## 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, VipNet CSP 3.2, Signal-COM CSP 2.2, ЛИССИ-CSP 1.17 или другое СКЗИ (в случае если СКЗИ ранее не приобреталось и не устанавливалось).

В качестве СКЗИ рекомендуется использовать следующие СКЗИ:

1. 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/.
2. VipNet CSP 3.2. Информацию о порядке приобретения VipNet CSP и инструкцию по установке можно получить на официальном сайте компании «ИнфоТеКС» http://www.infotecs.ru/downloads.
3. Signal-COM CSP 2.2. Информацию о порядке приобретения Signal-COM CSP и инструкцию по установке можно получить на официальном сайте компании «Сигнал-КОМ» http://www.signal-com.ru/products/crypt/signal-com.
4. 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/>.

Плагин подписи позволяет подписывать и выполнять проверку ЭП в операционных системах не ниже следующих версий:

* MacOS 10.14;
* Linux Ubuntu Bionic Beaver 18.04;
* Linux Debian 9.0 Stretch;
* Linux CentOS 8.

Электронная подпись работает корректно в web-браузерах не ниже перечисленных версий:

* Google Chrome (версия не ниже 71);
* Mozilla Firefox (версия не ниже 67).
* Safari (версия не ниже 12).

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

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

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

В целях обеспечения безопасности и достоверности статистической отчетности, формируемой и отсылаемой организацией, в т.ч. уполномоченным лицом в процессе электронного сбора статистической отчетности, все отчеты, перед оправкой в ТОГС должны быть подписаны электронной подписью (ЭП) организации.

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 организацией;
* сертификат открытого ключа организации, который необходимо будет передать в ТОГС, для осуществления проверки подлинности отчетности, присланной организацией.

Закрытый ключ и открытый ключ формируются в паре. Для их получения необходимо оформить заявку в доверенном 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 организации 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 выбранного 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-line модуля или хранить у себя на ключевом носителе.
4. Сертификат открытого ключа ЭП необходимо загрузить в ON-line-модуль при регистрации или загрузить позднее в разделе «Профиль» пунтка «Сертификаты» перед отправкой первого отчета. При помощи данного сертификата будет осуществляться проверка подлинности отчетов, полученных от организации.

### Установка сертификатов в системное хранилище

В данном разделе описан механизм установки сертификатов, которые являются секретными ключами на ключевых носителях и необходимы для реализации функционала проверки подлинности документов.

1. Запустить КриптоПро CSP.
2. Перейти на вкладку «Сервис».

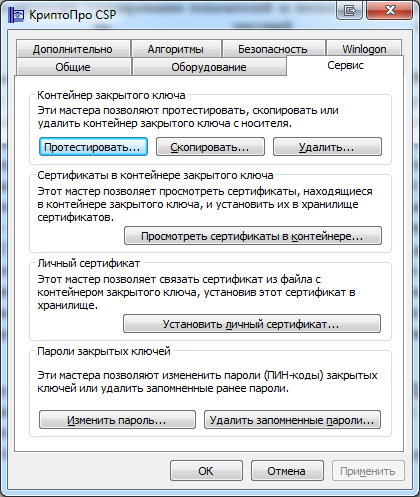


Рисунок 1 – Закладка «Сервис»

1. Нажать на кнопку «Просмотреть сертификаты в контейнеры».
2. В открывшемся окне нажать на кнопку «Обзор». Откроется список ключевых контейнеров.

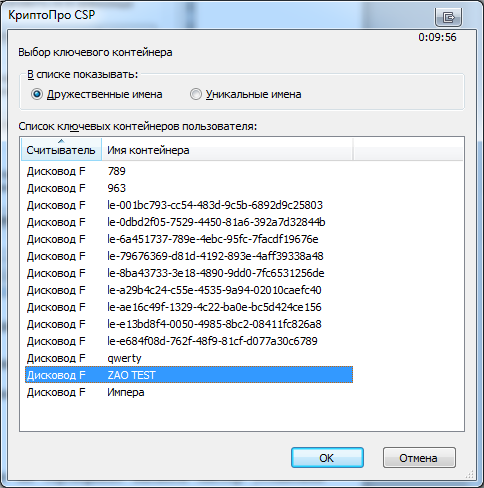


Рисунок 2 – Список контейнеров

1. Выбрать необходимый контейнер и нажать на кнопку **«**OK**»**.
2. В результате в поле «Имя ключевого контейнера» отобразится наименование контейнера.

