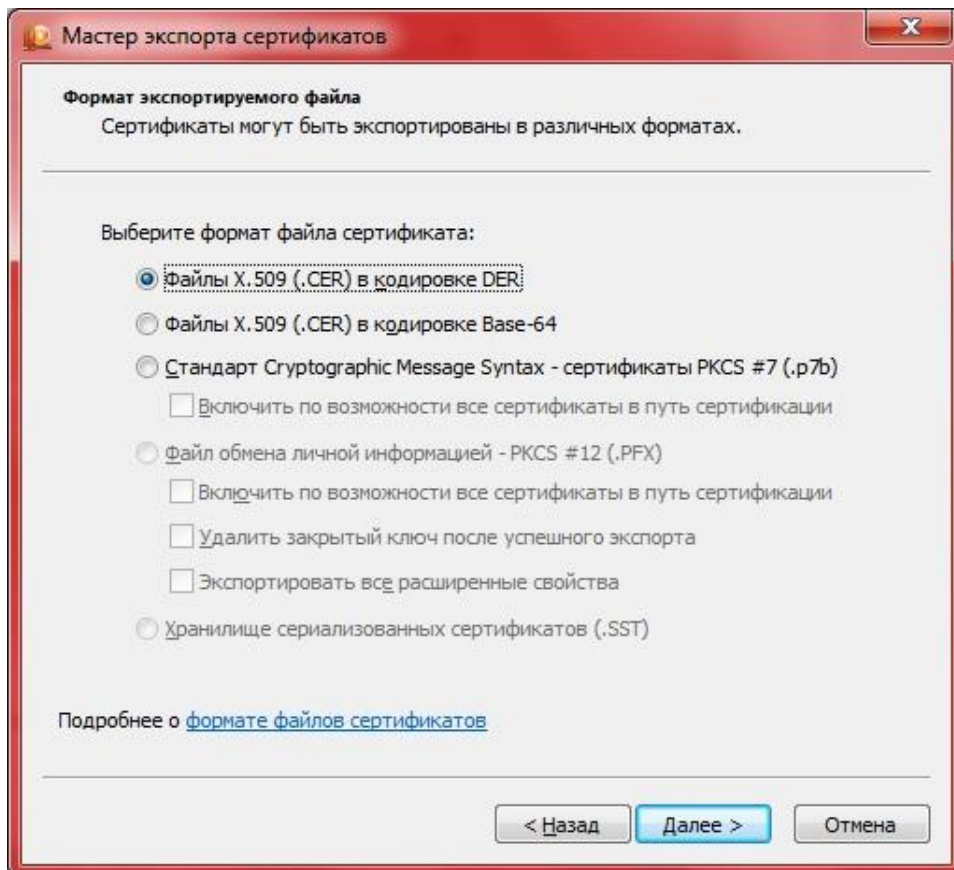
9) Для вызова мастера экспорта сертификатов нажать «Копировать в файл»:



