Приложение 2. Установка и настройка программ криптозащиты

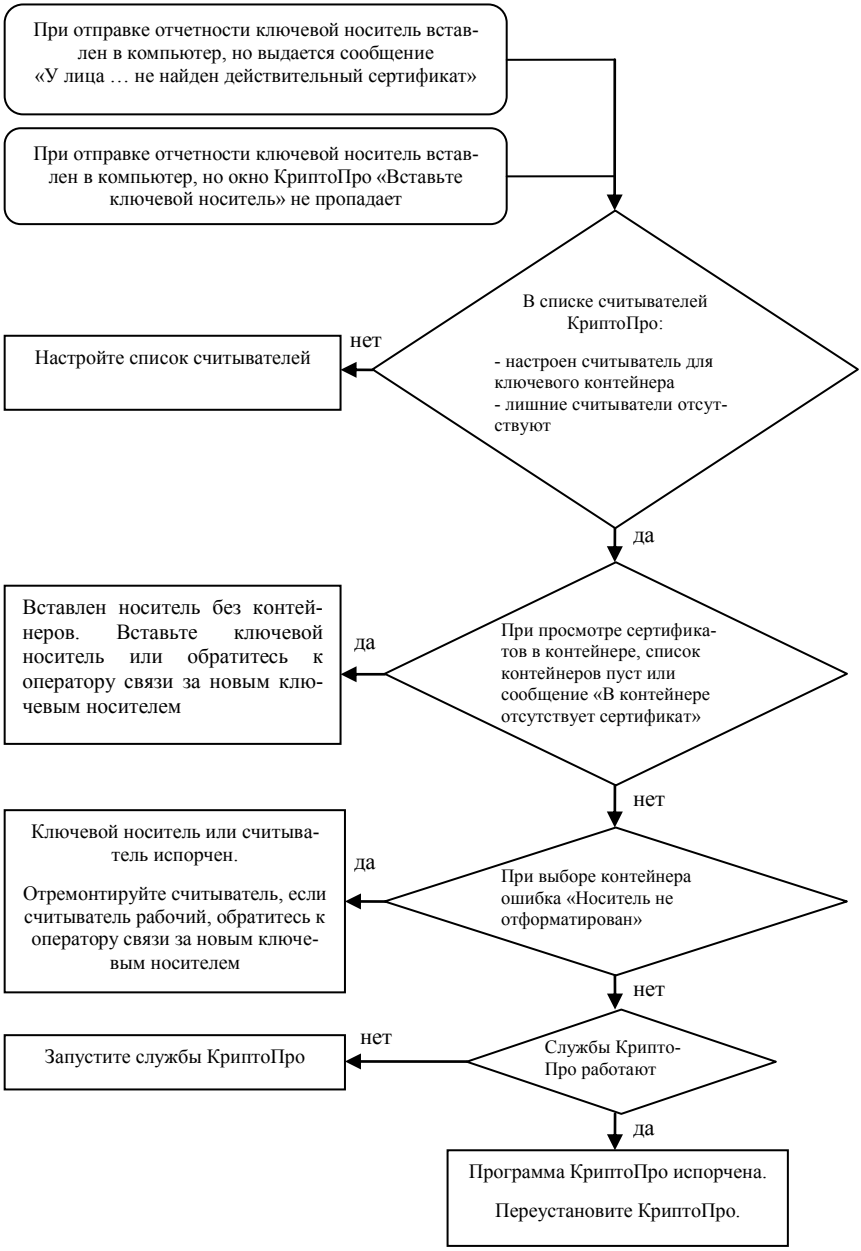
Общие сведения

Для работы с ключами подписи (ЭП), а именно отправки и получения документов или отчетов, может использоваться одна из существующих систем криптозащиты: **СКЗИ** «**КриптоПро CSP**», «**Signal-COM CSP**», «**LISSI-CSP**», «**VipNet CSP**». Программа устанавливается на той рабочей станции, на которой происходит отправка и получение отчетности.