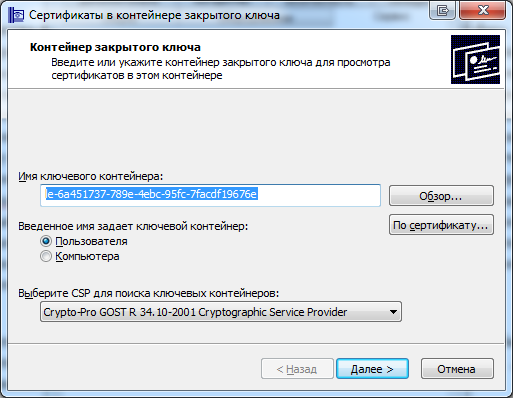


Рисунок 3 – Выбранный контейнер

1. Нажать на кнопку «Далее**»**.

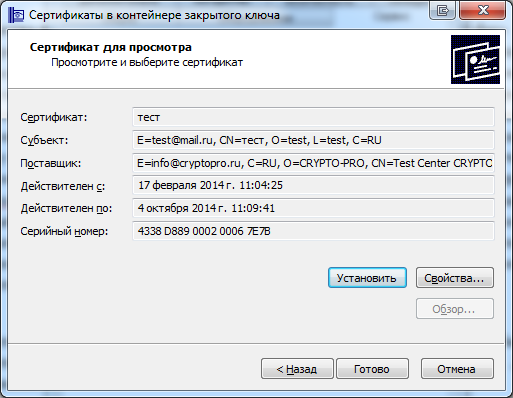


Рисунок 4 – Сведения о сертификате

1. Нажать на кнопку «Готово».
2. Сертификат будет установлен.

Также двойным нажатием левой кнопки мыши на сертификат вызвать мастер установки сертификата (Рисунок 5).

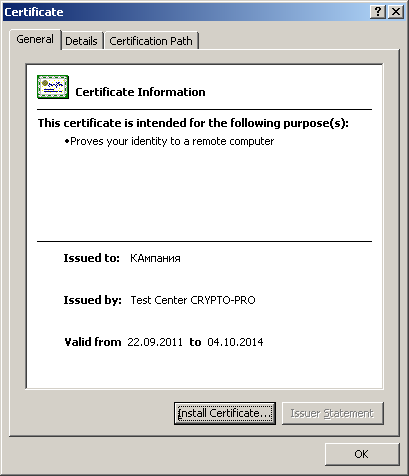


Рисунок 5 – Установка сертификата

В открывшемся окне нажать кнопку «Install Certificate», в окне «Certificate Import Wizard» нажать кнопку «Next» (Рисунок 6).

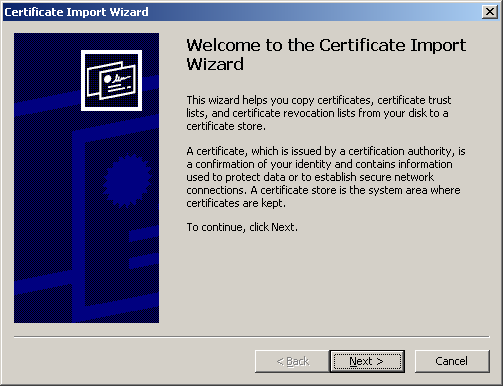


Рисунок 6 – Мастер установки сертификата

Для указания имени хранилища сертификатов нажать кнопку «Обзор» (Browse и выбрать хранилище «Личные» (Personal) и нажать кнопку «ОК» (Рисунок 7). Затем нажать кнопку «Next».

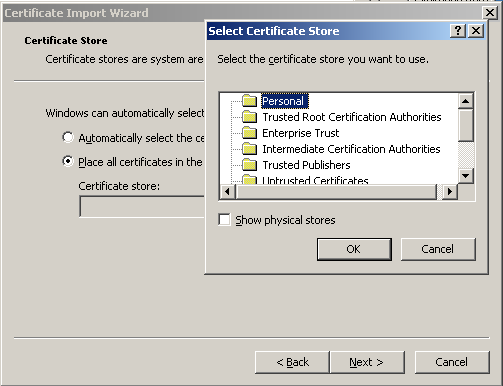


Рисунок 7 – Установка в хранилище текущего пользователя

В открывшемся окне «Completing the Certificate Import Wizard» нажать кнопку «Finish» (Рисунок 8). Процесс установки сертификата завершен.

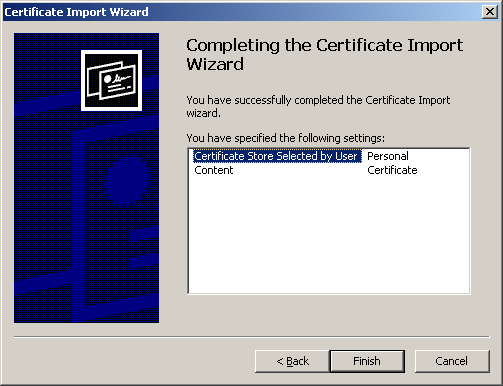


Рисунок 8 – Установка сертификата завершена

## Работа с ключами на ключевых носителях

### Обеспечение доступности секретного ключа сертификата в КриптоПро CSP

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» и перейти на закладку «Оборудование» и нажать кнопку «Настроить считыватели».

