

## **Краткая инструкция по установке и переносу программы Фельдгегерь 3.0**

В случае необходимости установки программы Фельдгегерь 3.0 или переноса программы с одного компьютера на другой с сохранением всех документов и настроек программы необходимо воспользоваться следующими инструкциями.

Если требуется перенести Фельдгегерь 3.0 с одного компьютера на другой вместе с базой данных, начните с пункта **1. Создание резервной копии базы данных.**

Если необходимо просто установить Фельдгегерь 3.0, перейдите к пункту **2. Установка программ.**

### **1. Создание резервной копии базы данных**

Запустите программу Фельдгегерь 3.0, откройте меню *Сервис - Параметры*. Укажите папку на компьютере для сохранения резервной копии в поле *Путь к папке резервного копирования*. Нажмите кнопку *Применить* и *Заккрыть*.

Откройте меню *Сервис – Создание резервной копии БД*. Дождитесь окончания процедуры создания резервной копии, резервная копия сохранится в виде архива *Васкурп-  
<дата >-<время>.zip* в указанной папке.

Скопируйте файл резервной копии на компьютер, на который требуется перенести Фельдгегерь 3.0, или на переносной носитель информации, если на компьютере будет переустанавливаться операционная система.

Если ключи для сдачи отчетности хранятся в реестре, то для их переноса (или до переустановки операционной системы) необходимо обратиться за помощью в службу технической поддержки

### **2. Установка программ**

Если ключи для сдачи отчетности хранятся в реестре или на флэш-накопителе, то перейдите к пункту **2.2. Скачайте и установите СКЗИ.**

#### **2.1. Скачайте и установите драйвера для ключевого носителя**

##### **2.1.1. Драйвер ключевого носителя eToken**

[http://download.rus-telecom.ru/aladdin/PKIClient\\_x32\\_5.1\\_SP1.msi](http://download.rus-telecom.ru/aladdin/PKIClient_x32_5.1_SP1.msi) - для 32-битных ОС  
[http://download.rus-telecom.ru/aladdin/PKIClient\\_x64\\_5.1\\_SP1.msi](http://download.rus-telecom.ru/aladdin/PKIClient_x64_5.1_SP1.msi) - для 64-битных ОС

Установите драйвер ключевого носителя eToken, следуя указаниям мастера установки.

##### **2.1.2. Драйвер JaCarta**

В случае, если используется ключевой носитель JaCarta (имеется надпись JaCarta на ключевом носителе), дополнительно необходимо установить программу JC-ClientPRO.

Для Windows XP:

[http://download.rus-telecom.ru/aladdin/JC-PROClient-1.0.2.30\\_x32-0.msi](http://download.rus-telecom.ru/aladdin/JC-PROClient-1.0.2.30_x32-0.msi) - для 32-битных ОС

[http://download.rus-telecom.ru/aladdin/JC-PROClient-1.0.2.30\\_x64-0.msi](http://download.rus-telecom.ru/aladdin/JC-PROClient-1.0.2.30_x64-0.msi) - для 64-битных ОС

Для Windows Vista, 7, 8, 8.1, 10:

[http://download.rus-telecom.ru/aladdin/JC-PROClient-1.5.0.199\\_x32.msi](http://download.rus-telecom.ru/aladdin/JC-PROClient-1.5.0.199_x32.msi) - для 32-битных ОС

[http://download.rus-telecom.ru/aladdin/JC-PROClient-1.5.0.199\\_x64.msi](http://download.rus-telecom.ru/aladdin/JC-PROClient-1.5.0.199_x64.msi) - для 64-битных ОС

Запустите установочный файл и следуйте указаниям мастера установки. Перезагрузите компьютер.

## **2.2. Скачайте и установите СКЗИ**

Скачайте и установите СКЗИ: КриптоПро CSP или LISSI-CSP, в зависимости от того, для какого СКЗИ выпущены ключи. В случае переноса ФЕ на новый ПК выберите в данной инструкции ссылку на то же СКЗИ, что было установлено на предыдущем компьютере. Если вы затрудняетесь определить свой тип СКЗИ, обратитесь за помощью в службу технической поддержки.

**Внимание: не устанавливайте на компьютер два СКЗИ, это приводит к сбою в работе программ и ключей.**

Во избежание конфликта СКЗИ до установки КриптоПро CSP или LISSI-CSP необходимо убедиться, что на ПК не установлено следующее ПО:

- Vipnet CSP
- Домен-К
- Агава CSP
- Персональный менеджер сертификатов AVEST (AVEST Personal Certificate Manager)

### *КриптоПро CSP*

Для установки КриптоПро CSP зайдите на сайт КриптоПро в раздел Загрузки <http://www.cryptopro.ru/products/csp/downloads> (для скачивания пройдите простую регистрацию на сайте).

