

**ПАМЯТКА**  
**пользователю электронной подписи, выданной УЦ**  
**ГБУ «МИАЦ» по установке программного обеспечения**  
**для работы с электронной подписью**

**г. Курган**  
**2017 г.**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

Данный документ предназначен для пользователей, осуществляющих самостоятельную установку средства криптографической защиты информации (далее - СКЗИ) ViPNet CSP и настройку автоматизированного рабочего места (далее - АРМ) для работы с электронной подписью (далее - ЭП).

В удостоверяющем центре ГБУ «МИАЦ» (далее - УЦ ГБУ «МИАЦ») срок действия ключей и сертификата ЭП установлен равным 2 года. При необходимости произвести плановую (до истечения срока действия ключей ЭП менее месяца) или внеплановую смену ключей ЭП (изменение учетных данных владельца сертификата, потеря доступа к ключевому носителю, потеря ключевого носителя и т.д.) обратитесь в ГБУ «МИАЦ».

Для правильной работы СКЗИ ViPNet CSP необходимо выполнить все пункты данного руководства в указанной последовательности.

Для корректной работы с ЭП на различных интернет-порталах в качестве интернет-обозревателя рекомендуется использовать Microsoft Internet Explorer версии 6.0 и выше.

## 2. ПОЛУЧЕНИЕ И УСТАНОВКА VIPNET CSP

**! Внимание ! Не рекомендуется устанавливать СКЗИ ViPNet CSP на компьютер, где уже установлены другие криптопровайдеры (например, СКЗИ «КриптоПро CSP»).**

1. Для получения ViPNet CSP необходимо перейти на официальный сайт разработчика по адресу [http://infotecs.ru/downloads/besplatnye-produkty/vipnet-csp.html?arrFilter\\_93=1824101684&set\\_filter=Y](http://infotecs.ru/downloads/besplatnye-produkty/vipnet-csp.html?arrFilter_93=1824101684&set_filter=Y) и выбрать дистрибутив ViPNet CSP, соответствующий Вашей операционной системе.

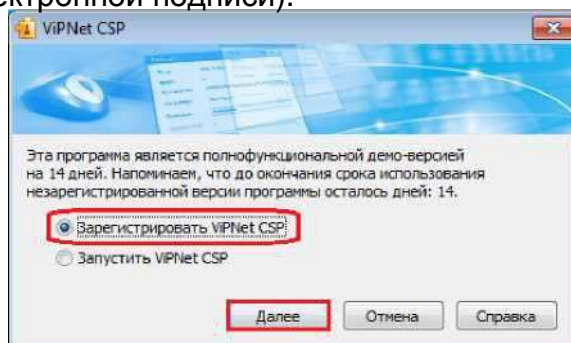
2. Пройдите установленную процедуру регистрации, согласившись с условиями лицензионного соглашения (EULA) и заполнив обязательные поля.

3. Перейдите по полученной ссылке для скачивания продукта и сохраните указанный серийный номер (также ссылка для скачивания продукта и серийный номер будут отправлены на указанный при регистрации адрес электронной почты). Сохраните загруженный архив с дистрибутивом на своем компьютере, распакуйте архив, а затем запустите установку ViPNet CSP файлом Setup.exe.

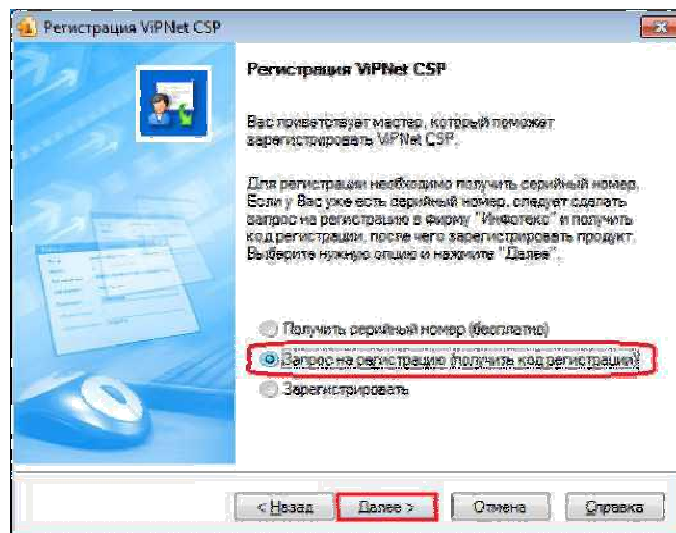
4. Выполните установку ViPNet CSP, следуя инструкциям мастера установки.

5. После перезагрузки компьютера запустите настройку ViPNet CSP из панели «Пуск».

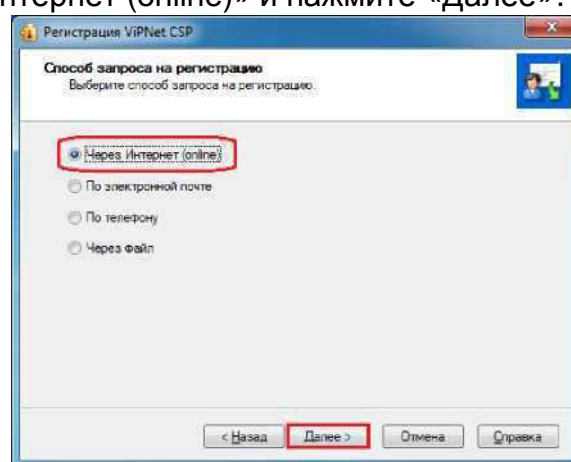
6. Выберите «Зарегистрировать ViPNet CSP» и нажмите «Далее» (без регистрации ViPNet CSP будет функционировать в течение 14 дней и не сможет обеспечить юридической значимости электронной подписи).



7. Выберите «Запрос на регистрацию (получить код регистрации)» и нажмите «Далее».

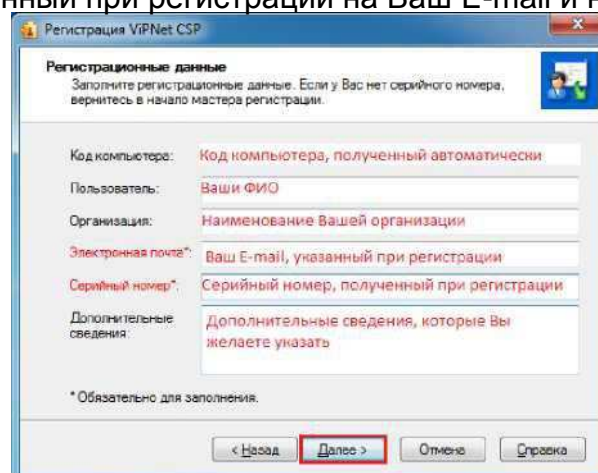


8. Выберите «Через Интернет (online)» и нажмите «Далее».



**! Внимание !** Если при выполнении следующих действий по каким-то причинам Вам не удастся зарегистрировать ViPNet CSP через Интернет (online) вернитесь в окно выбора способа регистрации и воспользуйтесь регистрацией «По электронной почте» или «По телефону», следуя инструкциям мастера регистрации.

9. Заполните форму своими регистрационными данными, включая «Серийный номер» ViPNet CSP, полученный при регистрации на Ваш E-mail и нажмите «Далее».

