РЕСПУБЛИКА ИНГУШЕТИЯ ГІАЛГІАЙ МОХК

ГБУЗ «СУНЖЕНСКАЯ ЦЕНТРАЛЬНАЯ РАЙОННАЯ БОЛЬНИЦА»

П Р И К А З № 225 А

«24» 08 2015г. г.п. Сунжа

«О назначении ответственного за обеспечение безопасности защиты персональных данных»

Во исполнение постановления Правительства РФ от 21 марта 2012 года № 221 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральными законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановления Правительства РФ от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»

П Р И К А З Ы В А Ю:

Назначить ответственного за обеспечение безопасности защиты персональных данных ГБУЗ «Сунженская ЦРБ» программиста - Оздоева Исраила Микаиловича.

Главный врач Р.М. Сайнароева

ГБУЗ «Сунженская центральная районная больница»

УТВЕРЖДАЮ:
Главный врач ГБУЗ
«Сунженская ЦРБ»
_____Р.М. Сайнароева
«24» 05 2015 г.
м.п.

Должностная инструкция ответственного за обеспечение безопасности защиты персональных данных

1. Общие положения.

1.1. Настоящая инструкция разработана на основании постановления Правительства Российской Федерации от 21 марта 2012г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», «Положением об организации и проведении работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных и других нормативно-правовых актов регулирующих обработку персональных данных в автоматизированных системах.

1.2. Инструкция определяет функции, права и обязанности ответственного за обеспечение безопасности персональных данных ГБУЗ «Сунженская центральная районная больница» (далее — больница) по вопросам обеспечения информационной безопасности при обработке персональных данных.

1.3. Ответственный за обеспечение безопасности персональных данных назначается из числа сотрудников больницы и обеспечивает правильность использования и нормальное функционирование установленных средств защиты информации (далее – СЗИ).

1.4. К СЗИ относятся средства защиты от несанкционированного доступа (далее – НСД), средства межсетевого экранирования, а также антивирусные средства.

1.5. К выполнению обязанностей в области организации разграничения доступа, настройке локальной вычислительной сети ответственный за обеспечение безопасности персональных данных может привлекать к работам сторонних сотрудников. Все работы должны согласовываться с гл. врачом больницы и проводиться только в присутствии ответственного за обеспечение безопасности персональных данных при этом не должны затрагиваться средства защиты информации от несанкционированного доступа и обрабатываемые персональные данные.

2.2.6. Сопровождение подсистемы обеспечения целостности информации в ИСПДн:
— организация периодического тестирования функций установленной на РС СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;
— организация восстановления программной среды, программных средств и настроек СЗИ при сбоях;
— организация поддержания установленного порядка и правил антивирусной защиты информации на ПЭВМ;
— контроль за периодическим обновлением антивирусных средств (баз данных), установленных на РС, контроль соблюдения пользователями порядка и правил антивирусной защиты.

2.2.7. Контроль соблюдения требований по размещению и использованию ИСПДн, указанных в Техническом паспорте.

3. Права и обязанности администратора безопасности

3.1. Для реализации поставленных задач и возложенных функций, ответственный за обеспечение безопасности персональных данных ОБЯЗАН:

3.1.1. Сопровождать СЗИ от НСД и ОТСС:
— вести учет и знать перечень установленных в ИСПДн ОТСС, СЗИ от НСД и перечень задач, решаемых с их использованием.
— осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на РС специальных программных и программно-аппаратных СЗИ от НСД.
— присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных РС и серверов, осуществлять проверку работоспособности системы зашиты после установки (обновления) программных средств в ИСПДн.
— периодически проверять состояние используемых СЗИ от НСД, осуществлять проверку правильности их настройки (выборочное тестирование).
— контролировать соответствие технического паспорта объекта вычислительной техники (далее – СВТ) фактическому составу (комплектности) СВТ в ИСПДн и вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения в ИСПДн).
— вести учет нештатных ситуаций, выполнения профилактических работ, установки и модификации аппаратных и программных средств ИСПДн.
— проводить инструктаж (первичный, периодический, внеочередной) сотрудников больницы, допущенных к обработке персональных данных в ИСПДн по правилам работы с используемыми средствами и системами зашиты информации.

3.1.2. Организовывать разграничения доступа:
а) участвовать в разработке и знать перечень защищаемых информационных ресурсов ИСПДн.
б) разрабатывать совместно с администраторами ЛВС решения по:
— приписке пользователей с одинаковыми правами, статусом безопасности и характером решаемых задач к соответствующим группам;
— определению списка устройств, логических дисков, каталогов общего пользования на серверах, с указанием состава допущенных к ним пользователей и режимов допуска (матрица доступа);
— осуществлению контроля за наличием активных компьютеров сети, состоянием активных пользователей, использованием разделяемых

4.1.4. Осуществлять оперативное вмешательство в работу пользователя ИСПДн при явной угрозе безопасности персональным данным в результате несоблюдения установленной технологии обработки персональных данных и невыполнения требований по безопасности с последующим докладом ответственному за обеспечение безопасности персональных данных.

4.1.5. Производить анализ защищенности ИСПДн путем применения специального программного обеспечения, осуществления попыток взлома системы защиты ИСПДн. Такие работы должны проводиться в часы наименьшей информационной нагрузки с обязательным уведомлением гл. врача больницы.

4.1.6. Вносить свои предложения по совершенствованию мер защиты в ИСПДн.

4.2. Ответственный за обеспечение безопасности защиты персональных данных несет ответственность за:

4.2.1. Реализацию принятых в ИСПДн мероприятий по защите персональных данных;

4.2.2. Программно — технические средства защиты информации, технические средства вычислительной техники ИСПДн, закрепленные за ним, а также за качество проводимых им работ по обеспечению защиты персональных данных в соответствии с функциональными обязанностями.

4.2.3. За несоблюдение требований по защите персональных данных ответственный за обеспечение безопасности персональных данных несет ответственность в соответствии с законодательством Российской Федерации.

Согласовано:

Юрисконсульт: _____

С инструкцией ознакомлен: _____

_____