Для установки и удаления СКЗИ требуется наличие у пользователя прав администратора.

КриптоПро CSP

Решение проблем



Переустановка СКЗИ «КриптоПро CSP»

Установка программы на рабочей станции происходит автоматически при установке системы СБИС. Необходимость в переустановке программы возникает, если:

1. Она не была установлена автоматически при инсталляции СБИС.
2. Требуется перенести доставку электронной отчетности на другой компьютер.
3. Возникли проблемы доставки отчетности.

Для того чтобы переустановка программы криптозащиты прошла корректно, ее необходимо удалить и установить заново.

Удалить КриптоПро CSP

Для удаления КриптоПро выполните «Пуск/ Настройка/ Панель управления/ **Установка и удаление программ (Программы и компоненты)**». Найдите в списке программ **КриптоПро CSP** и нажмите «**Добавить/ Удалить**». После того, как программа будет удалена, перезагрузите компьютер.

Установить КриптоПро CSP

Программа установки **КриптоПро CSP** будет загружена на ваш компьютер при соединении с оператором связи. Для этого:

1. В СБИС откройте карточку плательщика (меню «Контрагенты/ Налогоплательщики») и запустите «Мастер создания налогоплательщика». Ничего не меняя, пройдите до шага 2.
2. Установите флаг в поле «Обновить информацию о лицензиях» нажмите «Далее».
3. После соединения с оператором появится сообщение о получении СКЗИ и серийного номера продукта (при установке он автоматически пропишется в реестре). Нажмите Ок.

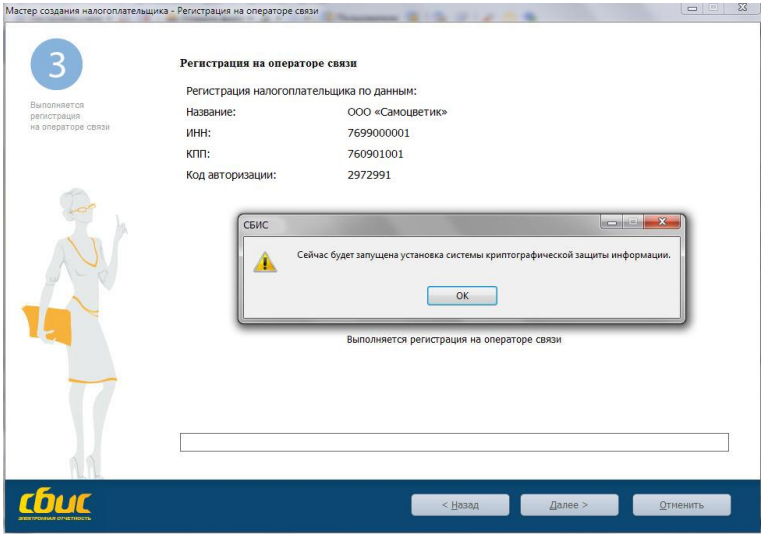


Рис. П 2-1 – Настройка считывателя

4. Запустится мастер установки СКЗИ, полученной по каналам связи. Пройдите по мастеру. По окончании установки, программа предложит выполнить перезагрузку компьютера. Оставьте опцию «Да, перезагрузить сейчас».
5. В открывшемся далее окне «Свойства КриптоПро CSP» нажмите кнопку «Ввод лицензии». Введите серийный номер.
6. Далее последует перезагрузка компьютера. После перезагрузки в корневое хранилище сертификатов Windows необходимо установить сертификат удостоверяющего центра (подробные инструкции приводятся в Базе знаний).

Если по каким-то причинам перезагрузка не была выполнена автоматически, выполните ее вручную.

7. Убедитесь в том, что установленный сертификат стал доступен в системе СБИС. Для этого войдите в программу, в карточке организации перейдите на закладку «Сертификаты». В поле «Статус» должна появиться запись «Сертификат действителен».