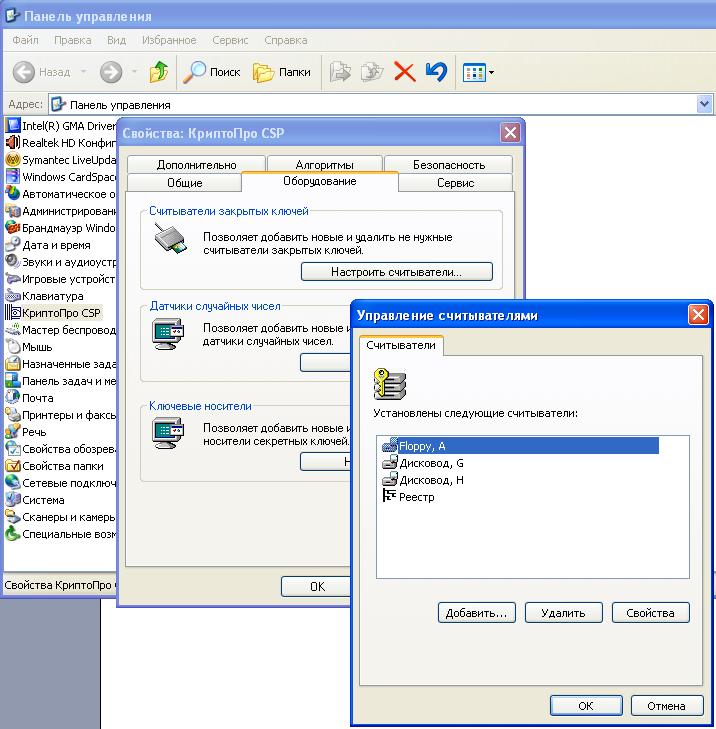


Рисунок 9 – Проверка ключевого носителя

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.

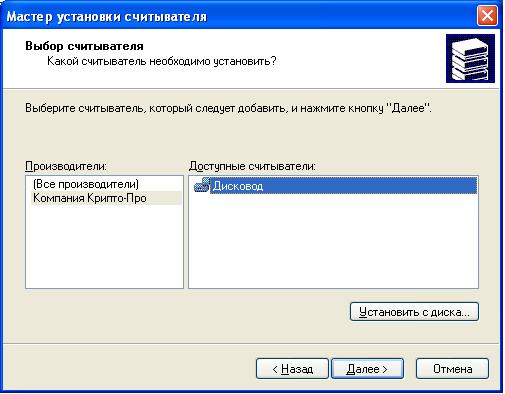


Рисунок 10 – Выбор считывателя

1. В списке «Производители» выбрать «Компания КриптоПро», а в Списке «Доступные считыватели» выбрать «Дисковод» и нажать кнопку «Далее >». Откроется окно выбора соединения (Рисунок 11).

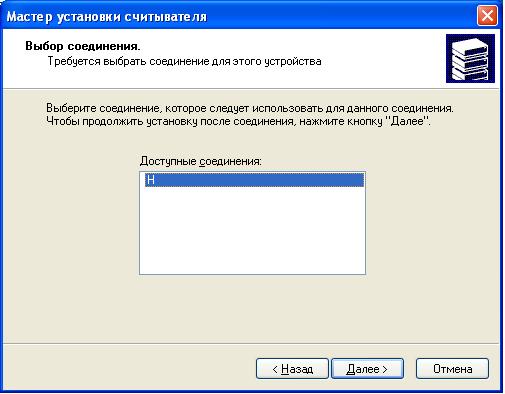


Рисунок 11 – Выбор соединения

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

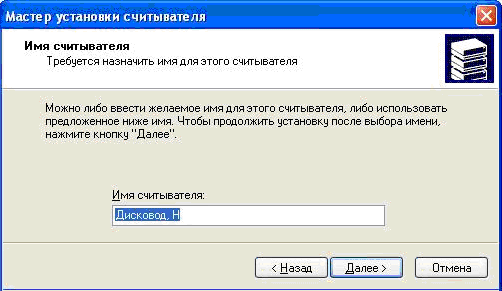


Рисунок 12 – Выбор имени считывателя

1. В случае необходимости изменить «Имя считывателя» и нажать кнопку «Далее >». Откроется окно завершения работы мастера установки считывателя.