Скачайте и установите дистрибутивы в зависимости от вашей ОС:

- [КриптоПро CSP 3.6 R4](#) - для Windows XP, Vista, 7, 8
- [КриптоПро CSP 3.9](#) - для Windows 7, 8, 8.1, 10

Обращаем Ваше внимание, что после обновления Windows 8.0 до Windows 8.1 версия КриптоПро CSP 3.6 работать перестанет. В этом случае будет необходимо обновить КриптоПро CSP до версии 3.9 и приобрести новую лицензию у представителей КриптоПро. Лицензия для КриптоПро CSP версии 3.6 не подходит для версии 3.9.

## *Lissi-CSP*

Скачайте и установите дистрибутивы в зависимости от вашей ОС:

<http://download.rus-telecom.ru/lissi-csp/1.13.0.15/LISSI-CSP-Setup-win32-1.13.0.15.exe> - для 32-х ОС

<http://download.rus-telecom.ru/lissi-csp/1.13.0.15/LISSI-CSP-Setup-x64-1.13.0.15.exe> - для 64-х ОС

Перезагрузите компьютер после установки СКЗИ.

### **2.3. Установка Фельдгегерь 3.0 и компонентов**

Скачайте дистрибутивы программ по следующим ссылкам:

Дистрибутив Фельдгегерь 3.0 - <https://download.rus-telecom.ru/sps.client3/SPS.Client3.Full.zip>

Документация Фельдгегерь 3.0 - <http://download.g-tel.ru/SPS.Client3/SPS.Client3.Doc.zip>

Распакуйте в выбранную папку архив SPS.Client3.Full.zip. Запустите файл SPS.Client3.exe и следуйте инструкциям Мастера установки. С подробной инструкцией по установке программы Фельдгегерь 3.0 можно ознакомиться в документации.

Если резервную копию базы данных восстанавливать не требуется, перейдите к пункту **4. Настройка Фельдгегерь 3.0.**

## **3. Восстановление данных из резервной копии БД**

Запустите Фельдгегерь 3.0, откройте меню *Сервис – Восстановление из резервной копии БД*. Укажите файл резервной копии, создававшейся ранее, нажмите *Открыть*. Дождитесь окончания процедуры восстановления данных из резервной копии.

Подключите ключевые носители к компьютеру и перейдите к пункту **4.2. Установка сертификатов с ключевых носителей.**

## **4. Настройка Фельдгегерь 3.0**

После установки Фельдгегерь 3.0 необходимо настроить подключения.

### **4.1. Настройка подключений.**

Подключите ключевые носители к компьютеру.

#### Настройка подключения ФНС

Откройте меню *Файл – Новое подключение – Подключение к серверу ФНС*. Откроется окно *Новое подключение*. Внизу нажмите ссылку *«Импортировать параметры учетной записи с сервера»*. Выберите сертификат вашей организации из списка. Если сертификат отсутствует, нажмите кнопку *«Установить с ключевого носителя»*. Параметры

подключения автоматически загрузятся с сервера. Проверьте настройки и нажмите ОК. Подключение ФНС появится в списке подключений слева.

#### Настройка подключения ПФР

Для настройки подключения ПФР выберите пункт меню **Файл – Новое подключение – Подключение к серверу ПФР**. В остальном настройка идентична настройке подключения ФНС.

#### Настройка подключения Росстат

Для настройки подключения Росстат выберите пункт меню **Файл – Новое подключение – Подключение к серверу Росстата**. В остальном настройка идентична настройке подключения ФНС и ПФР.

#### Настройка подключения ФСС

Для настройки подключения ФСС выберите пункт меню **Файл – Новое подключение – Подключение к серверу ФСС**. Выберите сертификат руководителя в соответствующем поле. Нажмите ОК, после обращения к серверу новое подключение появится в списке подключений.

#### Настройка подключения ЭДО

Для настройки подключения ЭДО выберите пункт меню **Файл – Новое подключение – Подключение к серверу ЭДО**. В остальном настройка идентична настройке подключения ФНС и ПФР.

### **4.2. Установка сертификатов с ключевых носителей.**


#### Установка сертификата через КриптоПро CSP:

Откройте меню **Пуск – Программы – КриптоПро - КриптоПро CSP**. Перейдите во вкладку **Сервис – Просмотреть сертификаты в контейнере – Обзор**. Выберите контейнер, нажмите **ОК**, нажмите **Далее**. Отобразятся сведения о сертификате. Нажмите **Установить**. Дождитесь сообщения об успешной установке сертификата в хранилище Личные.

#### Установка сертификата через LISSI-CSP:

Пока ключевой носитель вставлен в ПК, средства системы видят сертификат на ключевом носителе без дополнительных действий по импорту сертификата в систему.

#### Установка сертификата через Фельдгегерь 3.0:

Зайдите в параметры подключения через меню **Файл – Параметры подключения**. Найдите поле **Сертификат руководителя**. Нажмите рядом с этим полем кнопку . В открывшемся окне Сертификаты нажмите кнопку **Установить с ключевого носителя...** Выберите необходимый для установки сертификат, найденный на подключенных к компьютеру ключевых носителях, нажмите **Установить**. Нажмите **ОК**. В случае необходимости повторите описанные операции для сертификата бухгалтера.