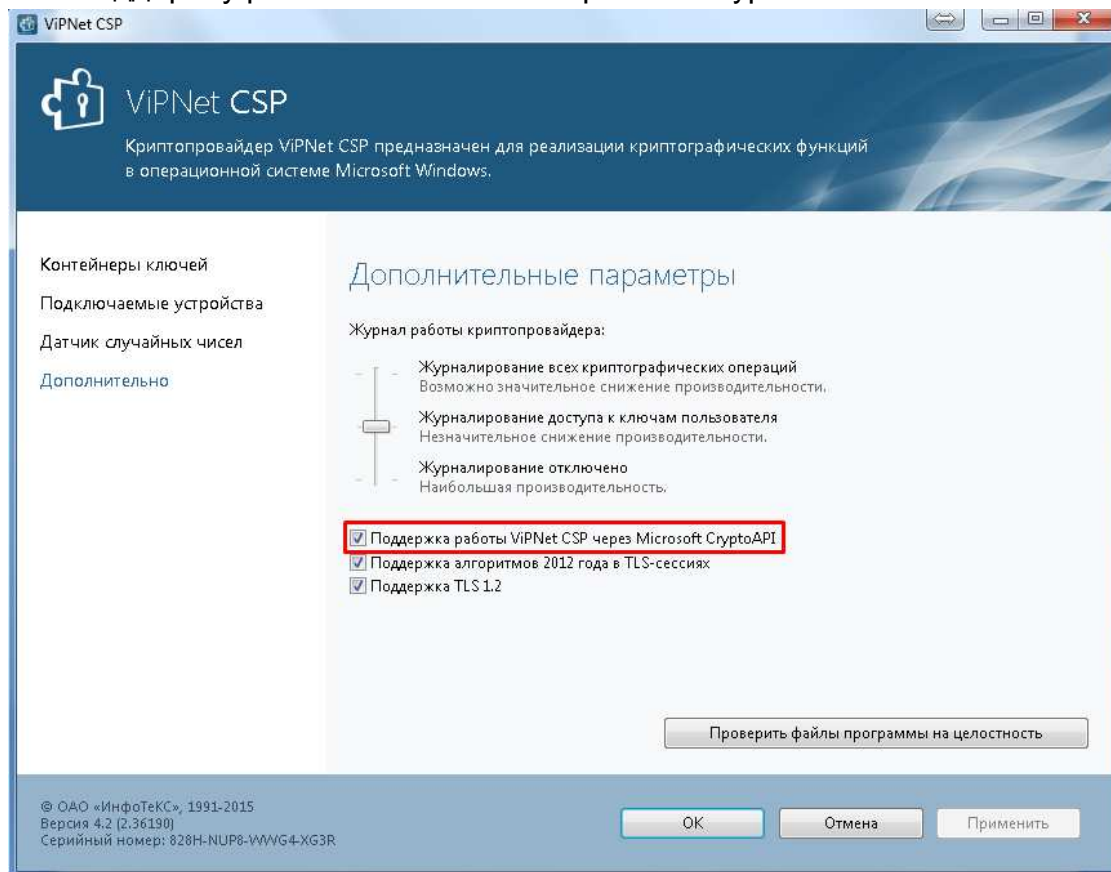


10. На вопрос «Запустить ViPNet CSP сейчас?» ответьте «Yes» или запустите ViPNet CSP позже из панели «Пуск».

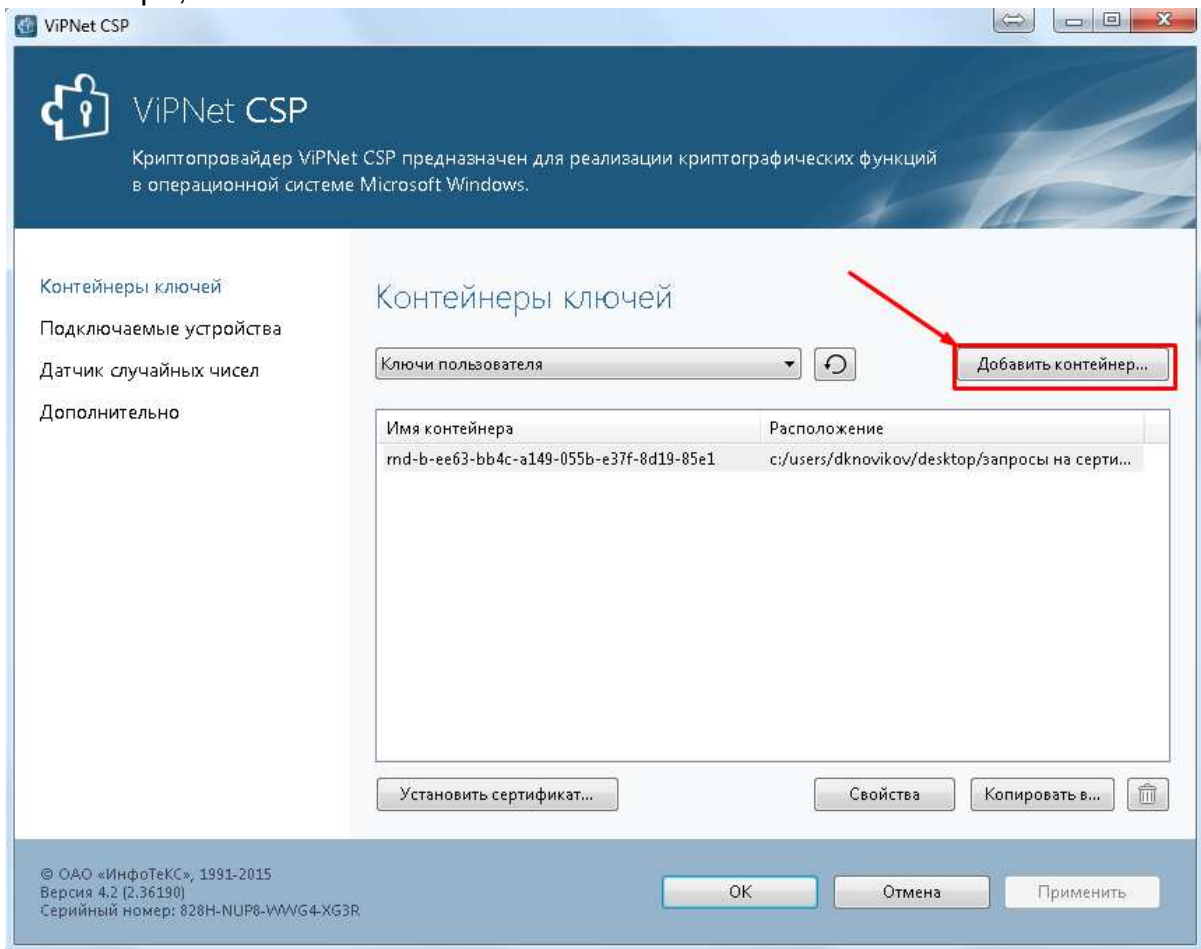
### 3. УСТАНОВКА ЛИЧНОГО СЕРТИФИКАТА С КЛЮЧЕВОГО НОСИТЕЛЯ.

Вставьте ключевой носитель в USB-порт компьютера.

