## Установка средств криптографической защиты (СКЗИ)

Для работы с сертификатами и подписания отчетов ЭП необходимо приобрести и установить средство криптографической защиты информации(СКЗИ) КриптоПро CSP 3.6, VipNetCSP 3.2, Signal-COMCSP 2.2, ЛИССИ-CSP 1.17 или другое СКЗИ (в случае если СКЗИ ранее не приобреталось и не устанавливалось).

В качестве СКЗИ рекомендуется использоватьследующие СКЗИ:

* + - * КриптоПро CSP 3.6. Информацию о порядке приобретения КриптоПро CSP и инструкцию по установке можно получить на официальном сайте компании «Крипто-Про» <http://www.cryptopro.ru/cryptopro/default.aspx>.

КриптоПроSharpei - программный продукт, позволяющий использовать средство криптографической защиты информации КриптоПро CSP на платформе Microsoft .NetFramework.

* VipNetCSP 3.2. Информацию о порядке приобретения VipNetCSP и инструкцию по установке можно получить на официальном сайте компании «ИнфоТеКС» <http://www.infotecs.ru/downloads>.
* Signal-COMCSP 2.2. Информацию о порядке приобретения Signal-COMCSP и инструкцию по установке можно получить на официальном сайте компании«Сигнал-КОМ» <http://www.signal-com.ru/products/crypt/signal-com>.
* ЛИССИ-CSP 1.17.Информацию о порядке приобретения ЛИССИ-CSP и инструкцию по установке можно получить на официальном сайте компании «ЛИССИ-Софт»<http://soft.lissi.ru/products/skzi/lissi-csp/>.

## Получение закрытого ключа и сертификата удостоверяющего центра (УЦ)

В целях обеспечения безопасности и достоверности статистической отчетности и работе по протоколу httpsнеобходимо получить и установить на вашем компьютере сертификат удостоверяющего центра (УЦ), который выдал сертификат для SSL-соединения и сам сертификат SSL сервера. Сертификат УЦ необходимо добавить в доверенные корневые сертификаты (TrustedRootCertificationAuthorities).

## Получение закрытого ключа и сертификата открытого ключа ЭП в доверенном УЦ

В целях обеспечения безопасности и достоверности статистической отчетности, формируемой и отсылаемой Респондентом в процессе электронного сбора статистической отчетности, все отчеты, заполняемые Респондентом, перед оправкой в ТОГС должны быть подписаны Электронной подписью (ЭП) Респондента.

Для предоставления статистической отчетности в электронном виде необходимо получить:

закрытый ключ, при помощи которого будет формироваться ЭП (подпись отчетов) и который будет гарантировать подлинность заполнения и предоставления отчета Респондентом;

Сертификат открытого ключа Респондента, который необходимо будет передать в ТОГС, для осуществления проверки подлинности отчетности, присланной Респондентом.

Закрытый ключ и открытый ключ формируются в паре. Для их получения вам необходимо оформить заявку в доверенном Удостоверяющем центре (УЦ).

Порядок получения закрытого ключа и сертификата открытого ключа выглядит следующим образом:

1. Необходимо обратиться в один из УЦ, входящих в сеть Доверенных УЦ Росстата, с просьбой изготовления и предоставления ключевой информации. Перечень доверенных УЦ, в которые можно обратиться, определяет ТОГС, перечень должен быть предоставлен Респонденту Администратором ТОГС. Если перечень доверенных УЦ отсутствует, необходимо обратиться в ТОГС с просьбой выслать перечень доверенных УЦ.
2. Информация по порядку получения ключа ЭП размещена на сайте конкретного УЦ.
3. После получения закрытого ключа и сертификата открытого ключа ЭП в одном из доверенных УЦ необходимо установить сертификат закрытого ключа в Системное хранилище сертификатов на компьютере, где планируется использование on-lineмодуля или хранить у себя на ключевом носителе.
4. Сертификат открытого ключа ЭП необходимо загрузить в on-line-модуль при регистрации или загрузить в on-line (в пункте меню «Профиль-Сертификаты» )перед отправкой первого отчета. При помощи данного сертификата будет осуществляться проверка подлинности отчетов, полученных от Респондента.

