Инструкция по настройке рабочего места для модуля «Диадок» в терминальном режиме

Содержание

В инструкции приняты следующие обозначения:

 — совет, носит рекомендательный характер;

 — важное сообщение.

В данной инструкции описан процесс настройки рабочего места для модуля «Диадок» в терминальном режиме. Настройка рабочего места заключается в следующем:

1. установка необходимых компонентов (см. раздел 2);
2. запрос и установка сертификата на терминальном компьютере (см. раздел 3);
3. настройка проброса смарт-карт (см. раздел 4);
4. установка сертификата на терминальном сервере (см. раздел 5).

1. Аппаратно-программные требования

Для работы модуля требуется:

- Одна из операционных систем компании Microsoft:
  - Windows XP с пакетом обновления 3 (SP3) и выше;
  - Windows Server 2003 с пакетом обновления 1 (SP1) и выше;
  - Windows Vista с пакетом обновления 1 (SP1) и выше;
  - Windows 7;
  - Windows 2008 (в том числе R2).
- Интернет-браузер Internet Explorer версии не ниже 7.0.
- Подключение к сети Интернет по выделенному каналу либо по коммутируемым линиям связи с использованием модема (рекомендуемая скорость подключения не менее 0,5 Мбит/сек).
- Должен быть открыт доступ к адресам вида *https://*.kontur.ru*. (за помощью обращайтесь к системному администратору).
- Должен быть открыт доступ по 80 и 443 порту на сервер Оператора *.kontur.ru (за помощью обращайтесь к системному администратору).
- Процессор с тактовой частотой не менее 400 МГц, оперативная память не менее 128 Мбайт.
- Свободное дисковое пространство не менее 200 Мбайт.
- Наличие USB-порта. Для подключение Рутокена или Рутокена Лайт.

Если на одном компьютере планируется использовать систему «Диадок» и программы, которые используют средства криптографической защиты информации (например, Клиент-Банк, Интернет-Банк), убедитесь, что они используют одну и ту же версию СКЗИ «КриптоПро CSP». Использование разных криптографических средств на одном компьютере может привести к неработоспособности программ и системы.

2. Установка необходимых компонентов

Для начала работы установите программное обеспечение на локальный компьютер и на терминальный сервер:

И на терминал, и на сервер устанавливается одинаковое программное обеспечение. Установку следует производить с правами администратора.

1. В строке интернет-браузера введите адрес веб-диска https://install.kontur.ru/diadoc**.**
2. При первом входе необходимо установить утилиту **AddToTrusted** (либо **Kontur-Install-KE** при использовании интернет-браузера, отличного от Internet Explorer).

   *Если при входе на веб-диск не появляется сообщение о необходимости установки **AddToTrusted**, то перейдите к п. 1.2. инструкции.*

   Если при входе на веб-диск появляется сообщение о том, что все необходимые компоненты уже установлены, то перейдите к п. 2 инструкции.

   Утилита ***AddToTrusted*** добавляет необходимые домены в надежные узлы, а также настраивает для них параметры безопасности. Для ее установки выполните следующее:

   а. Нажмите на ссылку **AddToTrusted** (либо **Kontur-Install-KE)** (рис. 1).

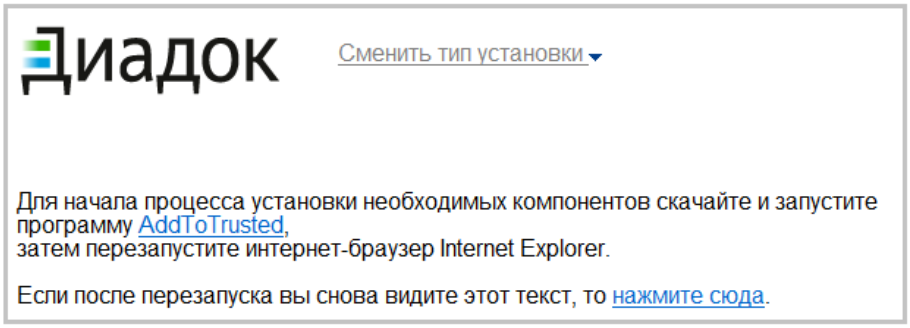

Рис. 1. Окно веб-диска при первом входе

   б. В появившемся внизу окна сообщении нажмите на кнопку **Выполнить.**

Либо утилиту можно сохранить в любую папку и запустить оттуда файл AddToTrusted_User.exe (рис 2).

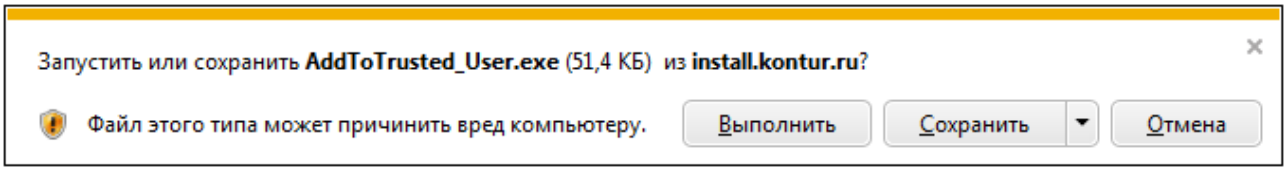

Рис. 2. Установка AddToTrusted

   в. После завершения установки утилиты закройте все окна интернет-браузера и заново зайдите на веб-диск по адресу https://install.kontur.ru/diadoc.