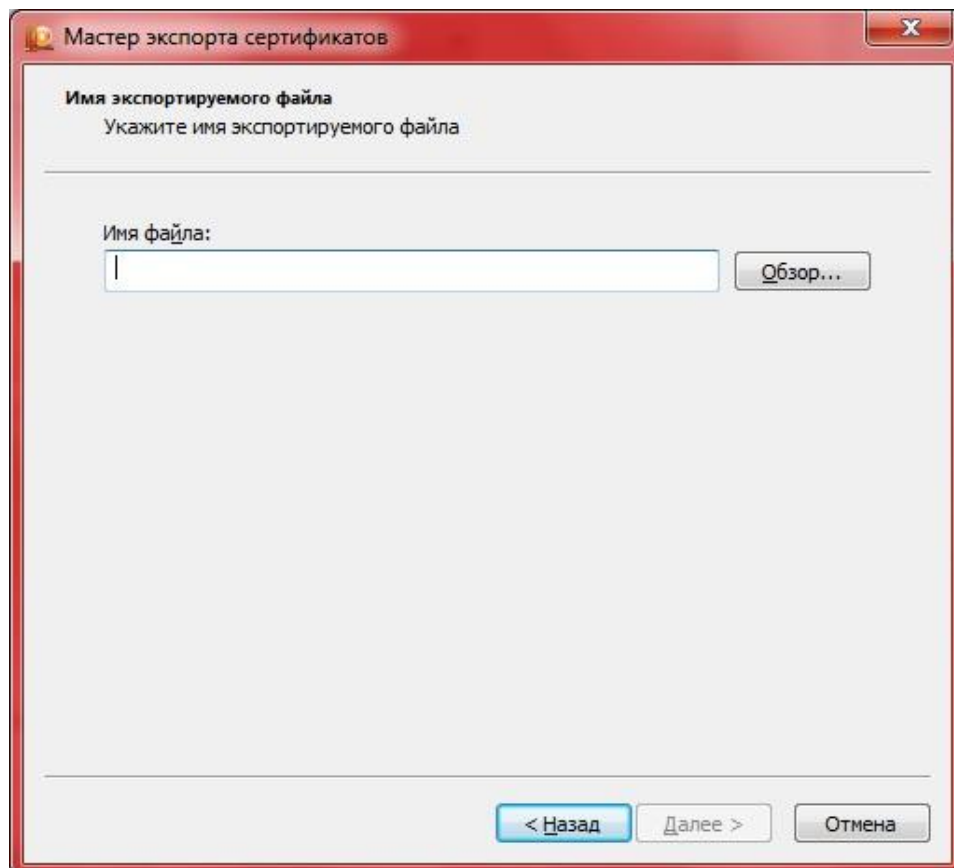
10) Нажать кнопку «Далее»:



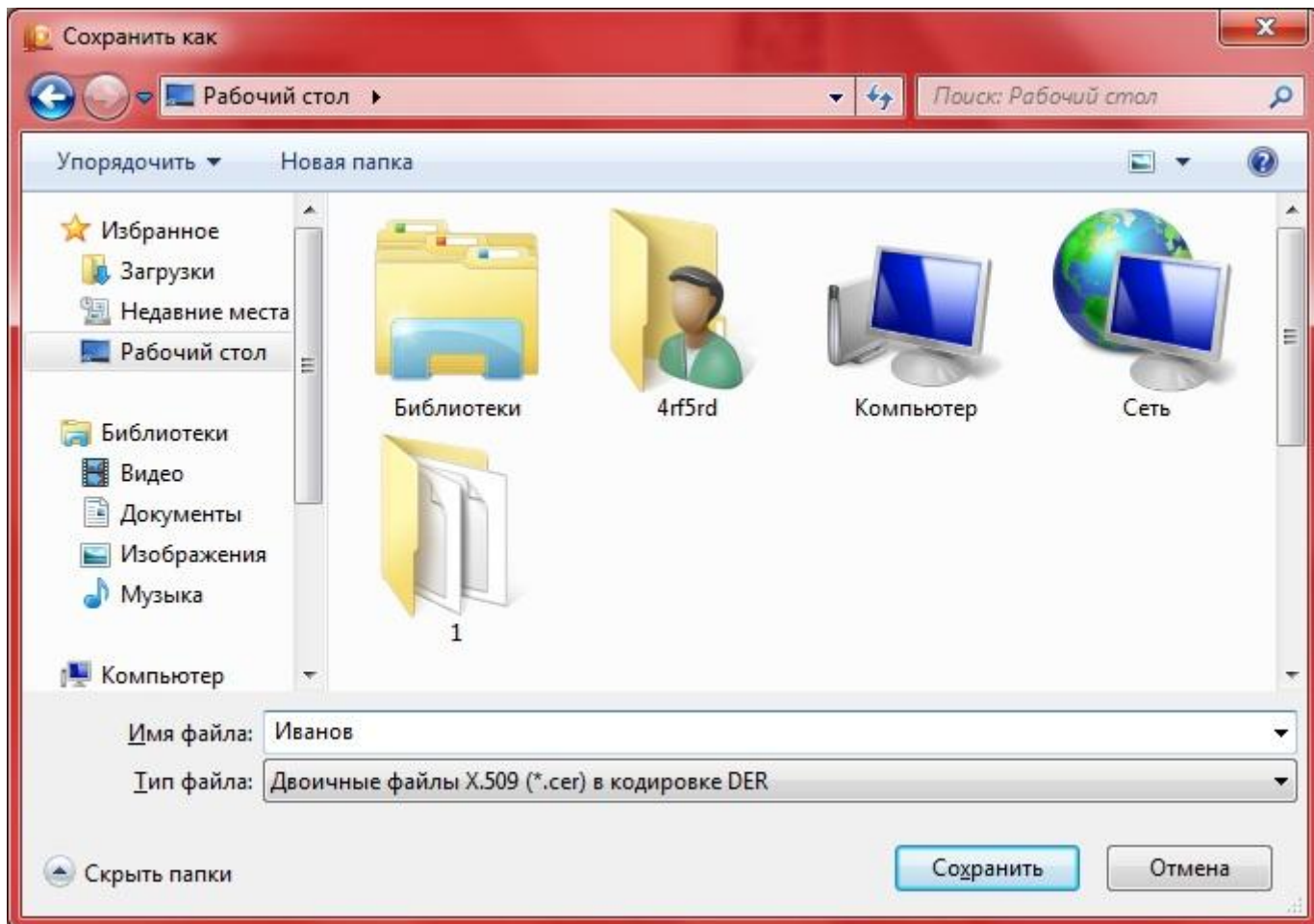
11) Выбрать «Нет, не экспортировать закрытый ключ», нажать кнопку «Далее»:



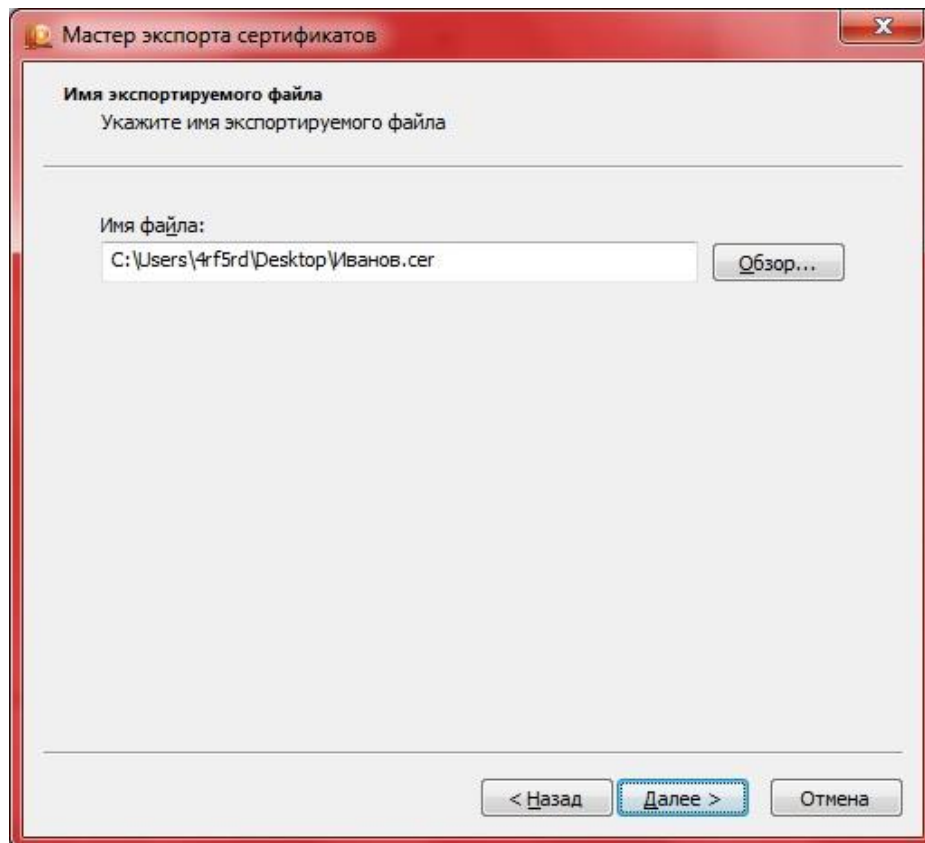
12) Выбрать кодировку «DER», нажать кнопку «Далее»:



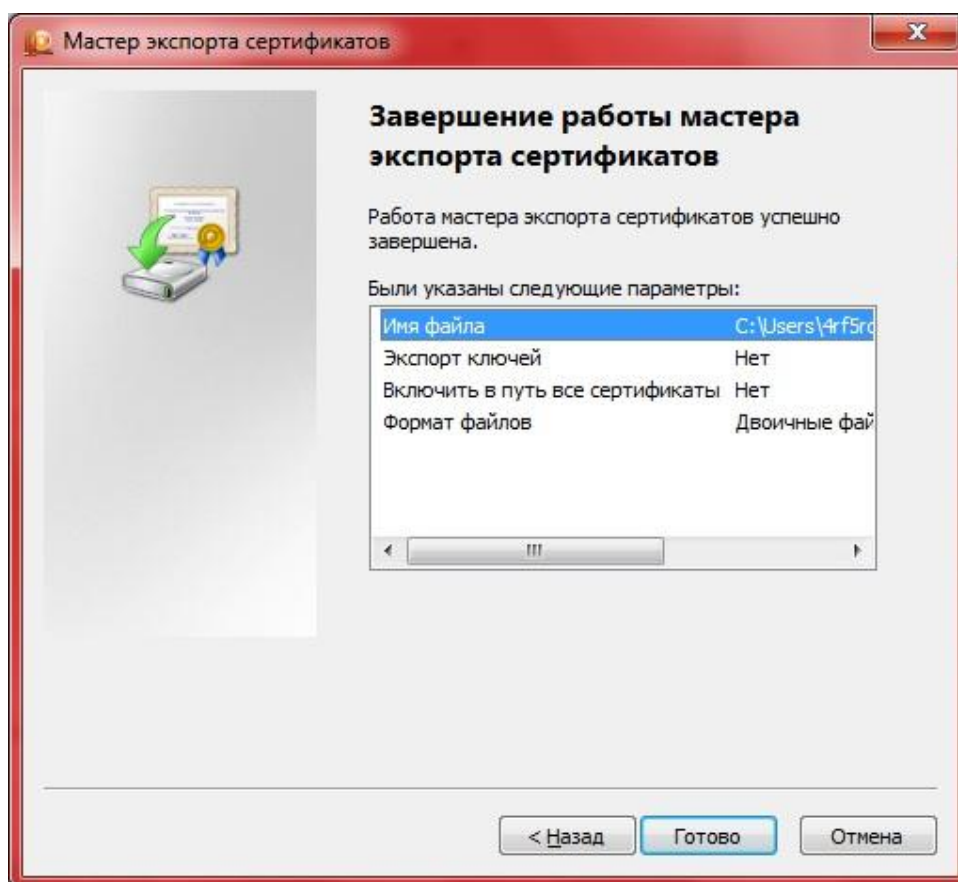
13) Нажать кнопку «Обзор»:



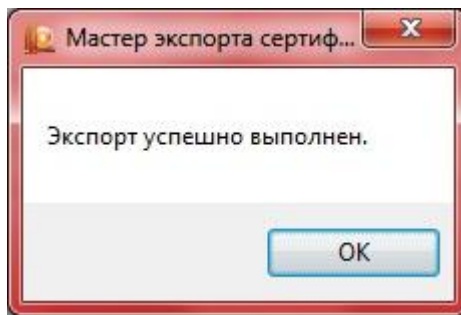
14) Выбрать место сохранения файла и ввести произвольное имя сохраняемого файла (например, ФИО владельца сертификата), после чего нажать кнопку «Сохранить»:



15) Нажать кнопку «Далее»:



16) Нажать кнопку «Готово». Свидетельством успешного завершения экспорта будет следующее сообщение:



17) Экспортируемый сертификат КПЭП будет отображаться следующим образом:

