Распоряжение Министерства здравоохранения Удмуртской Республики от 26 ноября 2020 г. N 1424 "О ведомственной защищенной сети передачи данных Министерства здравоохранения Удмуртской Республики"

В соответствии с Федеральными законами от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 27 июля 2006 года N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 05.05.2018 N 555 "О единой государственной информационной системе в сфере здравоохранения" в целях защиты информации, обрабатываемой в Региональном сегменте Единой государственной информационной системы в сфере здравоохранения Удмуртской Республики (Региональная медицинская информационная система):

1. Утвердить прилагаемое Положение о ведомственной защищенной сети передачи данных Министерства здравоохранения Удмуртской Республики.

2. Определить Министерство здравоохранения Удмуртской Республики владельцем ведомственной защищенной сети передачи данных.

3. Определить бюджетное учреждение здравоохранения Удмуртской Республики "Республиканский медицинский информационно-аналитический центр Министерства здравоохранения Удмурткой Республики" (далее - БУЗ УР "РМИАЦ МЗ УР") оператором ведомственной защищенной сети передачи данных Министерства здравоохранения Удмуртской Республики.

4. Директору БУЗ УР "РМИАЦ МЗ УР" организовать разработку проектов документов и актов, регулирующих условия подключения к ведомственной защищенной сети передачи данных Министерства здравоохранения Удмуртской Республики, в течение одного месяца с даты подписания настоящего распоряжения.

5. Руководителям организаций, подведомственных Министерству здравоохранения Удмуртской Республики, обеспечить соблюдение требований и условий подключения к ведомственной защищенной сети передачи данных Министерства здравоохранения Удмуртской Республики.

6. Руководителям организаций частной системы здравоохранения рекомендовать обеспечить соблюдение требований и условий подключения к ведомственной защищенной сети передачи данных Министерства здравоохранения Удмуртской Республики.

7. Разместить настоящее распоряжение на официальном сайте Министерства здравоохранения Удмуртской Республики.

8. Контроль за исполнением настоящего распоряжения оставляю за собой.

Министр Г.О. Щербак

Положение
о ведомственной защищенной сети передачи данных Министерства здравоохранения Удмуртской Республики
(утв. распоряжением МЗ УР от 26 ноября 2020 г. N 1424)

1. Общие положения

1.1. Настоящее Положение определяет цели и задачи создания ведомственной защищенной сети передачи данных Министерства здравоохранения Удмуртской Республики (далее - ЗСПД), требования, предъявляемые к работе ЗСПД, полномочия оператора и администратора ЗСПД, права участника ЗСПД, условия подключения к ЗСПД.

1.2. Для целей настоящего Положения используются следующие понятия:

1) ЗСПД - виртуальная, наложенная на физические каналы связи защищенная транспортная сеть, построенная с использованием технологий межсетевого экранирования и VPN и использующая для криптографической защиты информации алгоритмы ГОСТ 34.12-2018 и ГОСТ 34.13-2018, реализованная на сертифицированных в установленном порядке средствах защиты информации;

2) оператор ЗСПД - государственное учреждение Удмуртской Республики, осуществляющее от имени Министерства здравоохранения Удмуртской Республики управление ЗСПД;

3) участник ЗСПД - государственный орган исполнительной власти Удмуртской Республики, федеральное/региональное государственное учреждение или частная организация, расположенные на территории Удмуртской Республики, осуществляющие деятельность в области здравоохранения или оказывающие медицинские услуги, подписавшие с оператором ЗСПД двустороннее соглашение о подключении к ЗСПД и подключенные в установленном порядке к ЗСПД;

4) компоненты ЗСПД - подключаемые с применением оборудования к ЗСПД автоматизированные рабочие места пользователей, серверы баз данных, ЗСПД участников, иные объекты, подключение которых необходимо и/или целесообразно для функционирования ЗСПД;

4) автоматизированное рабочее место администратора (далее - АРМ администратора) - компьютер с установленным специальным программным обеспечением для администрирования ЗСПД, установленный в учреждении, осуществляющей администрирование ЗСПД;

5) оборудование - аппаратно-программный комплекс, выполняющий функции межсетевого экрана и криптомаршрутизатора, имеющий сертификат соответствия Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации, устанавливаемый у участника ЗСПД;

6) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку посредством информационных технологий и технических средств;

7) администратор ЗСПД - структурное подразделение или учреждение, осуществляющее администрирование ЗСПД с использованием АРМ администратора, имеющее следующие виды лицензии (Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности"):

- на осуществление деятельности по технической защите конфиденциальной информации, в соответствии постановлением Правительства Российской Федерации от 03.02.2012 N 79 "О лицензировании деятельности по технической защите конфиденциальной информации";

- на разработку, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, в соответствии с Постановление Правительства Российской Федерации от 16.04.2012 N 313;

8) администрирование ЗСПД - действия администратора ЗСПД, непосредственно направленные на конфигурирование и управление компонентами ЗСПД, в соответствии с законодательством Российской Федерации, в том числе нормативно-правовыми актами иных органов, настоящим Положением и эксплуатационной документацией на средства защиты информации;

9) техническое сопровождение ЗСПД - это комплекс сервисов и услуг, предоставляемых

администратором ЗСПД с целью содействия оператору ЗСПД и участникам ЗСПД в продуктивном и результативном использовании оборудования для эффективного функционирования ЗСПД, включающий обновление программного обеспечения, устранение ошибок на узлах ЗСПД, консультирование пользователей ЗСПД и т.д.;

10) информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами.

2. Цель и задачи создания ЗСПД

2.1. Основной целью создания ЗСПД является обеспечение безопасной передачи конфиденциальной информации между участниками ЗСПД, в том числе информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, с использованием публичных и выделенных каналов связи путем организации виртуальной сети.

2.2. Основными задачами создания защищенной сети являются:

1. обеспечение безопасного взаимодействия участников ЗСПД при работе в ведомственных информационных системах (далее - ИС);

2. обеспечение безопасной передачи через открытые каналы связи информации ограниченного доступа между участниками ЗСПД;

3. обеспечение безопасного межсетевого взаимодействия между защищаемыми компонентами ЗСПД участников ЗСПД и сетью Интернет.

3. Требования, предъявляемые к работе ЗСПД

3.1. ЗСПД состоит из АРМ администратора и оборудования, установленного в помещениях участников ЗСПД, принадлежащих им на правах владения, аренды, безвозмездного пользования или на иных условиях, обеспечивающих защиту от несанкционированного доступа к оборудованию третьих лиц, а также каналов передачи данных.

3.2. Участник ЗСПД должен обеспечить информационную безопасность каждого подключаемого компонента ЗСПД в соответствии с действующим законодательством Российской Федерации.

3.3. Оборудование, устанавливаемое у участников ЗСПД, должно находиться в пределах их контролируемой зоны.

3.4. Оборудование, установленное у участника защищенной сети, должно находиться в работоспособном состоянии, быть доступным для других участников ЗСПД при межсетевом, защищенном взаимодействии с использованием сети Интернет, за исключением времени проведения ремонтно-профилактических работ.

3.5. Администрирование и техническое сопровождение ЗСПД осуществляется оператором ЗСПД самостоятельно, либо с привлечением сторонних организаций. Привлекаемые для администрирования и технического сопровождения ЗСПД организации осуществляют данную деятельность в соответствии с действующим законодательством Российской Федерации, настоящим Положением и эксплуатационной документацией на используемое (применяемое) оборудование и программное обеспечение.

4. Полномочия оператора ЗСПД.

4.1. Оператор защищенной сети выполняет следующие функции:

1) заключает соглашения о подключении участника ЗСПД;

2) определяет полномочия и порядок работы администратора ЗСПД при работе с ЗСПД;

3) ведет реестр участников ЗСПД;

4) определяет технологию, предназначенную для построения ЗСПД путем использования системы межсетевых экранов на защищаемых элементах распределенной сети (рабочие станции, сервера, локальные сети) и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающую шифрование сетевого трафика между этими элементами, применяет и использует ее при функционировании ЗСПД;

5) с учетом требований действующего законодательства Российской Федерации определяет наименование применяемого в ЗСПД оборудования, а также его количество, характеристики и требования к нему, в том числе в области защиты информации;

6) разрабатывает и предоставляет участникам ЗСПД документы, регламентирующие порядок и условия подключения к ЗСПД, порядок работы участников ЗСПД в ЗСПД, проекты соглашений о подключении к ЗСПД.