3. В открывшемся окне нажмите на кнопку **Начать проверку** и дождитесь окончания проверки установленных программ (рис. 3). При использовании веб-диска происходит автоматическая проверка уже установленных на рабочем месте компонентов.

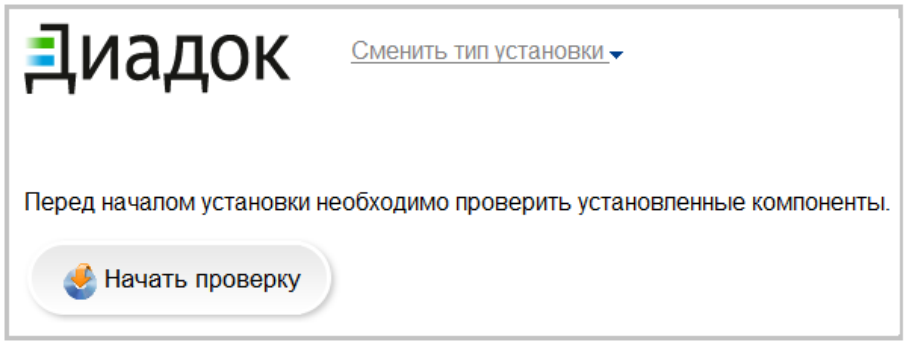

Рис. 3. Начало проверки

4. Нажмите на кнопку **Установить** для полной установки системы (рис. 4). Запустится процесс установки системы.

   При этом будут установлены только недостающие для корректной работы компоненты. Данный способ установки является рекомендуемым.

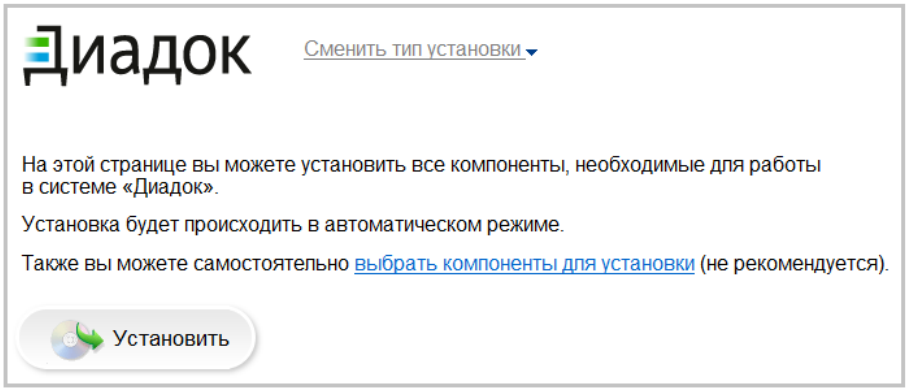

Рис. 4. Основное окно веб-диска

Для выборочной установки компонентов (не рекомендуется) нажмите на ссылку ***выбрать компоненты для установки*** *(рис. 4). Установите флажок для необходимых компонентов для установки и нажмите на кнопку* ***Начать установку*** *(рис. 5).*

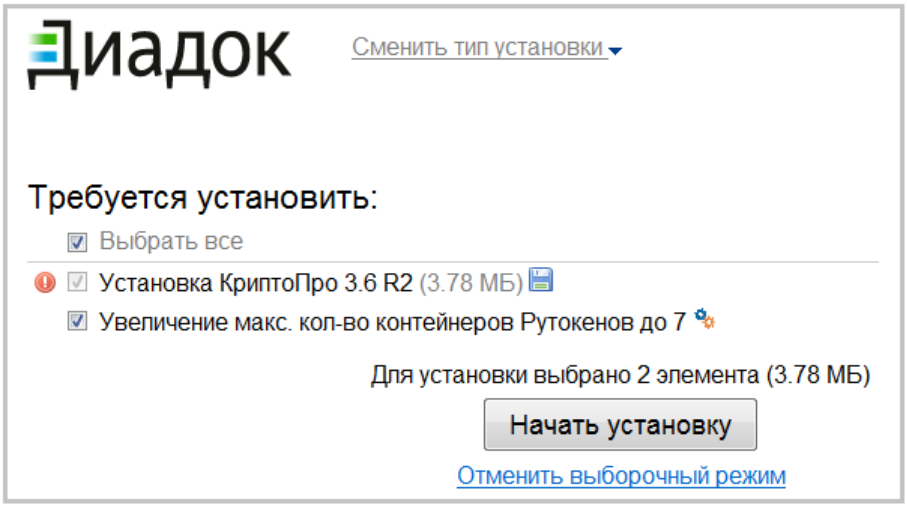

Рис. 5. Выборочная установка

Дождитесь окончания процесса установки.