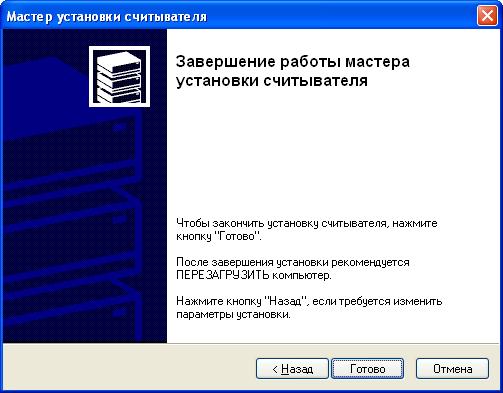


Рисунок 13 – Окно завершения работы мастера установки считывателя

1. Для завершения установки необходимо закрыть окно по кнопке «Готово».

### Обеспечение доступности секретного ключа сертификата в VipNet CSP

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 выбрать раздел «Контейнеры» (Рисунок 14).

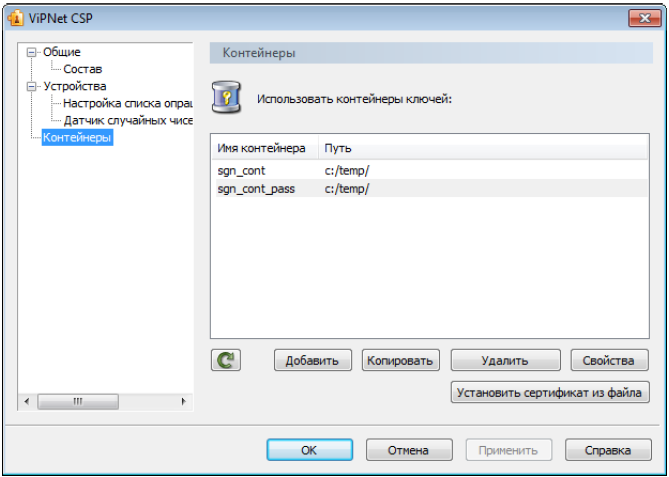


Рисунок 14 – Панель управления контейнерами

1. В разделе «Контейнеры» нажать кнопку «Добавить».
2. В окне ViPNet CSP - инициализация контейнера ключей нажать кнопку «Обзор» (Рисунок 15):

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

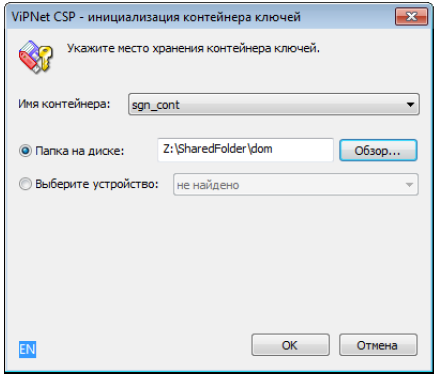


Рисунок 15 – Инициализация контейнера ключей из папки

1. Из списка «Имя контейнера» необходимо выбрать файл контейнера или оставить значение по умолчанию.
2. Нажать «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.

При нажатии кнопки «Да», сертификаты будут автоматически установлены в хранилище пользователя.

Если сертификаты устанавливать не требуется (или установка будет происходить вручную), необходимо нажать «Нет».

Для просмотра списка сертификатов в контейнере необходимо нажать кнопку «Сертификаты» (Рисунок 16).

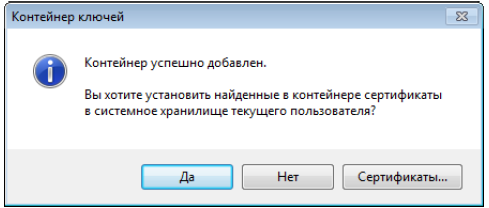


Рисунок 16 – Установка сертификатов из контейнера в хранилище

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

### Обеспечение доступности секретного ключа сертификата в Signal-COM CSP

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 необходимо выполнить команду «Пуск» → «Все программы» → «LISSI» → «ЛИССИ-CSP» → «Управление контейнерами» (Рисунок 17).

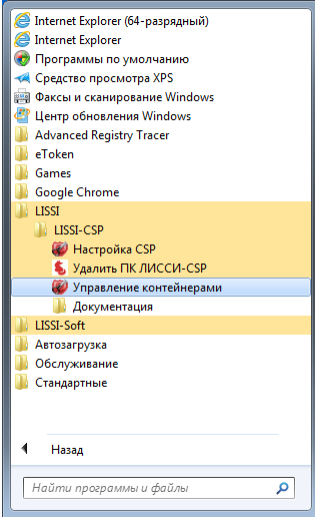


Рисунок 17 – Управление контейнерами

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» (Рисунок 18).

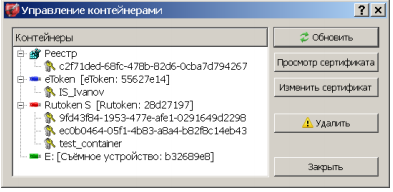


Рисунок 18 – Контейнеры

Если ключевой носитель был вставлен в порт компьютера после запуска утилиты, то для его отображения в окне утилиты необходимо нажать кнопку «Обновить».