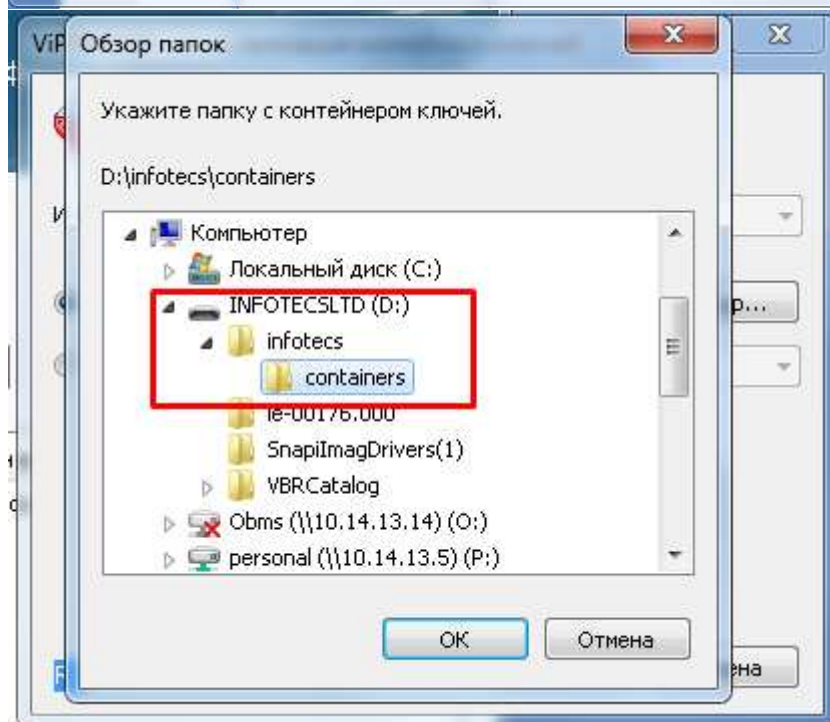
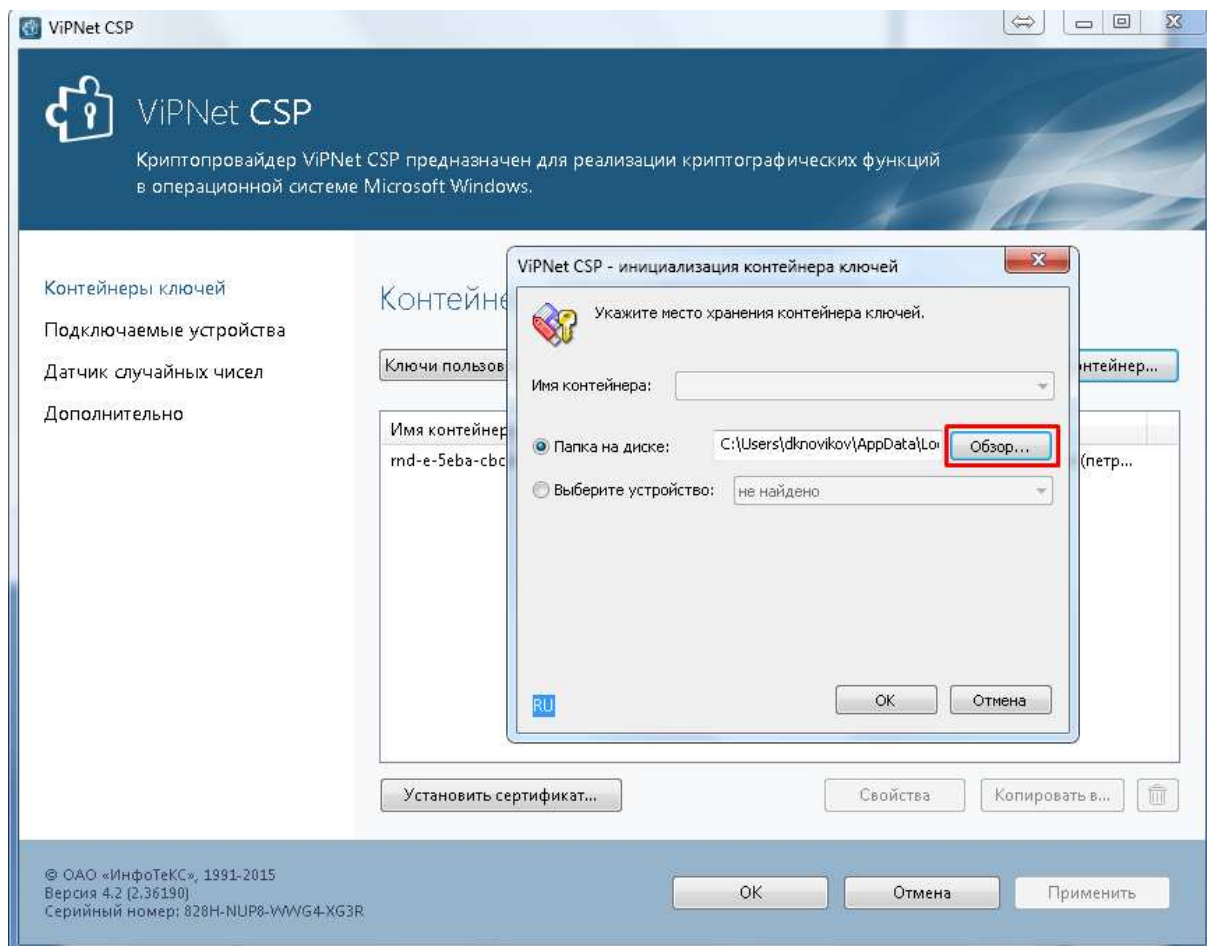
Запустите ViPNet CSP и убедитесь, что на закладке "Общие" включена опция "Включить поддержку работы ViPNet CSP через MS Crypto API".



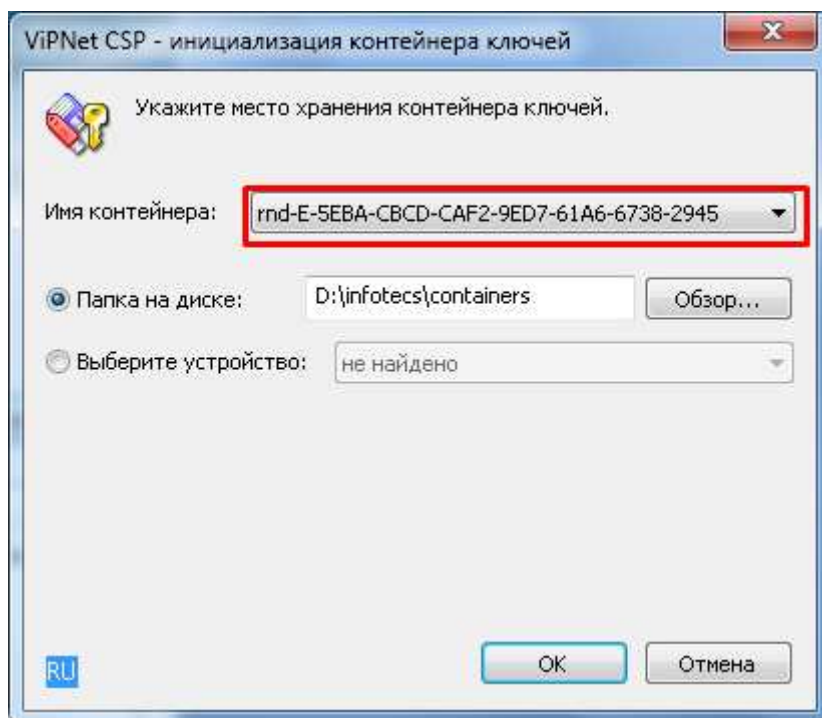
Перейдите на закладку "Контейнеры ключей". Нажмите на кнопку «Добавить контейнер»,



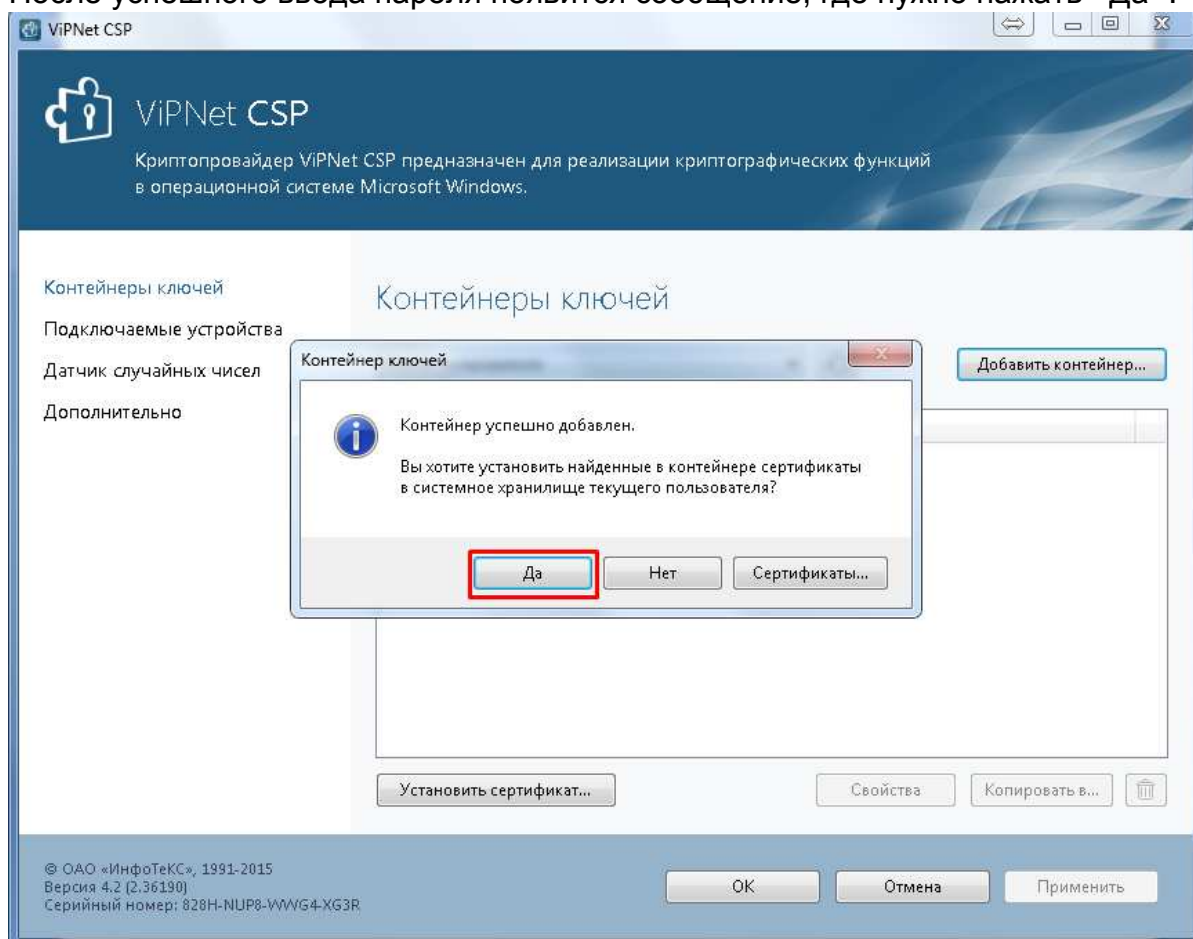
В открывшемся окне нажмите на кнопку «Обзор» и укажите путь к контейнеру ключей «буква съемного диска:\infotecs\containers»



контейнер выберется автоматически. Нажать кнопку «OK» и ввести пароль.

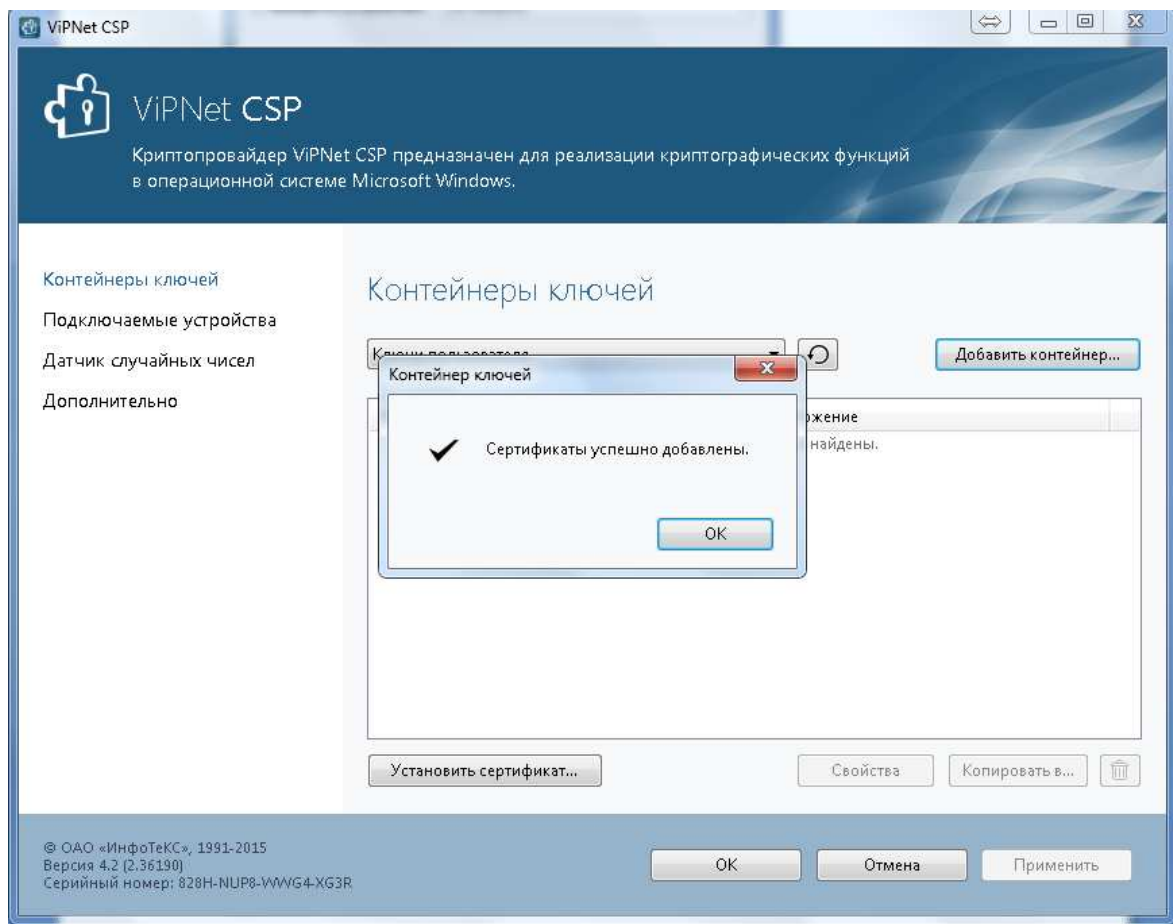


После успешного ввода пароля появится сообщение, где нужно нажать «Да»:

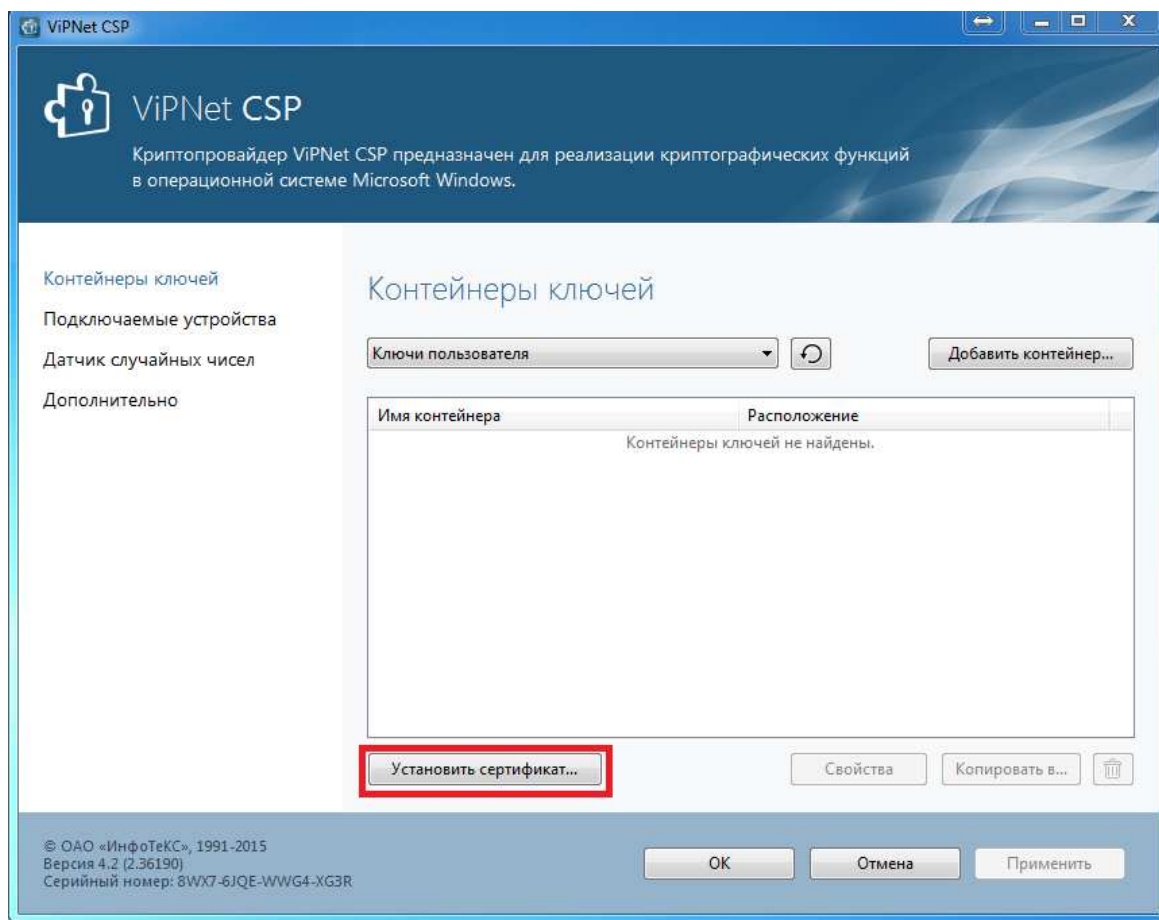


После этого установка личного сертификата завершена

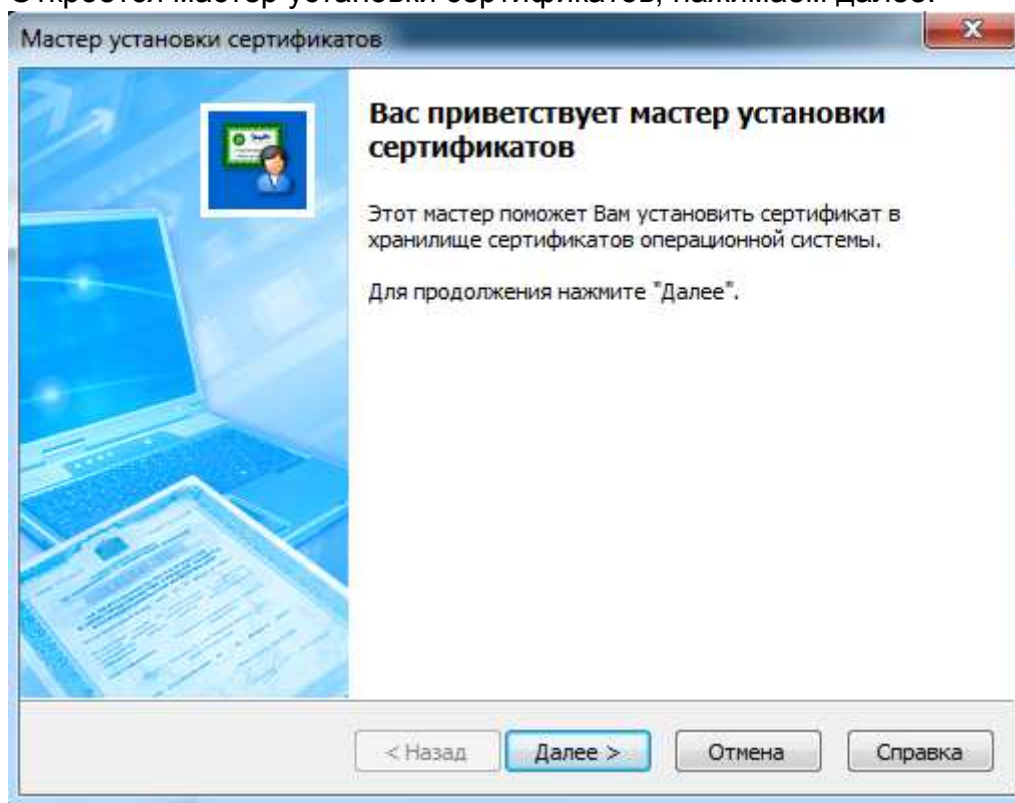


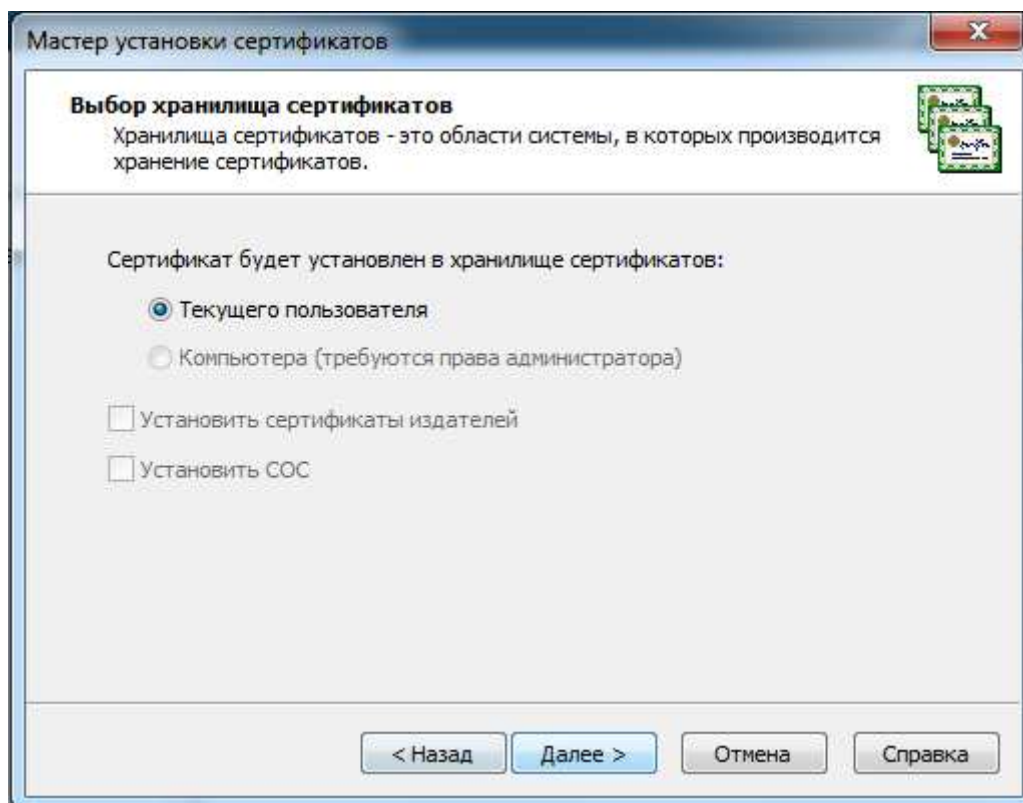


Далее необходимо связать контейнер с закрытым ключом и сертификатом, для