5. Если была установлена программа **КриптоПро**, то для ее регистрации введите 25-значный серийный номер (рис. 6).

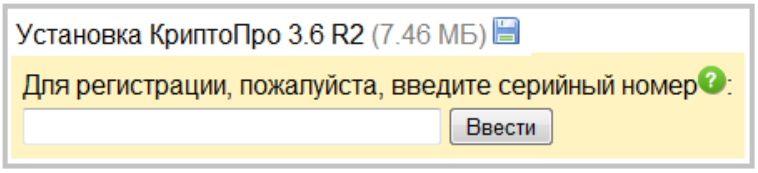

Рис. 6. Ввод серийного номера

*Серийный номер **КриптоПро** указан в приложении к договору на абонентское обслуживание «Лицензия на использование программного продукта КриптоПро CSP». Если в договоре данное приложение отсутствует, обратитесь в сервисный центр по месту подключения.*

6. Перезагрузить компьютер.

3. Запрос и установка сертификата на терминальном компьютере

После установки всех компонентов запросите и установите личный сертификат на терминальном компьютере.

Если сертификат ЭЦП не был получен в сервисном центре при подключении к системе, необходимо самостоятельно выполнить запрос на его получение, а затем установить полученный сертификат (см. раздел 3.2.1).

Если сертификат ЭЦП был получен, перейдите к его установке (см. раздел 3.2.2).

Запрос и установка сертификата выполняется только с ключевым носителем (Рутокеном, дискетой), выданным в сервисном центре.

3.1. Запрос и установка сертификата

Чтобы сформировать и установить сертификат ЭЦП:

1. В строке интернет-браузера введите адрес веб-диска https://install.kontur.ru/diadoc**.**
2. Нажмите на кнопку **Начать проверку** и дождитесь окончания проверки. Откроется страница для запроса и установки сертификата (см. рис. 7).

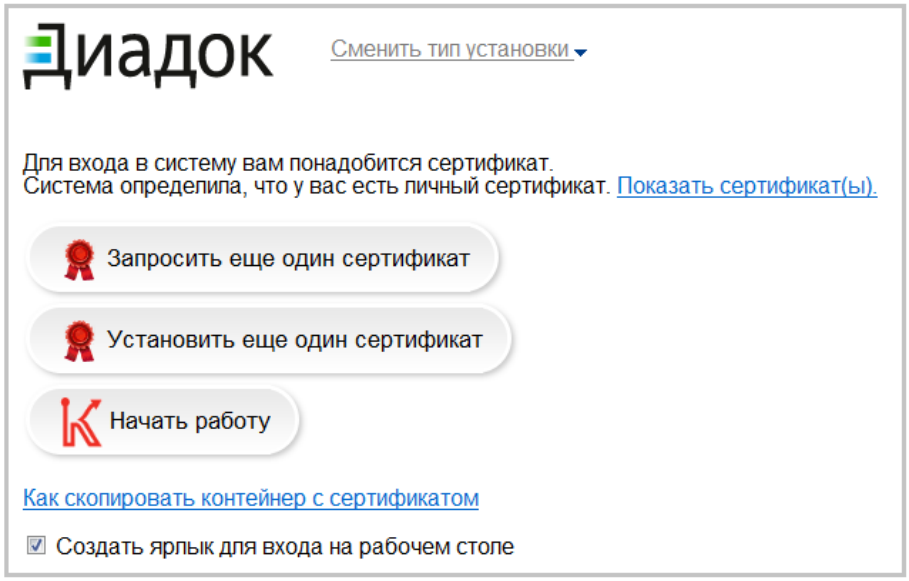

Рис. 7. Установка и запрос сертификатов с помощью веб-диска

3. Для того чтобы получить новый сертификат (при первом подключении или продлении обслуживания), нажмите на кнопку **Запросить сертификат.** Откроется окно программы для получения сертификатов.
4. В открывшемся окне (рис. 8) нажмите **Далее.**

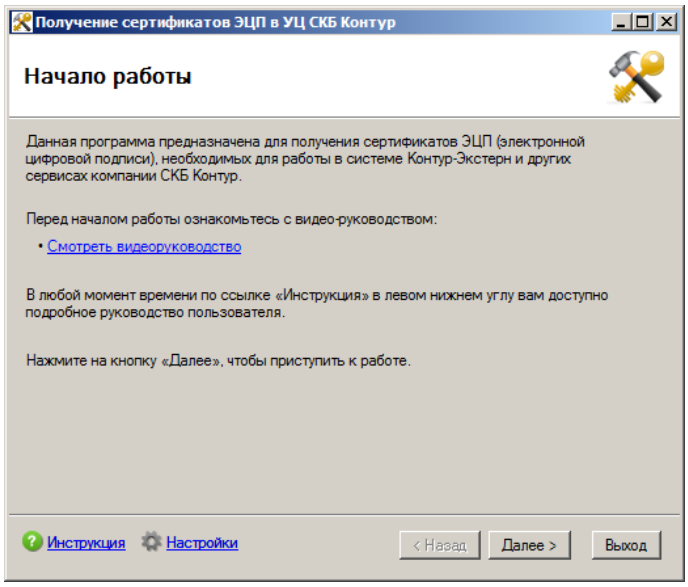

Рис. 8. Окно «Начало работы»

5. В открывшемся окне **Выбор режима работы** нажмите **Далее.**
6. В окне **Выбор ключевого носителя** (рис. 9) выберите ключевой носитель, полученный в сервисном центре.

