ДЕПАРТАМЕНТ ОХРАНЫ ЗДОРОВЬЯ НАСЕЛЕНИЯ КЕМЕРОВСКОЙ ОБЛАСТИ

ПРИКАЗ

«07» 04 2017 г. № 497

г. Кемерово

Об утверждении положения о защищенной сети передачи данных №753 системы здравоохранения Кемеровской области

В целях совершенствования единой государственной политики по регулированию информационного взаимодействия в сфере здравоохранения Кемеровской области, в соответствии с Федеральным законом от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», приказом Минздравсоцразвития России от 28 апреля 2011 года № 364 «Об утверждении Концепции создания единой государственной информационной системы в сфере здравоохранения», пунктом 32 Плана мероприятий («Дорожной карты») по развитию Единой государственной информационной системы в сфере здравоохранения в 2015-2018 годах, утвержденного Соглашением между Министерством здравоохранения Российской Федерации и Коллегией Администрации Кемеровской области «О взаимодействии в сфере развития ЕГИСЗ в 2015-2018 гг.» от 1 июля 2015 года

ПРИКАЗЫВАЮ:

1. Утвердить положение о защищенной сети передачи данных №753 системы здравоохранения Кемеровской области, согласно приложению к настоящему приказу.
2. Директору ГБУЗ КО «Кемеровский областной медицинский информационно-аналитический центр» Д.Е. Беглову осуществлять координацию и мониторинг мероприятий по развитию защищенной сети передачи данных №753 системы здравоохранения Кемеровской области.
3. Контроль за исполнением приказа возложить на первого заместителя начальника департамента охраны здоровья населения Кемеровской области А.В. Брежнева.

Начальник департамента В.М. Шан-Син

ДЛЯ ПРИКАЗОВ

КОПИЯ ВЕРНА

Приложение к приказу
департамента охраны здоровья населения
Кемеровской области
от _07.04.2017___ года № _497__

ПОЛОЖЕНИЕ
о защищенной сети передачи данных №753
системы здравоохранения Кемеровской области

1. Общие положения

1.1. Настоящее Положение определяет цели и задачи создания защищенной сети передачи данных №753 системы здравоохранения Кемеровской области (далее – защищенная сеть), требования, предъявляемые к работе защищенной сети, полномочия оператора защищенной сети, права участника защищенной сети и условия подключения к защищенной сети.

1.2. Нормативно-правовое и терминологическое обеспечение содержится в нижеследующих документах:

- Федеральный Закон от 26 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по

обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказ Департамента охраны здоровья населения Кемеровской области 30.11.2016 года № 1305 «Об утверждении положения о Региональном сегменте Единой государственной информационной системы в сфере здравоохранения Кемеровской области (РС ЕГИСЗ)»;
- План мероприятий («Дорожная карта») по развитию единой государственной информационной системы в сфере здравоохранения в Кемеровской области, утвержденный Соглашением между Министерством здравоохранения Российской Федерации и Коллегией Администрации Кемеровской области о взаимодействии в сфере развития Единой государственной информационной системы в сфере здравоохранения в 2015-2018 гг. от 1 июля 2015 г.

1.3. Для целей настоящего Положения используются следующие понятия:

- защищенная сеть – виртуальная, наложенная на физические каналы связи защищенная транспортная сеть, построенная с использованием технологий межсетевого экранирования и VPN, реализованная сертифицированными в установленном порядке средствами защиты информации, являющаяся частью информационно-коммуникационной инфраструктуры РС ЕГИСЗ;
- оператор защищенной сети – Государственное бюджетное учреждение здравоохранения Кемеровской области «Кемеровский областной медицинский информационно-аналитический центр» (ГБУЗ «КОМИАЦ»), осуществляющий от имени департамента охраны здоровья населения Кемеровской области управление защищенной сетью;
- участники защищенной сети – медицинские организации, аптечные и фармацевтические организации, подключенные в установленном порядке к защищенной сети;
- компоненты защищенной сети – подключаемые, с применением оборудования, к защищенной сети автоматизированные рабочие места пользователей, серверы баз данных, аппаратно-программные комплексы, подключение которых необходимо для целей функционирования защищенной сети;
- автоматизированное рабочее место администратора (далее – АРМ администратора) – компьютер с установленным специальным программным обеспечением для администрирования защищенной сети;
- 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 защищенной сети;

- информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- администратор защищенной сети – уполномоченные сотрудники оператора защищенной сети, осуществляющие администрирование защищенной сети, с использованием АРМ администратора;
- администрирование защищенной сети – действия администратора защищенной сети, непосредственно направленные на конфигурирование и управление компонентами защищенной сети, в соответствии с законодательством Российской Федерации, в том числе нормативно-правовыми актами иных органов, настоящим Положением и эксплуатационной документацией на средства защиты информации, с использованием АРМ администратора;
- техническое сопровождение защищенной сети – консультирование участников защищенной сети по вопросам работы оборудования;
- информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами.

2. Цель и задачи создания защищенной сети

2.1. Основной целью создания защищенной сети является обеспечение безопасной передачи информации между участниками защищенной сети, 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:

- обеспечение доступа к информационным ресурсам регионального сегмента единой государственной информационной системы здравоохранения Кемеровской области (далее – РС ЕГИСЗ);
- обеспечение защищенной передачи данных по открытым каналам связи между участниками защищенной сети;
- обеспечение межсетевого взаимодействия между защищаемыми компонентами защищенной сети участников защищенной сети и сетью Интернет.

3. Требования, предъявляемые к работе защищенной сети

3.1. Защищенная сеть состоит из АРМ администратора и оборудования, установленного в помещениях участников защищенной сети, 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 защищенной сети должен обеспечить информационную безопасность каждого подключаемого компонента защищенной сети в соответствии с законодательством Российской Федерации.

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

3.4. Защищенная сеть должна находиться в работоспособном режиме постоянно.

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

3.6. Администрирование и техническое сопровождение защищенной сети осуществляется оператором защищенной сети самостоятельно.

4. Полномочия оператора защищенной сети

4.1. Оператор защищенной сети выполняет следующие функции:

- обеспечивает бесперебойный и безопасный доступ подключенных участников защищенной сети к расположенным в ней компонентам защищенной сети;
- обеспечивает администрирование защищенной сети, наблюдение за работоспособностью защищенной сети и по необходимости принимает меры по восстановлению её работоспособности;
- управляет доступом участников защищенной сети к компонентам защищенной сети и сетевым сервисам защищенной сети;
- обеспечивает защиту оборудования защищенной сети от несанкционированных действий внутренних и внешних пользователей в рамках своих полномочий;
- предпринимает необходимые меры для развития и поддержания работоспособности защищенной сети;
- подключает к защищенной сети новых участников защищенной сети в соответствие с настоящим Положением;
- осуществляет техническое сопровождение защищенной сети;

- ведет реестр участников защищенной сети;
- определяет технологию, предназначенную для построения защищенной сети путем использования системы межсетевых экранов на защищаемых элементах распределенной сети (рабочие станции, серверы, локальные сети) и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающую шифрование сетевого трафика между этими элементами, применяет и использует её при функционировании защищенной сети;
- с учетом требований законодательства определяет наименование применяемого в защищенной сети оборудования, а также его количество, характеристики и требования к нему, в том числе в области защиты информации.

4.2. Оператор защищенной сети имеет право:

- разрабатывать документацию по вопросам, касающимся эксплуатации и управления защищенной сетью;
- запрашивать и получать от участников защищенной сети необходимые материалы и сведения об использовании ими защищенной сети;
- отключать, от защищенной сети участников защищенной сети, нарушающих требования настоящего Положения.

5. Права участника защищенной сети

5.1. Участник защищенной сети имеет право:

- получать доступ к защищенной сети в соответствии с условиями, определяемыми оператором защищенной сети;
- получать справочную и иную информацию о работе и использованию защищенной сети;
- получать от оператора защищенной сети документацию, регламентирующую порядок и условия подключения к защищенной сети.

5.2. Полномочия участника защищенной сети определяются договором с оператором защищенной сети.

6. Условия подключения к защищенной сети

6.1. Подключение к защищенной сети осуществляется на основании договора с оператором защищенной сети.