этого нажимаем на установить сертификат:

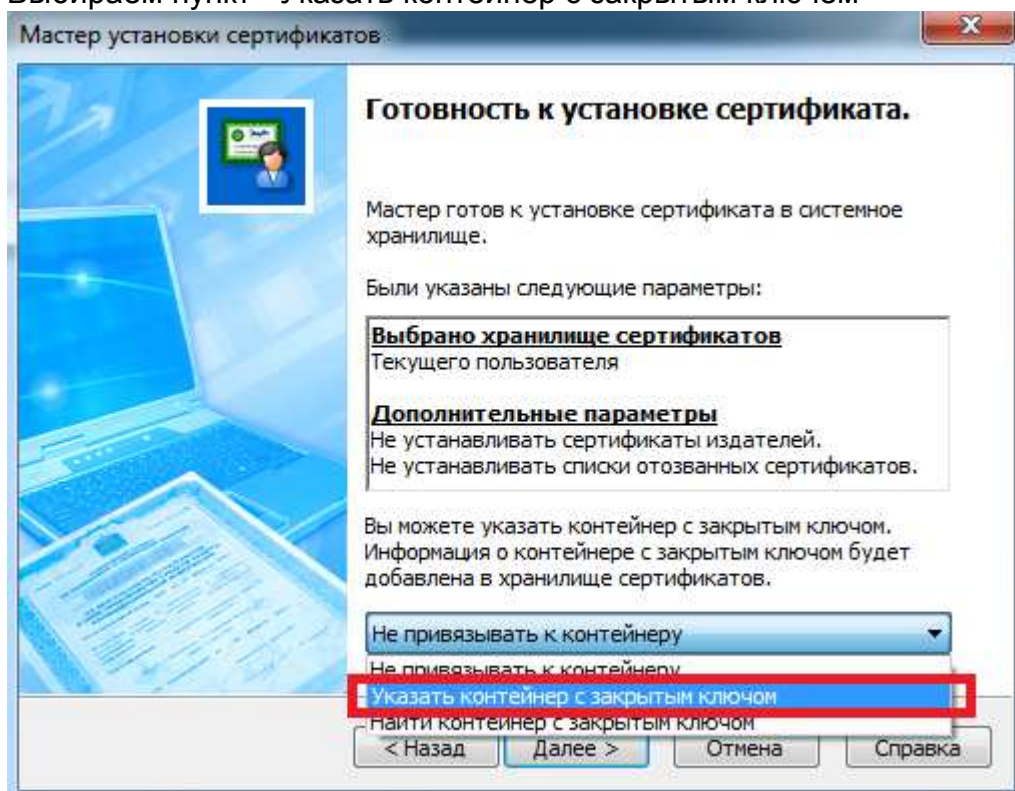


Откроется мастер установки сертификатов, нажимаем далее:

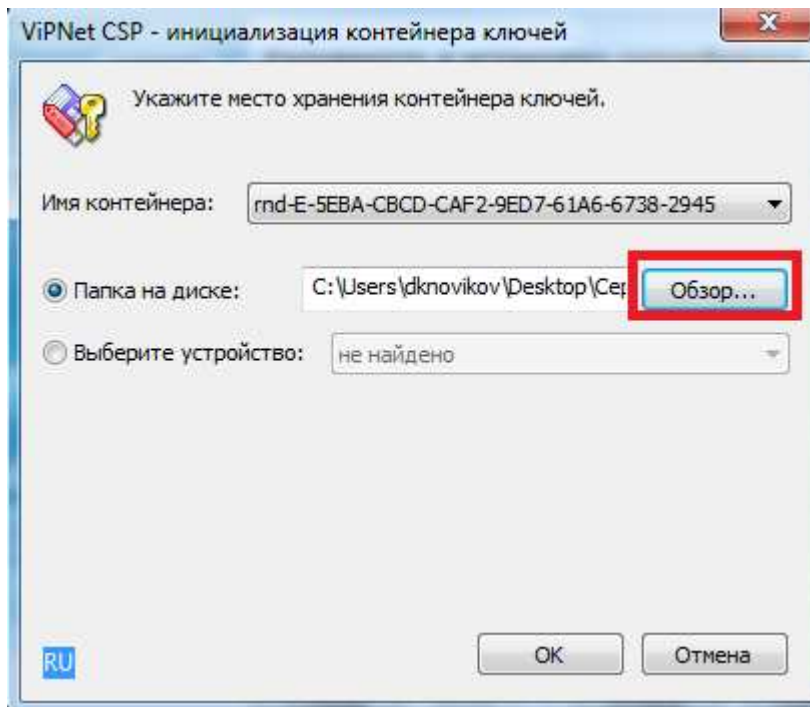




Выбираем пункт «Указать контейнер с закрытым ключом»