Если в окне не отображается нужный ключевой носитель, вставьте его в компьютер и нажмите ***Обновить список.***

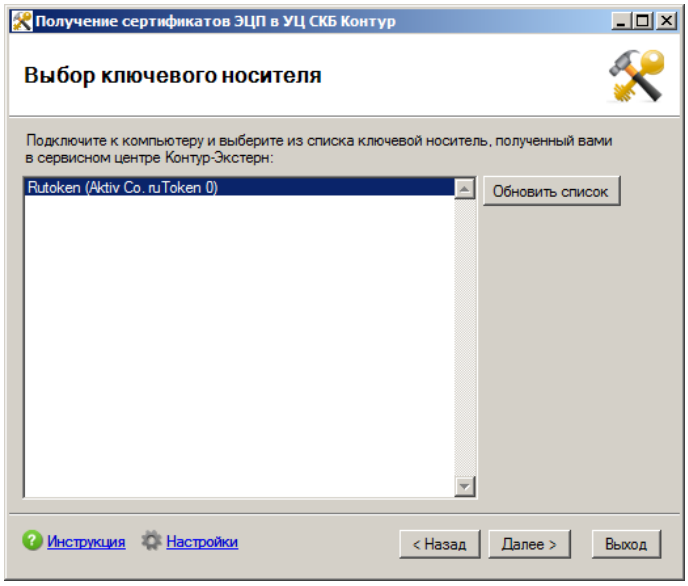

Рис. 9. Окно выбора ключевого носителя

7. Убедитесь, что есть соединение с Интернетом, и нажмите **Далее**. Начинается запрос данных с сервера. После этого:
    - В окне **Запрос на получение сертификата** (рис. 10) появляются ФИО ответственного лица, для которого запрашивается сертификат. Перейдите к п. 8.

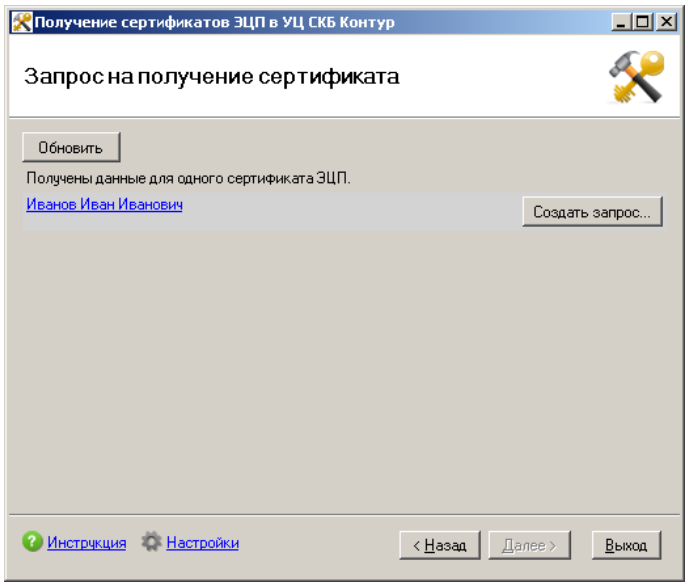

Рис. 10. Окно загрузки данных с сервера

- Если возникла проблема с соединением, открывается окно **Изменение настроек прокси-сервера**. Настройте соединение через прокси-сервер самостоятельно с помощью пункта **Использовать ручные настройки** (рис. 11) или обратитесь к системному администратору.

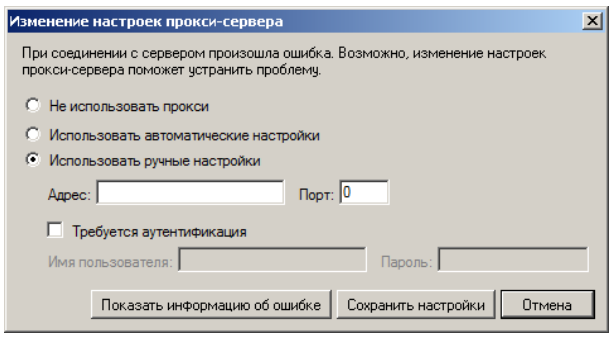

Рис. 11. Изменение настроек прокси-сервера

8. Нажмите на название организации или ФИО и проверьте информацию в окне **Данные запроса**.

   Если данные указаны некорректно, обратитесь в сервисный центр, иначе документы будет передаваться с неверными реквизитами организации.

9. Закройте окно **Данные запроса** и нажмите **Создать запрос**.
10. В открывшемся окне (рис. 12) с помощью полосы прокрутки выберите ключевой носитель, выданный в сервисном центре, и нажмите **OK**.