## Работа с ключами на ключевых носителях

### Обеспечение доступности секретного ключа сертификата в КриптоПроCSP

1. Вставить флэш-диск в компьютер и посмотреть, под какой буквой подключился диск.
2. Удостовериться, добавлен ли данный диск в КриптоПро как ключевой носитель. Для этого необходимо выполнить команду Пуск → Все программы → CryptoPro→ КриптоПро CSP, перейти на закладку «Оборудование» и нажать кнопку «Настроить считыватели».

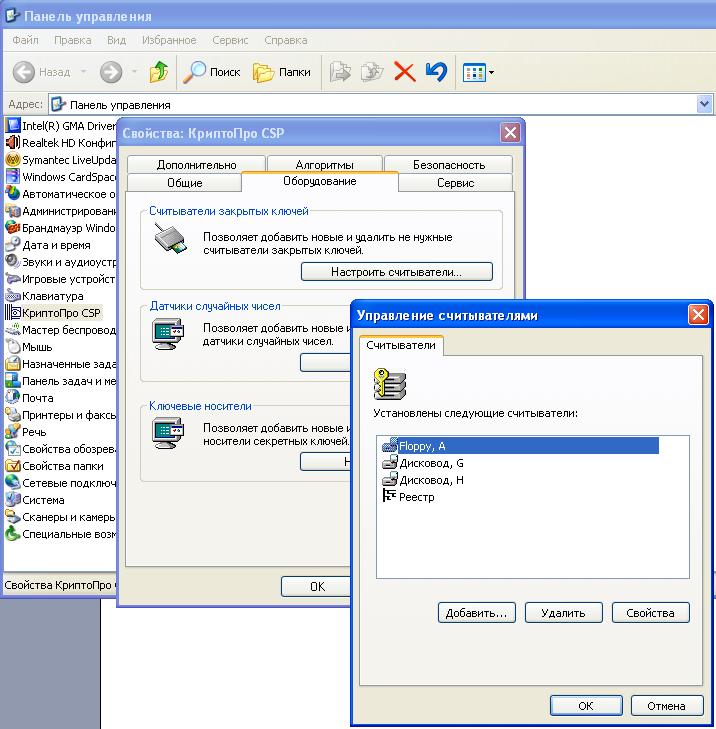


Рис. 2Проверка ключевого носителя

В списке «Установлены следующие считыватели» должен присутствовать дисковод с именем подключенного диска.

1. Если дисковода с таким именем в списке нет, то его следует добавить, нажав кнопку «Добавить…». Начнет работать мастер установки считывателя. В первом окне мастера установки считывателя необходимо нажать кнопку «Далее >». Откроется окно для выбора считывателя.

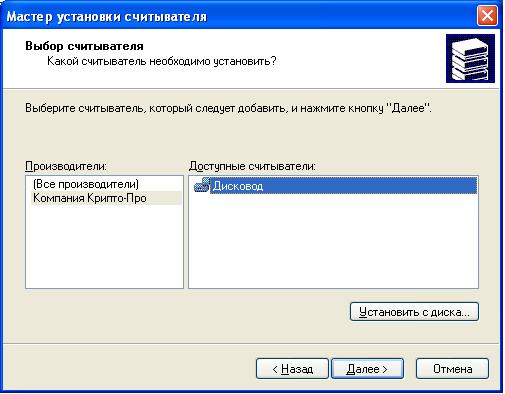


Рис. 3Выбор считывателя

1. В списке «Производители» выбрать «Компания КриптоПро», а в Списке «Доступные считыватели» выбрать «Дисковод» и нажать кнопку «Далее >». Откроется окно выбора соединения.