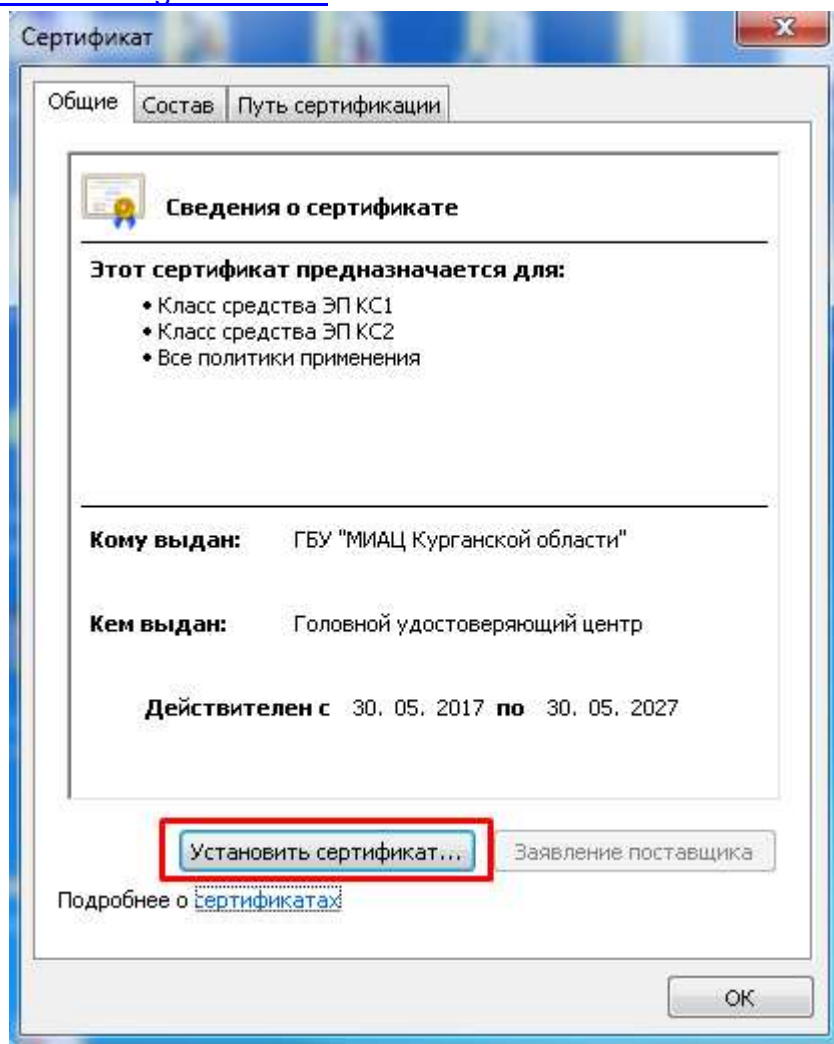
Указываем путь к контейнеру



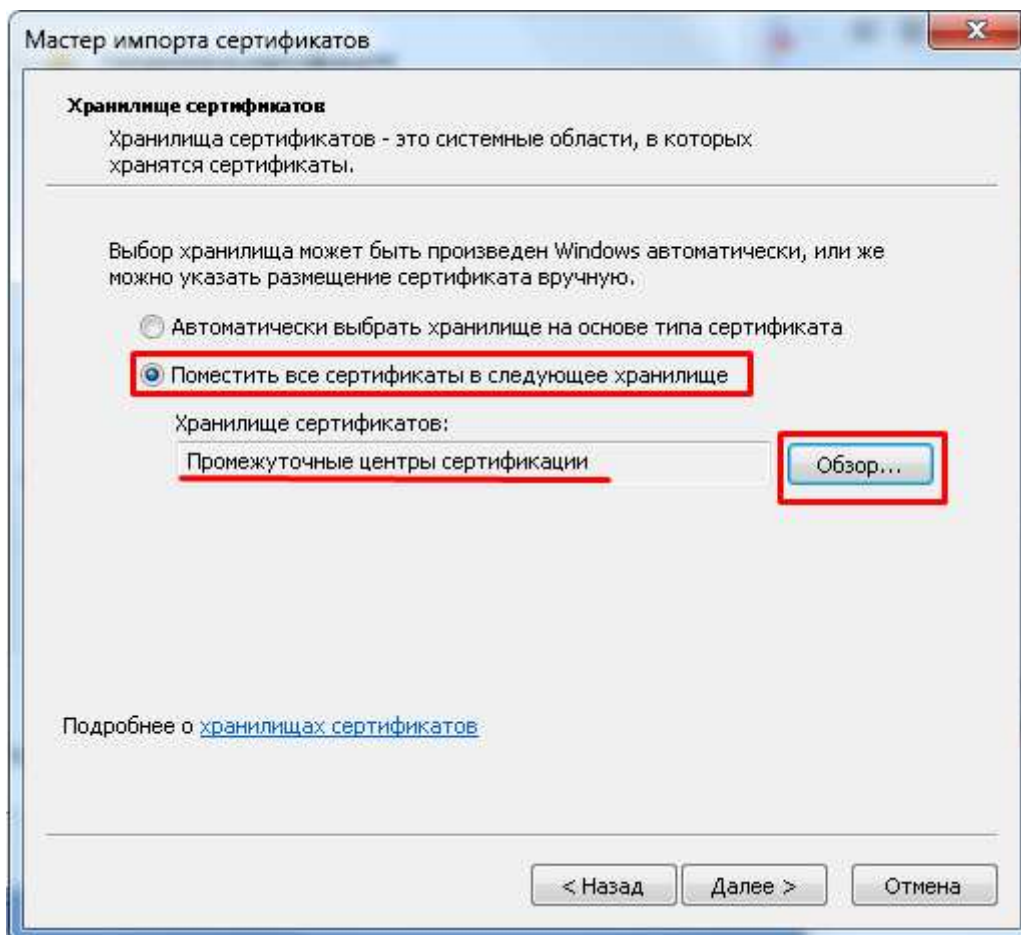
На этом связь личного сертификата с контейнером завершена

#### 4. УСТАНОВКА КОРНЕВОГО СЕРТИФИКАТА И СЕРТИФИКАТА ГОЛОВНОГО УЦ

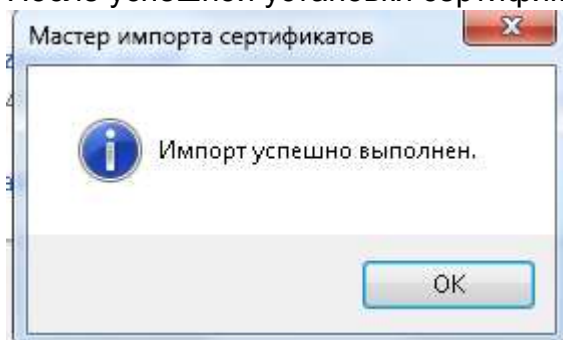
Откройте файл корневого сертификата УЦ ГБУ «МИАЦ» по ссылке <http://kurgan-med.ru/fbase/uc/gbumiac.cer>