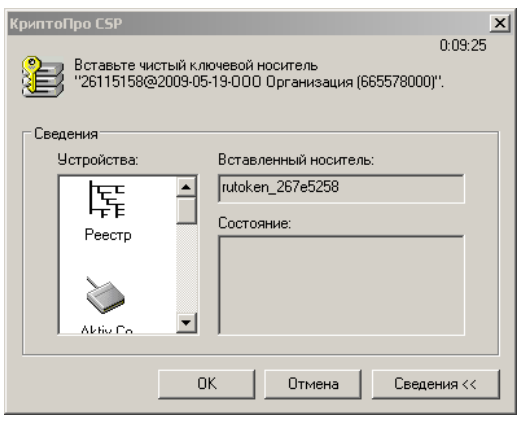

Рис. 12. Окно выбора ключевого носителя

11. Для формирования закрытого ключа перемещайте курсор мыши в области окна датчика случайных чисел (рис. 13).

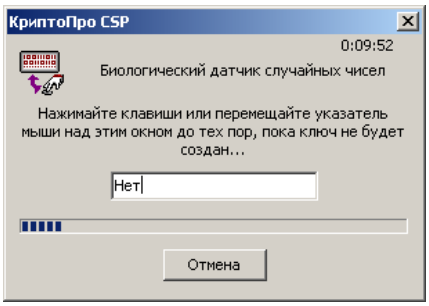

Рис. 13. Окно генератора случайных чисел

12. В открывшемся окне установки pin-кода/пароля на ключевой контейнер:

- для Рутокена, Рутокена Лайт (рис. 14) – pin-код обязателен. Введите значение pin-кода по умолчанию — 12345678 или свой pin-код, если он был установлен при настройке Рутокена.

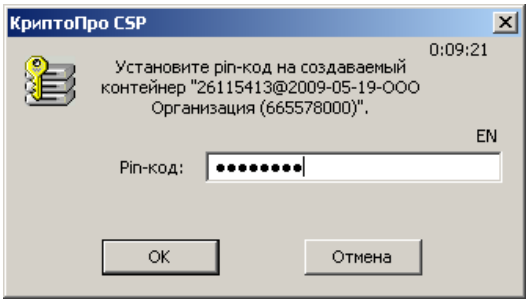

Рис. 14. Окно ввода pin-кода для Рутокена

- для дискеты (рис. 15) – устанавливать пароль не обязательно.

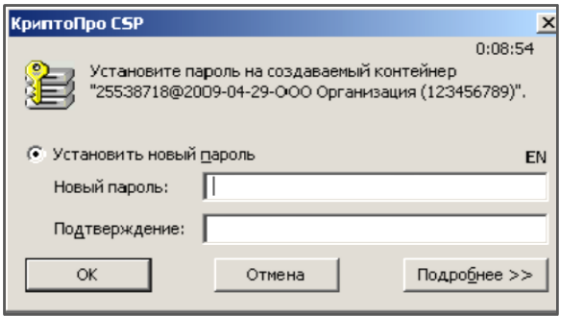

Рис. 15. Окно ввода пароля для дискеты

Обратите внимание, если пароль будет утерян, то дальнейшая работа в системе станет невозможной.

13. Нажмите **ОК**. Создается запрос на сертификат, открывается файл запроса и окно печати.

14. Распечатайте бланк запроса. Один экземпляр запроса, подписанный владельцем сертификата, необходимо отправить в сервисный центр.

Если с рабочего места, на котором формируется запрос, нет возможности распечатать бланк запроса, сохраните его, нажав на кнопку **Сохранить бланк запроса**, и распечатайте с другого рабочего места.

Сохранить бланк запроса на сертификат можно только в текущем сеансе работы.

Формирование запроса на сертификат завершено. Запрос отправлен в Удостоверяющий центр.

15. Дождитесь обработки запроса. Не закрывайте программу, т.к. обычно запрос обрабатывается 10-20 минут.

    Чтобы проверить статус сертификата нажмите **Обновить.**

    - Если напротив сертификата появляется статус «Сертификат готов», перейдите к установке сертификата (пункт 16).
    - Если через обозначенное время сертификат не готов, закройте программу и проверьте готовность сертификата позже, выполнив пункты 1 – 3.

    В соответствии с регламентом Удостоверяющего центра сертификаты выдаются в течение 3-х рабочих дней.

16. Если сертификат готов, нажмите **Установить.**
17. Если в качестве ключевого носителя используется Рутокен, в открывшемся окне введите pin-код (см. пункт 12) и нажмите **ОК**.
18. Дождитесь завершения установки. Напротив сертификата появляется статус «Сертификат установлен». Нажмите **Выход.**

Установка сертификата завершена.