Просмотр и настройка считывателя

Как правило, ключевой носитель выдается владельцу ключа на защищенном носителе (Рутокен или eToken), для использования которого требует-

ся установка драйвера и настройка считывателей. Рассмотрим настройку на примере Рутокен.

1. Драйвер для Рутокен можно найти на установочном диске в каталоге «Программы» или на сайте поставщика.
2. Запустите файл установки. Следуйте инструкциям мастера. При необходимости – перезагрузите компьютер.
3. Все считыватели должны добавиться автоматически. Считыватель Рутокен определяется СКЗИ как "Aktiv Co. ruToken 0","Aktiv Co. ruToken 1","Aktiv Co. ruToken 2". Эти имена соответствуют одновременному последовательному подключению нескольких носителей к разным USB-портам.

Если считыватели в СКЗИ автоматически не добавились, то выполните «Пуск/ Настройка/ Панель управления/ КриптоПро CSP».

1. В открывшемся окне перейдите на вкладку «Оборудование» и нажмите кнопку «Настроить считыватели»:

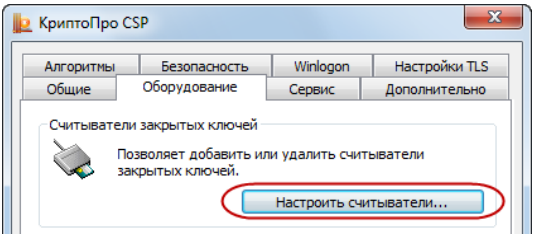


Рис. П 2-2 – Настройка считывателя

В результате откроется список установленных считывателей:

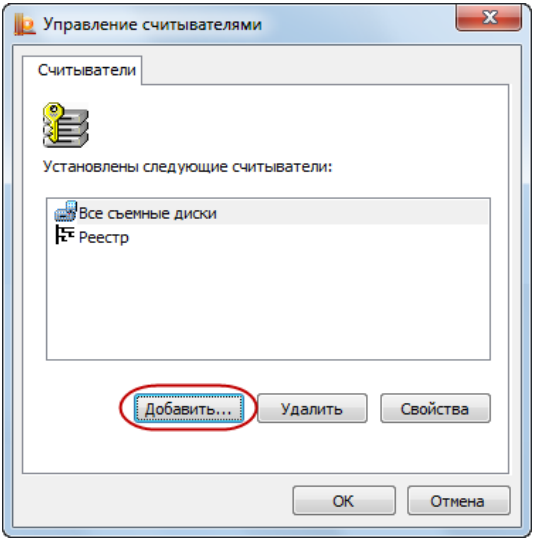


Рис. П 2-3 – Список установленных считывателей

Вставьте Рутокен. Нажмите «**Добавить**» и следуйте указаниям мастера установки считывателя.

2. В списке считывателей выберите последовательно «Aktiv Co. ruToken 0», «Aktiv Co. ruToken 1», «Aktiv Co. ruToken 2».

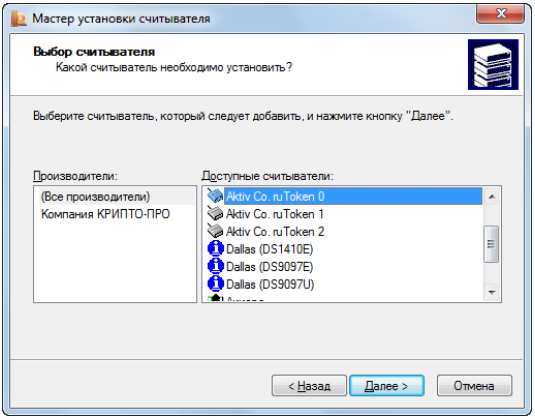


Рис. П 2-4 – Добавление считывателя для Рутокен

В следующем окне, не меняя имя считывателя, нажмите «Далее», затем «Готово».