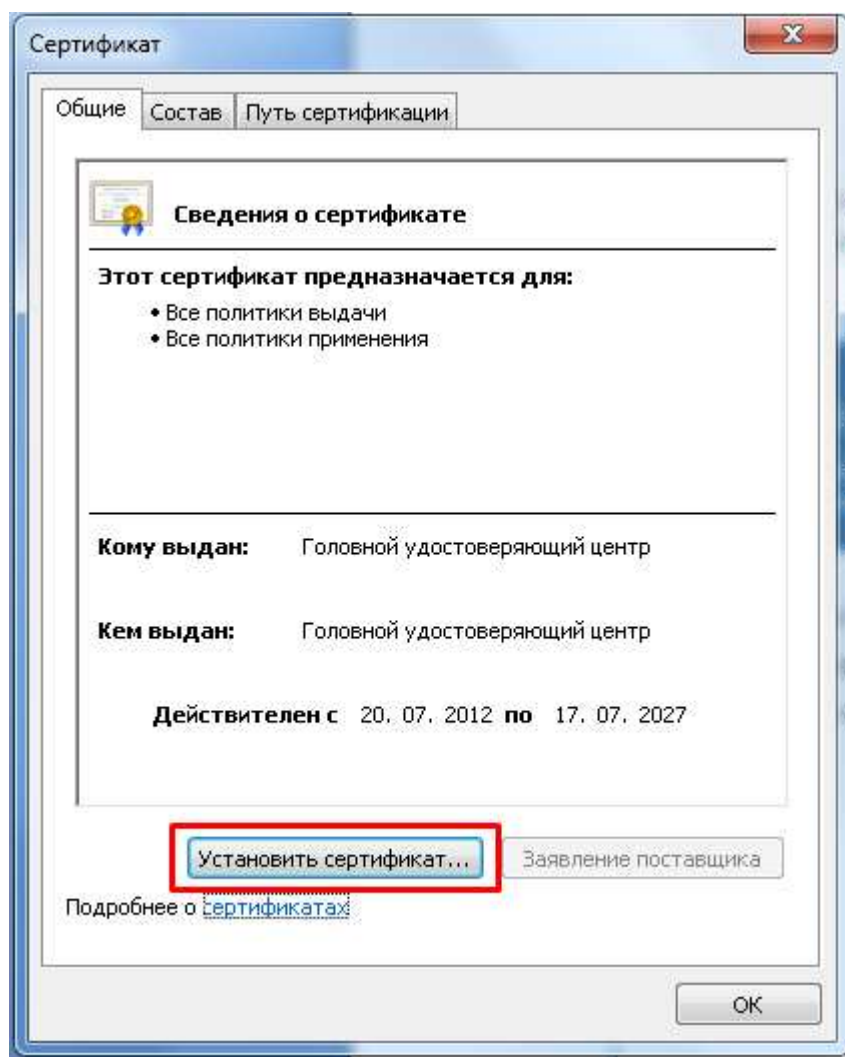
Нажмите «Установить сертификат» и «Далее». В открывшемся окне выберите вариант «Поместить все сертификаты в следующее хранилище», нажмите «Обзор» и выберите «Промежуточные центры сертификации».



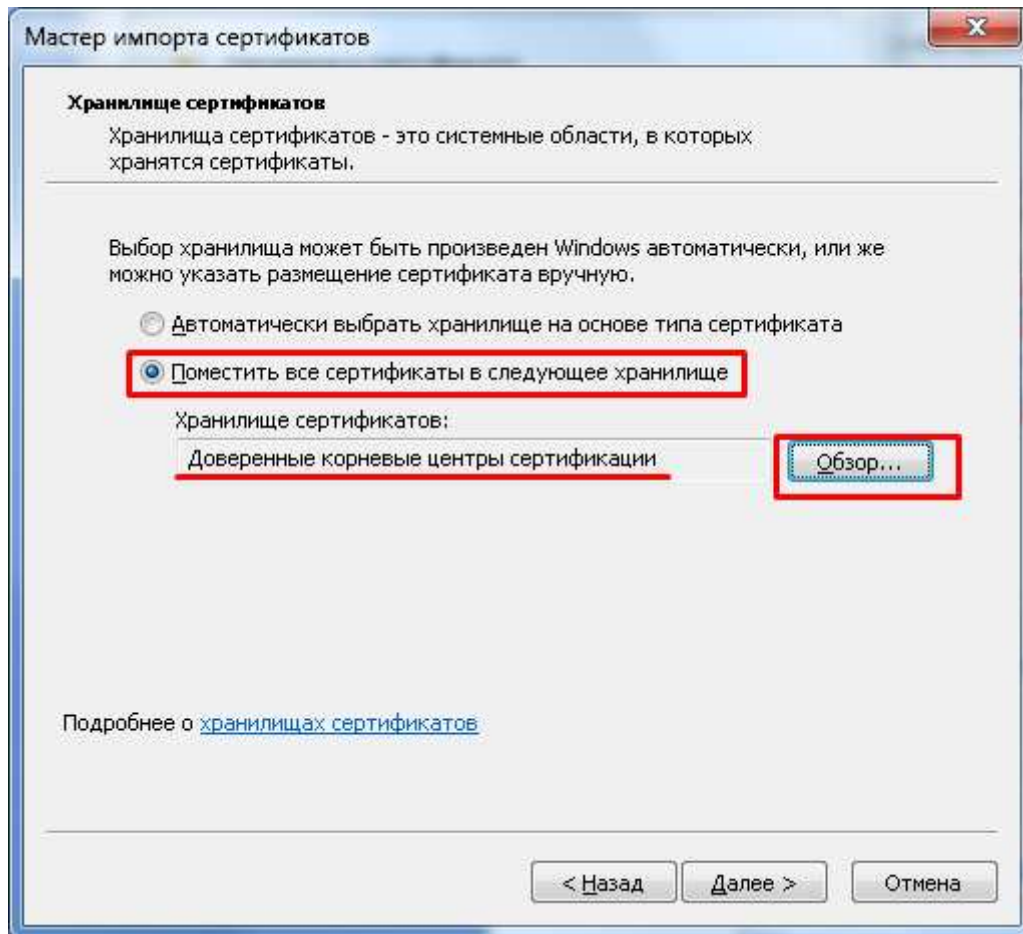
После успешной установки сертификата появится окно:



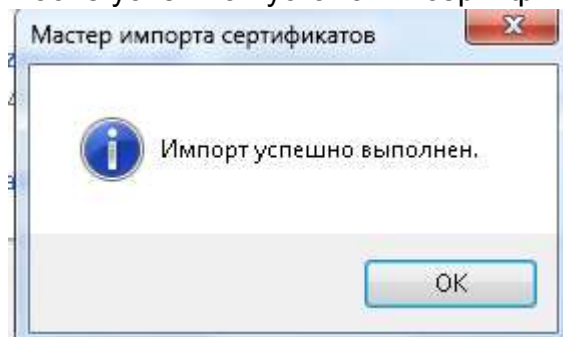
Откройте файл корневого сертификата Головного удостоверяющего центра по ссылке <https://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=8CAE88BBFD404A7A53630864F9033606E1DC45E2>



Нажмите «Установить сертификат» и «Далее». В открывшемся окне выберите вариант «Поместить все сертификаты в следующее хранилище», нажмите «Обзор» и выберите «Доверенные корневые центры сертификации». Если будет выведено предупреждение, нажмите «Да».



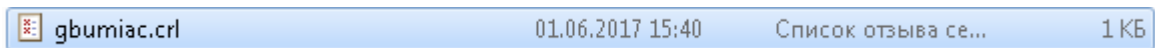
После успешной установки сертификата появится окно:





## 5. УСТАНОВКА СПИСКА ОТОЗВАННЫХ СЕРТИФИКАТОВ.

Откройте ссылку <http://kurgan-med.ru/fbase/uc/gbumiac.crl>



По файлу списка отозванных сертификатов щёлкните правой клавишей мыши и укажите «Установить список отзыва (CRL)», затем следуйте указаниям мастера установки.