3.2. Установка сертификата с носителя

Если сертификат уже был получен в сервисном центре при подключении к системе (или находится на ключевом носителе), выполните следующие действия:

1. В строке интернет-браузера введите адрес веб-диска https://install.kontur.ru/diadoc**.**
2. Нажмите на кнопку **Начать проверку** и дождитесь окончания проверки. Откроется страница для запроса и установки сертификата (см. рис. 7).
3. Нажмите на кнопку **Установить сертификат ЭЦП**. Открывается окно **Установка сертификатов** (см. рис. 16), в котором отображается запись о сертификате.

*Если запись о сертификате не отображается, вставьте ключевой носитель в компьютер и нажмите **Обновить.***

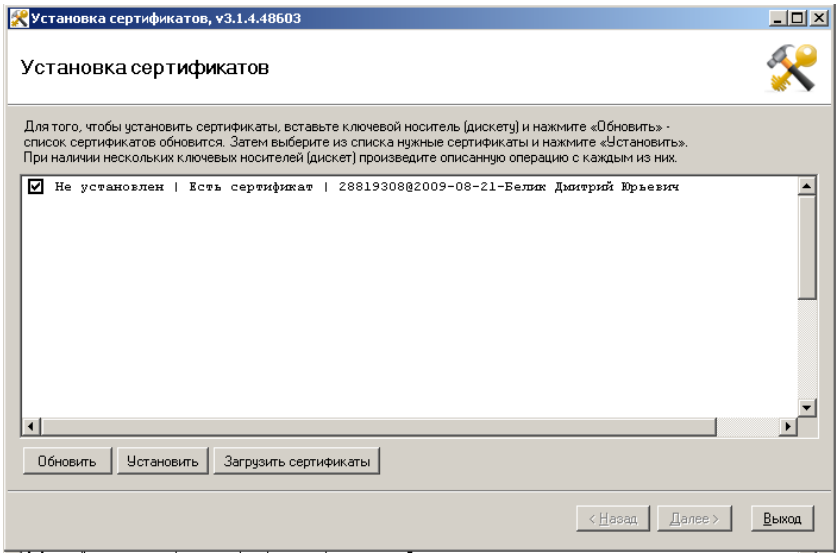

Рис. 16. Окно установки сертификата

4. Убедитесь, что в записи о сертификате указано «Не установлен | Есть сертификат», перейдите к пункту 4.

    Если указано «Не установлен | Нет сертификата»:

- Для Рутокена, Рутокена Лайт – свяжитесь с сервисным центром.
- Для дискеты – выделите строку с записью, нажмите **Загрузить сертификаты**. В открывшемся окне выберите сертификат (размещен на диске 3.5”) и нажмите **ОК**.

5. Выделите строку с сертификатом и нажмите **Установить.**
6. В открывшемся окне установки pin-кода/пароля на ключевой контейнер:
   - для Рутокена, Рутокена Лайт (см. рис. 14) – pin-код обязателен. Введите значение pin-кода по умолчанию — 12345678 или свой pin-код, если он был установлен при настройке Рутокена.
   - для дискеты (см. рис. 15) – устанавливать пароль не обязательно.
7. Нажмите **ОК**. Дождитесь завершения установки. В записи о сертификате указано: «Установлен | Есть сертификат».
8. Нажмите **Выход.**

Установка сертификата завершена.

4. Настройка проброса смарт-карт

Настройте проброс смарт-карт с терминала на сервер (за помощью обратитесь к своему системному администратору).

Настройка проброса смарт-карт необходима для корректной работы Рутокена на терминальном сервере.

5. Установка сертификата на терминальном сервере

Работа с локальным закрытым ключом в терминальной сессии возможна только в том случае, если ключ находится на Рутокене.

Для установки сертификата выполните следующее:

1. Вставьте Рутокен в USB-порт локального компьютера.
2. Для установки сертификата на терминальный сервер, следует войти в систему под администратором. В терминальной сессии нажмите **Пуск / Все программы / Крипто-Про / КриптоПро CSP**.
3. Выберите вкладку **Сервис** и нажмите на кнопку **Просмотреть сертификаты в контейнере** (рис. 17).