3. После того, как все считыватели появятся в списке установленных считывателей, закройте окно свойств и перезагрузите компьютер.

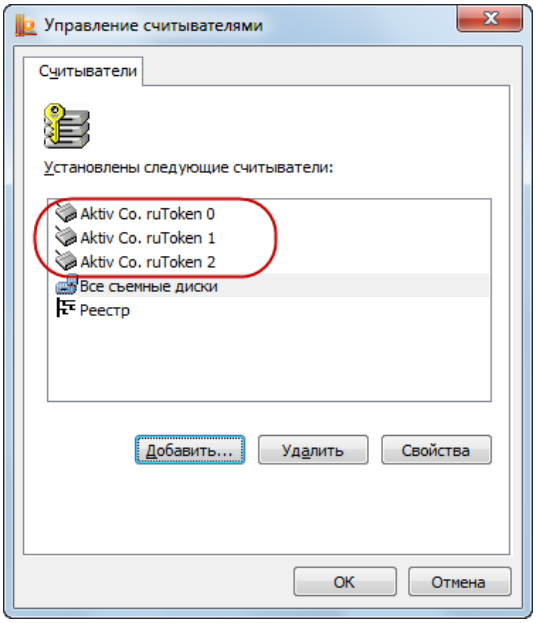


Рис. П 2-5 – Считыватели для Рутокен

Копирование ключевого контейнера

Копирование контейнера с ключевой информацией без санкции владельца ключа запрещено.

Для того, чтобы скопировать ключевой контейнер:

1. Вставьте ключевой носитель в считывающее устройство (считыватель).
2. Выполните «**Пуск/ Настройка/ Панель управления/ КриптоПро CSP**».
3. В открывшемся окне перейдите на закладку «Сервис» и нажмите кнопку «Скопировать».

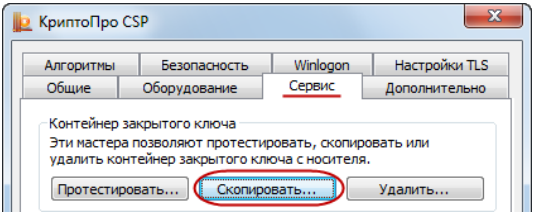


Рис. П 2-6 – Копирование ключевого контейнера

4. В окне копирования контейнера нажмите «Обзор» и выберите в открывшемся списке доступных контейнеров, тот который требуется скопировать. Имя выбранного контейнера появится в поле «Имя ключевого контейнера».

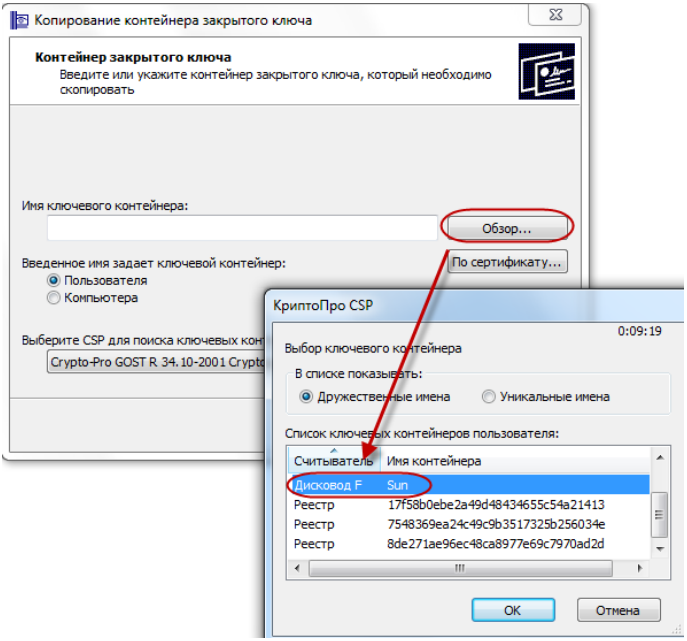


Рис. П 2-7 – Выбор ключевого контейнера для копирования

5. В следующем окне задайте имя копии контейнера.

