ТРЕБОВАНИЯ
по подключению территориально удаленных автоматизированных рабочих мест пользователей и локальных сетей организаций участников ОМС к Информационной системе «ТФОМС Самарской области» (центрам обработки конфиденциальных данных) ТФОМС Самарской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Требования по подключению территориально удаленных автоматизированных рабочих мест пользователей и локальных сетей организаций участников ОМС к Информационной системе «ТФОМС Самарской области» (центрам обработки конфиденциальных данных) ТФОМС Самарской области (далее - Требования) регламентируют порядок подключения отдельных АРМ и локальных сетей к системам, предназначенным для обработки информации, содержащей сведения конфиденциального характера в Информационной системе «ТФОМС Самарской области».

1.2. Информационная система «ТФОМС Самарской области» включает Специальные автоматизированные рабочие места (АРМ), которые обеспечивают автоматизацию процессов сбора, проверки, хранения конфиденциальных данных, формирования регламентных документов, обработки полученной информации с помощью аналитических инструментов ТФОМС Самарской области.

1.3. Требования являются дополнением к действующим нормативным документам по вопросам защиты информации и не исключают обязательного выполнения их требований.

1.4. Настоящие Требования публикуются на официальном интернет сайте ТФОМС Самарской области и обязательны к применению организациями при подключении к Информационной системе «ТФОМС Самарской области».

2. ОСНОВНЫЕ ТРЕБОВАНИЯ

2.1. В целях соблюдения принципа персональной ответственности каждый удаленный пользователь проходит двустороннюю аутентификацию с сервером доступа ТФОМС Самарской области.

Примечание:

Подключение анонимных удаленных пользователей к Специальным АРМ ТФОМС Самарской области запрещено.

2.2. Для организации подключения пользователей к ресурсам защищаемой сети (VPN) используется ViPNet Custom сеть № 654, а также дополнительное программное обеспечение - средство криптографической защиты информации (далее - Абонентский пункт или АП) ViPNet Client v.4.x.

2.3. Для организации подключения удаленных пользователей и локальных сетей, защищенных криптографическими шлюзами (КШ), к ресурсам Информационной системы «ТФОМС Самарской области» используется Центр управления сетью и комплекс криптографических шлюзов ТФОМС Самарской области (ЦУС).

2.4. Администратор безопасности осуществляет администрирование сети криптошлюзов (КШ) и входящих в состав комплекса средств криптографической защиты информации (СКЗИ) в рамках управления ЦУС.

2.5. Администратор безопасности проверяет неизменность настроек сети КШ объекта информатизации и технологического процесса передачи информации в части обеспечения безопасности информации.

2.6. Неизменность настроек сети КШ и технологического процесса передачи информации в части обеспечения безопасности информации контролируется не реже одного раза в год, а также при изменении программной среды и персонала; при необходимости привлекаются на договорной основе организации, проводившие оценку соответствия (аттестационные испытания).

3. ПОДКЛЮЧЕНИЕ ЛОКАЛЬНЫХ СЕТЕЙ И АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ К СПЕЦИАЛЬНЫМ АРМ

3.1. Инициатор (сторонняя организация или входящая в состав системы ОМС) для подключения АРМ или ЛВС к Специальным АРМ Информационной системы «ТФОМС Самарской области» должен:

- при отсутствии соглашения о конфиденциальности с ТФОМС Самарской области заключить его (см. Регламент УЦ ТФОМС Самарской области);
- обеспечить защиту подключаемого объекта информатизации (АРМ или ЛВС) в соответствии с требованиями действующего законодательства РФ;
- обеспечить организацию защищенного VPN-канала с использованием КШ или СКЗИ ViPNet Client v.4.x в зависимости от выбранной схемы подключения;
- провести оценку соответствия (аттестовать) подключаемый информационный ресурс (объект информатизации) по уровню защищенности персональных данных – 2 в соответствии с требованиями руководящих документов ФСТЭК России.

3.2. После выполнения указанных мероприятий необходимо зарегистрировать АП или КШ, представив в ОИТ ТФОМС Самарской области[1]:

- копию соглашения о конфиденциальности, заключенного данной организацией с ТФОМС Самарской области;
- копию заключения по результатам оценки соответствия подключаемой АРМ на соответствие требованиям безопасности информации ФСТЭК России, ФСБ России, РКН;
- заявление на изготовление сертификата ключа пользователя АП (см. Регламент УЦ ТФОМС Самарской области), подписанное руководителем

[1] Требуется предварительное согласование данной процедуры со специалистом ОИТ по телефону: +7 (846) 339-15-02

предприятия зарегистрированного работника (только для абонентского пункта);

- заявление на подключение криптографического шлюза (см. Регламент УЦ ТФОМС Самарской области), подписанное начальником структурного подразделения организации, ответственным за эксплуатацию подключаемого КШ (только для криптошлюза);
- защищенное средство хранения ключевой информации (usb-носитель) для записи закрытого ключа сертификата пользователя (только для абонентского пункта);
- файлы конфигурации (только для организации связи с КШ, управляемым другим ЦУС).

3.3. Оригиналы заявлений и копии заключения по результатам оценки соответствия хранятся у администратора безопасности в ОИТ ТФОМС Самарской области.

3.4. Администратор безопасности изготавливает закрытый ключ и сертификат открытого ключа (стандарт x509v3) подключаемого пользователя, заполняет журнал поэкземплярного учета СКЗИ и передает закрытый ключ и сертификат пользователю.

3.5. Пользователь устанавливает полученный сертификат на АРМ, руководствуясь технической документацией на СКЗИ.

3.6. За 1 месяц до истечения срока действия сертификата открытого ключа Абонентского пункта пользователь должен инициировать процесс переиздания ключа и сертификата, для чего направить в ОИТ ТФОМС Самарской областизаявление на изготовление сертификата ключа пользователя Абонентского пункта и usb-носитель для записи ключевой информации.

4. ПРАВА И ОБЯЗАННОСТИ УДАЛЕННОГО ПОЛЬЗОВАТЕЛЯ СПЕЦИАЛЬНОЙ АРМ КОРПОРАЦИИ

4.1. Передача ключевых носителей разрешена лично пользователю или его доверенному лицу.

4.2. Пользователь после получения закрытого ключа и сертификата обязан сменить стандартный пароль.

4.3. Владельцы ключей доступа должны быть предупреждены об ответственности за разглашение парольной информации.

4.4. Удаленный пользователь не имеет права сообщать кому-либо личный пароль и закрытый ключ (ключи) электронной подписи (ЭП), а также заносить его на носители, доступные другим пользователям объекта информатизации или работникам.