Руководство пользователя кабинета ОНМСЗ от 11.10.2018
Выдержки

2.1 ТРЕБОВАНИЯ К АРМ ПОЛЬЗОВАТЕЛЯ

Для обеспечения информационного взаимодействия поставщиков информации с ЕГИССО, АРМ пользователя кабинета организации назначающей МСЗ должен удовлетворять следующим требованиям:

1. Операционная система — Windows 7 (32/64-разрядная), WindowsServer 2008 (32/64-разрядная), WindowsServer 2008 R2 (64-разрядная), Windows 8 (32/64-разрядная), Windows 8.1 (32/64-разрядная), WindowsServer 2012 (64-разрядная), WindowsServer 2012 R2 (64-разрядная);

2. Веб-браузер — InternetExplorer 10 или более поздней версии;

3. УстановленныйкриптопровайдерViPNet CSP 4.2 или КриптоПро CSP 4.0 (для криптопровайдера должна быть включена поддержка MicrosoftCryptoAPI), одновременная установка двух криптопровайдеров недопустима. Критерием выбора критопровайдера должен являться тип ПАК УЦ издателя квалифицированного сертификата электронной подписи, используемого пользователем. Описание выбора используемого криптопровайдера приведено в разделе 2.2.4 настоящего документа;

4. Установленный модуль криптографической защиты информации для рабочего места пользователя ППО УЭПШ Crypto+ DE;

5. Для операционной системы и веб-браузера должны быть установлены самые последние пакеты обновлений;

6. Пользователь должен обладать квалифицированным сертификатом электронной подписи.

2.2 ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО ПОДКЛЮЧЕНИЯ К КАБИНЕТУ ОРГАНИЗАЦИИ, НАЗНАЧАЮЩЕЙ МСЗ

Подключение к внутренним порталам ЕГИССО осуществляется по Интернет-соединению, защищенному протоколом TLS с прохождением односторонней аутентификации. В результате канал подключения к внутренним порталам будет защищен от перехвата и подмены информации с использованием удовлетворяющих нормативным требованиям криптографических алгоритмов, обеспечивающих конфиденциальность передаваемой информации.

Для организации защищенного подключения к кабинету организации, назначающей МСЗ, пользователю необходимо:

1. Установить на АРМ криптопровайдерViPNet CSP 4.2, или КриптоПро CSP 4.0 R2 (сертифицированная версия) и корневой сертификат кабинета организации назначающей МСЗ. ViPNet CSP 4.2 является бесплатным и рекомендованным к использованию в ЕГИССО криптопровайдером, инструкция по его установке и настройке приведена в разделе 2.2.1 настоящего документа. Установка и настройка КриптоПро CSP 4.0 R2 осуществляется в соответствии с поставляемой с ним эксплуатационной документацией, рекомендации по настройке КриптоПро

CSP 4.0 R2 для взаимодействия с кабинетом организации назначающей МСЗ приведены в разделе 2.2.3 настоящего документа;

2. Произвести настройку интернет подключения и браузера для взаимодействия с кабинетом организации назначающей МСЗ. Требования и рекомендации по настройке интернет подключения и браузера для взаимодействия с кабинетом организации назначающей МСЗ приведены в разделе 2.2.2 настоящего документа;

3. Произвести установку и настройку модуля криптографической защиты информации для рабочего места пользователя ППО УЭПШ Crypto+ DE. Установка и настройка ППО УЭПШ Crypto+ DE осуществляется в соответствии с положениями следующих документов, доступных на официальном сайте ПФР в разделе ЕГИССО (http://www.pfrf.ru/knopki/egisso/project/~4022):

- Программное обеспечение управления электронной подписью и шифрованием. Модуль криптографической защиты информации для рабочего места пользователя. Crypto+ DE (DesktopEdition). Руководство пользователя;

- Методические рекомендации по работе с ППО УЭПШ Crypto+ DE в ЕГИССО.

После выполнения соответствующих настроек АРМ пользователя кабинета ОНМСЗ, поставщику информации, осуществляющему взаимодействие с ЕГИССО через кабинет поставщика информации, остается добавить учетную запись уполномоченного представителя в группу доступа «Уполномоченный сотрудник ОНМСЗ» в ЕСИА.