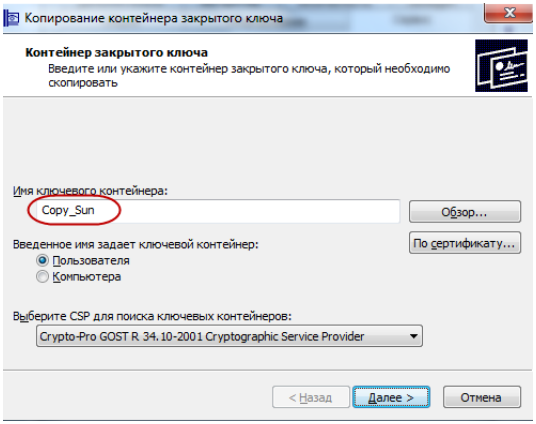


Рис. П 2-8 – Ввод имени ключевого контейнера

6. Далее вставьте носитель, на который будет производиться копирование и выберите из списка считыватель.

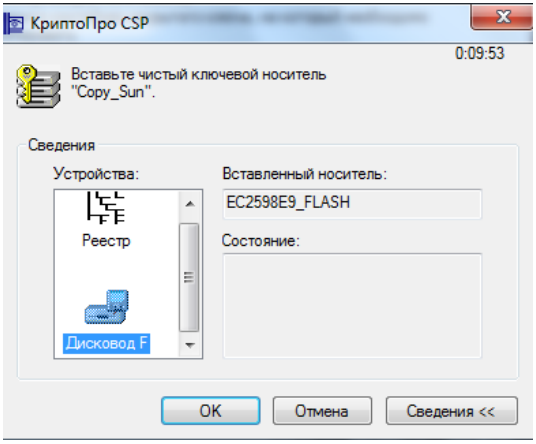


Рис. П 2-9 – Выбор считывателя для сохранения копии контейнера

7. В следующем окне введите пароль на создаваемый контейнер. Если пароль не требуется, оставьте поля пустыми. Нажмите «ОК» – копия будет сохранена.

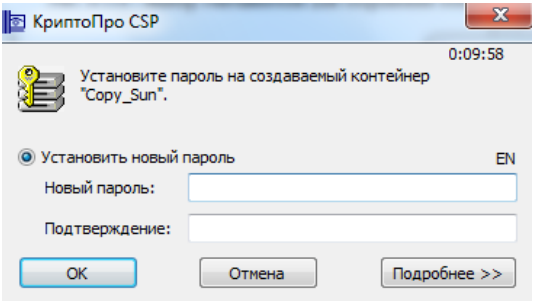


Рис. П 2-10 – Установка пароля на создаваемый контейнер

8. Убедитесь, что копия действительно находится на указанном считывателе. Для этого в свойствах КриптоПро CSP перейдите на закладку «Сервис» и нажмите кнопку «Просмотреть сертификаты в контейнере».

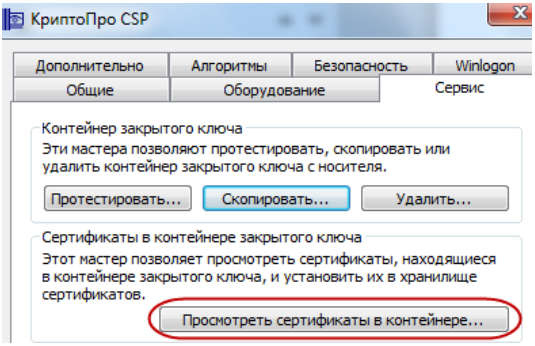


Рис. П 2-11 – Просмотр сертификатов в контейнере

9. В открывшемся окне выбора контейнера нажмите кнопку «Обзор» и убедитесь, что в списке доступных контейнеров присутствует созданная вами копия.