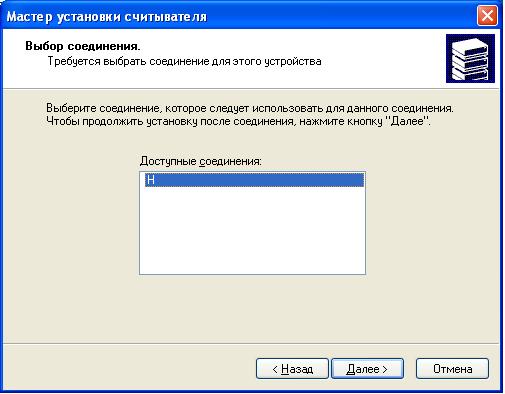


Рис. 4Выбор соединения

1. В списке «Доступные соединения» выбрать название (букву) флеш-диска, подключенного к системе, и нажать кнопку «Далее >». Откроется окно «Имя считывателя».

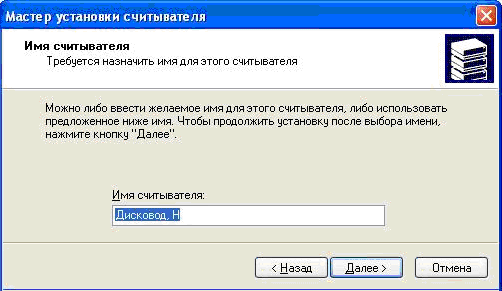


Рис. 5Выбор имени считывателя

1. В случае необходимости, измените «Имя считывателя» и нажмите кнопку «Далее >». Откроется окно завершения работы мастера установки считывателя.

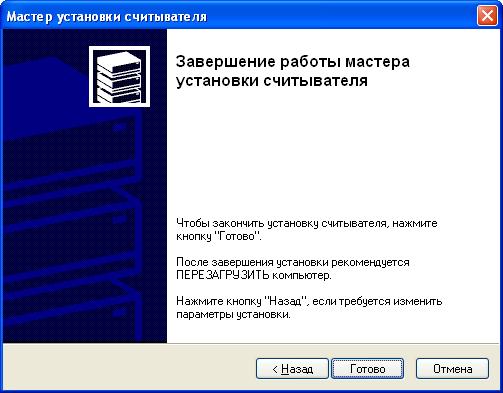


Рис. 6Окно завершения работы мастера установки считывателя

1. Для завершения установки нажмите кнопку «Готово».

### Обеспечение доступности секретного ключа сертификата в VipNetCSP

1. Вставить флэш-диск в компьютер и посмотреть, под какой буквой подключился диск.
2. Удостовериться, добавлен ли данный диск в ViPNet как ключевой носитель. Для этого необходимо выполнить команду Пуск → Все программы → ViPNet → ViPNet CSP.
3. В окне программы **ViPNet CSP** выберите раздел **Контейнеры**.

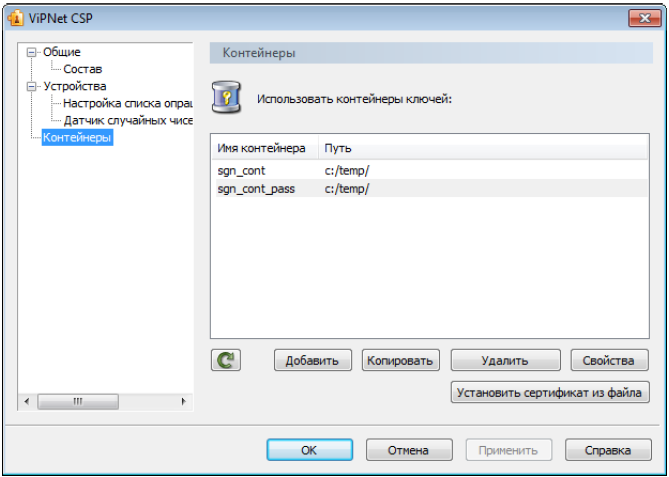


Рис. 7Панель управления контейнерами

1. В разделе **Контейнеры** нажмите кнопку **Добавить**.
2. В окне **ViPNet CSP - инициализация контейнера ключей** нажмите кнопку **Обзор**.

* Если контейнер хранится на жестком диске, в окне **Обзор папок** укажите путь к папке, содержащей контейнер.
* Если контейнер хранится на съемном флэш-диске, в окне **Обзор папок** укажите этот съемный диск. В поле **Папка на диске** автоматически будет подставлен путь, например E:\Infotecs\Containers.