4.2. Оператор защищенной сети имеет право:

1) Разрабатывать документацию по вопросам, касающимся эксплуатации и управления ЗСПД;

2) запрашивать и получать от участников ЗСПД необходимые материалы и сведения об использовании ими ЗСПД;

3) принимать решения об отключении от ЗСПД участников ЗСПД, нарушающих требования настоящего Положения или действующего законодательства Российской Федерации в сфере защиты информации, уведомив об этом администратора ЗСПД, не менее чем за 2 рабочих дня.

4.3. Администратор ЗСПД выполняет следующие функции:

1) Обеспечивает бесперебойный и безопасный доступ подключенных участников ЗСПД к расположенным в ней компонентам ЗСПД;

2) обеспечивает администрирование ЗСПД, наблюдение за работоспособностью ЗСПД и, по необходимости, принимает меры по восстановлению ее работоспособности;

3) управляет доступом участников защищенной сети к компонентам ЗСПД и сетевым сервисам ЗСПД;

4) настраивает маршруты, туннелируемых адресов, межсетевое экранирование;

5) настраивает связи между узлами ЗСПД;

6) обеспечивает защиту оборудования ЗСПД от несанкционированных действий внутренних и внешних пользователей, в рамках своих полномочий;

7) управляет техническими средствами ЗСПД;

8) предпринимает необходимые меры для развития и поддержания работоспособности ЗСПД;

9) проверяет наличие и тестирует каналы связи в информационно-телекоммуникационную сеть Интернет для обеспечения работоспособности узлов ЗСПД;

10) определяет по согласованию с оператором ЗСПД необходимые меры и технологии (в том числе криптографические) для обеспечения безопасной передачи данных по ЗСПД;

11) подключает по согласованию с оператором ЗСПД защищенную сеть к другим сетям для осуществления межсетевого взаимодействия;

12) приостанавливает по согласованию с оператором ЗСПД функционирование ЗСПД не более чем на 10 часов в месяц для проведения обслуживания оборудования, при обязательном уведомлении всех участников ЗСПД о планируемых работах, не позднее, чем за 1 рабочий день до их начала, а также уведомляет об окончании таких работ, путем направления официального письма по государственной информационной системе Удмуртской Республики "Система электронного документооборота государственных органов Удмуртской Республики", а также на официальные адреса электронной почты оператора ЗСПД и участников ЗСПД;

13) подключает к ЗСПД новых участников ЗСПД в соответствии с настоящим Положением;

14) инициативно обращается к оператору ЗСПД в случае выявления участников ЗСПД, нарушающих требования настоящего Положения или действующего законодательства Российской

Федерации в сфере защиты информации;

15) осуществляет техническое сопровождение ЗСПД;

16) осуществляет ремонтно-профилактические работы на оборудовании ЗСПД;

17) диагностирует оборудование, отвечающее за функционирование ЗСПД, и выдает рекомендации по его ремонту;

18) проводит консультации с оператором ЗСПД и участниками ЗСПД по вопросам настройки, реконфигурации и эксплуатации и модернизации узлов ЗСПД;

19) определяет по согласованию с оператором ЗСПД необходимый перечень программного и аппаратного обеспечения (в том числе специального) для обеспечения функционирования АРМ администратора.

5. Права участника ЗСПД

5.1. Участник защищенной сети имеет право:

1) получать доступ к ЗСПД в соответствии с условиями, утвержденными оператором ЗСПД;

2) получать справочную и иную информацию о работе и использованию ЗСПД;

3) получать от оператора защищенной сети документацию, регламентирующую порядок и условия подключения к ЗСПД, проекты соглашений о подключении к ЗСПД;

4) на техническое сопровождение ЗСПД.

5.2. Полномочия участника ЗСПД при работе с защищенной сетью определяются соглашением о подключении к ЗСПД.

6. Условия подключения к ЗСПД

6.1. Подключение осуществляется после заключения соглашения о подключении к ЗСПД между оператором ЗСПД и участником ЗСПД.

6.2. Подключение и взаимодействие с участниками ЗСПД, имеющими собственные ЗСПД, может быть осуществлено при условии заключения с оператором ЗСПД соглашения о конфиденциальности.