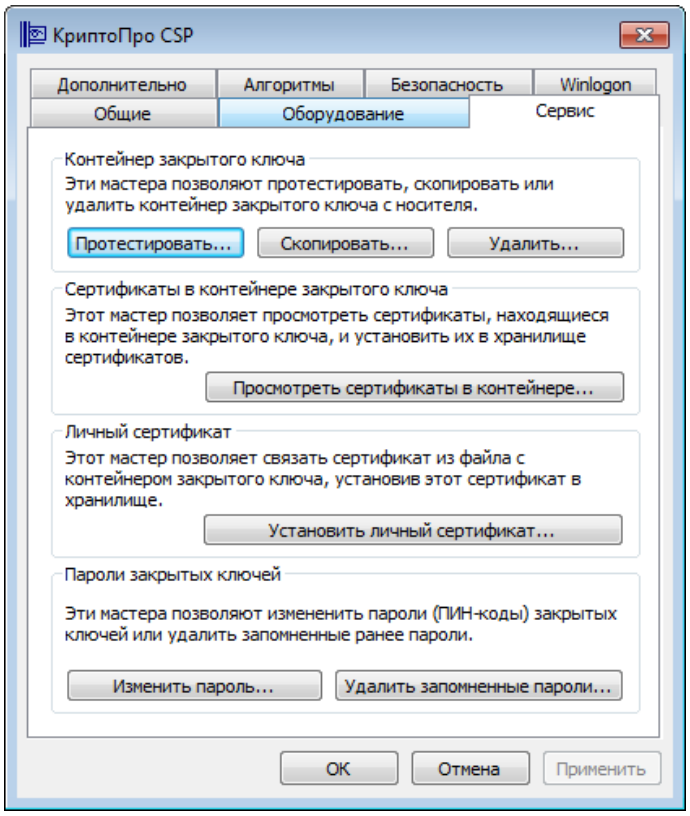

Рис. 17. Установка сертификата с помощью КриптоПро

4. В открывшемся окне нажмите на кнопку **Обзор** (рис. 18).

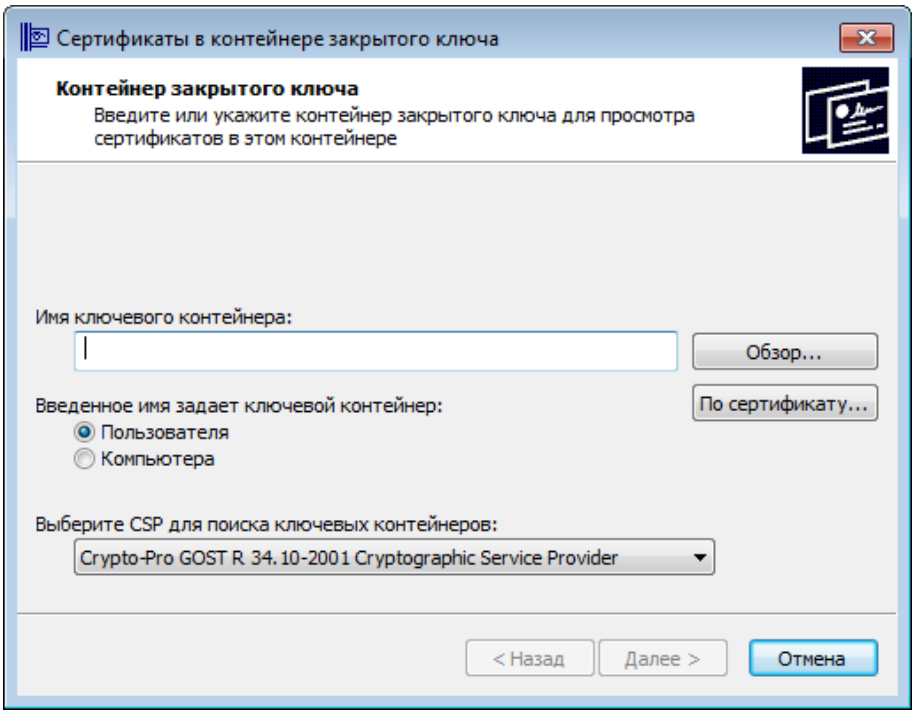

Рис. 18. Окно выбора ключевого контейнера

5. Выберите сертификат и нажмите **OK** (рис. 19).

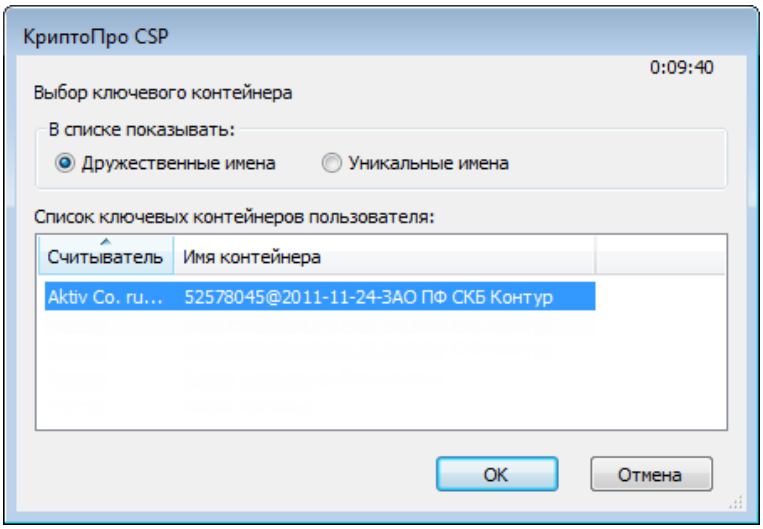

Рис. 19. Окно со списком ключевых контейнеров

6. Нажмите **Далее** (рис. 20). Откроется окно просмотра сертификата с указанием ФИО владельца ключа и сроком действия сертификата.