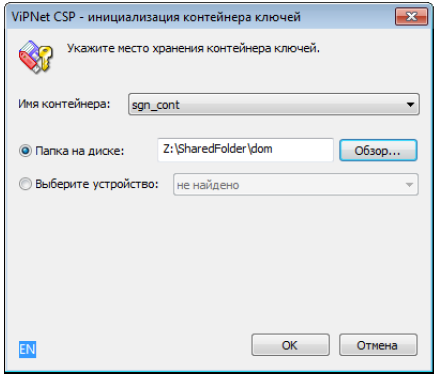


Рис. 8 Инициализация контейнера ключей из папки

1. Из списка **Имя контейнера** выберите файл контейнера или оставьте значение по умолчанию.
2. Нажмите **ОК**. В окне **Контейнер ключей** появится сообщение об успешном добавлении контейнера и предложение по установке сертификата в хранилище. Для работы с сертификатами их необходимо установить в хранилище текущего пользователя.

Нажмите кнопку **Да**, сертификаты будут автоматически установлены в хранилище пользователя.

Если сертификаты устанавливать не требуется (или установка будет происходить вручную), нажмите **Нет**.

Для просмотра списка сертификатов в контейнере нажмите кнопку **Сертификаты**.

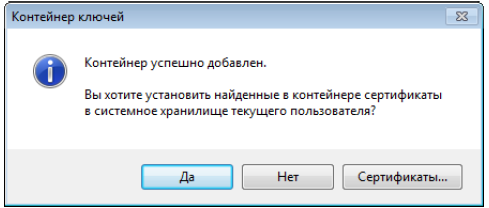


Рис. 9 Установка сертификатов из контейнера в хранилище

1. После установки (или отмены установки) сертификатов в хранилище в списке доступных контейнеров появится добавленный контейнер.

### Обеспечение доступности секретного ключа сертификата в Signal-COMCSP

Если в качестве носителя ключевой информации используется дискета или flash-носитель, не требуется выполнять никаких дополнительных настроек - программа сама обнаружит и запомнит используемый носитель ключевой информации.

### Обеспечение доступности секретного ключа сертификата в ЛИССИ-CSP

Для управления ключевыми контейнерами «ЛИССИ-CSP» используется утилита «Управление контейнерами». Для запуска утилиты выполните команду Пуск→ Все программы → LISSI → ЛИССИ-CSP → Управление контейнерами.

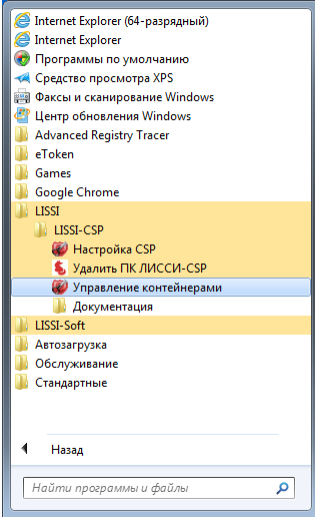


Рис. 10 Управление контейнерами

После запуска утилиты в окне «Контейнеры» появится иерархический список носителей, поддерживаемых «ЛИССИ-CSP» и присутствующих в данный момент. Для отображения съёмных носителей (электронные USB ключи, флэшка, дискета) необходимо, чтобы они были вставлены в USB-порт (в случае с дискетой в дисковод)компьютера.

Носитель может содержать список представленных на нём ключевых контейнеров. Если носитель не содержит список, то это означает, что на нём нет ключевых контейнеров «ЛИССИ-CSP».

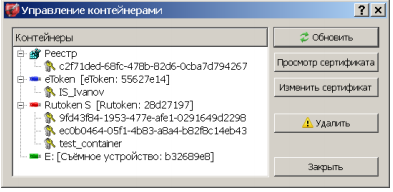


Рис. 11 Контейнеры

Если ключевой носитель был вставлен в порт компьютера после запуска утилиты,

то для его отображения в окне утилиты необходимо нажать кнопку «Обновить».