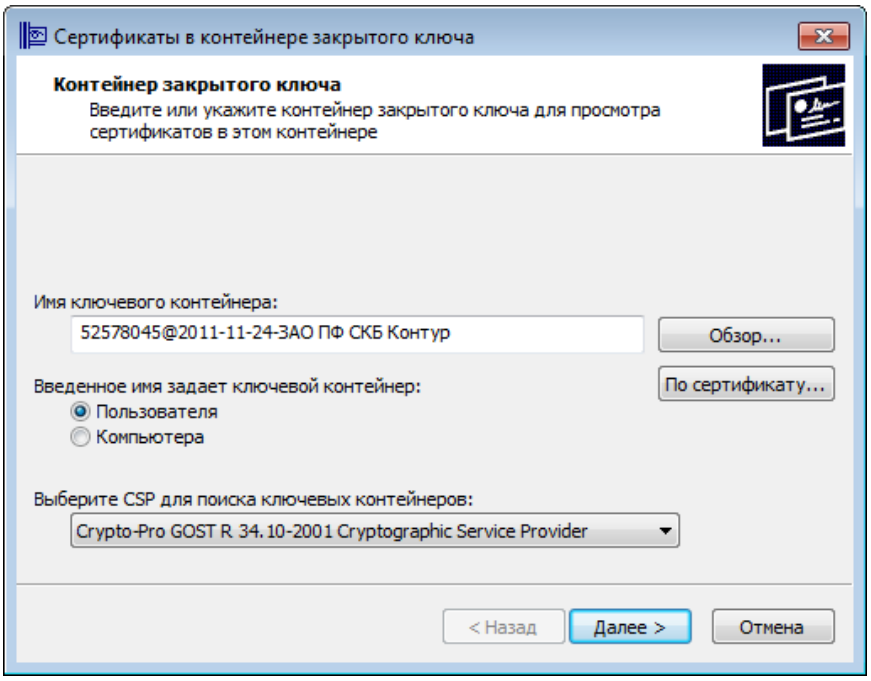

Рис. 20. Окно с выбранным контейнером закрытого ключа

7. Проверьте данные и нажмите на кнопку **Установить** (рис. 21).

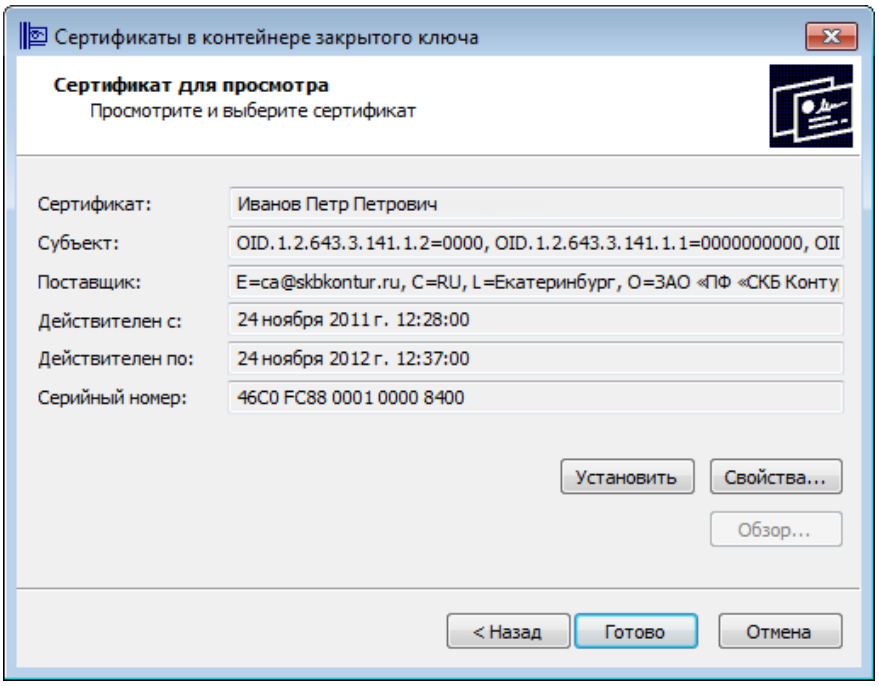

Рис. 21. Окно просмотра сертификата

8. При успешной установке сертификата на экране появится сообщение «Сертификат был установлен в хранилище «Личные» текущего пользователя». Нажмите **Ок** (рис. 22).

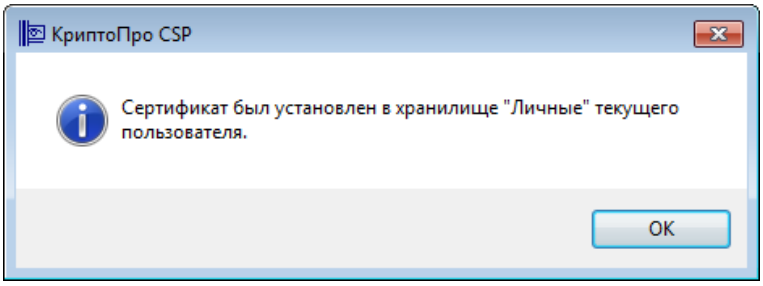

Рис. 22. Сообщение об успешной установке сертификата

После установки сертификата можно приступить к работе с модулем «Диадок» для 1С в терминальном режиме.