Государственное бюджетное учреждение здравоохранения
Тюменской области

«ОБЛАСТНАЯ БОЛЬНИЦА № 4»
(г. Ишим)

УТВЕРЖДАЮ
Главный врач ГБУЗ ТО «ОБ № 4» (г. Ишим)
_____ В.Л. Афанасьев

«01» августа 2019 г.

ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Лабораторная диагностика» ГБУЗ ТО «ОБ № 4» (г. Ишим)

1. Общие положения

1.1 Данные требования по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Лабораторная диагностика» ГБУЗ ТО «ОБ № 4» (г. Ишим) (далее – ИСПДн) разработаны на основании приказа 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», частной модели угроз безопасности ПДн при их обработке в ИСПДн.

1.2 Требования определяют совокупность организационных и технических мероприятий, необходимых для обеспечения заданного уровня безопасности персональных данных при их обработке в ИСПДн «Лабораторная диагностика» ГБУЗ ТО «ОБ № 4» (г. Ишим).

2. Организационные мероприятия по обеспечению безопасности персональных данных

2.1 Задаются требования по: охране помещений, допуску лиц, выбору технических средств, их расположению в помещениях. Кроме того, задаются дополнительные требования по обеспечению конфиденциальности, целостности и доступности персональных данных (далее – ПДн).

2.2 К числу мер, необходимых и достаточных для обеспечения выполнения обязанностей оператора могут относиться:

2.2.1 Назначение оператором ответственного за организацию обработки персональных данных;

2.2.2 Издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

2.2.3 Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

2.2.4 Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона от 27.07.2006 N 152-ФЗ (в ред. Федеральных законов от 25.11.2009 N 266-ФЗ, от 27.12.2009 N 363-ФЗ, от 28.06.2010 N 123-ФЗ, от 27.07.2010 N 204-ФЗ, от 27.07.2010 N 227-ФЗ, от 29.11.2010 N 313-ФЗ от 23.12.2010 N 359-ФЗ, от 04.06.2011 N 123-ФЗ, от 25.07.2011 N 261-ФЗ) «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом от 27.07.2006 N 152-ФЗ (в ред. Федеральных законов от 25.11.2009 N 266-ФЗ, от 27.12.2009 N 363-ФЗ, от 28.06.2010 N 123-ФЗ, от 27.07.2010 N 204-ФЗ, от 27.07.2010 N 227-ФЗ, от 29.11.2010 N 313-ФЗ от 23.12.2010 N 359-ФЗ, от 04.06.2011 N 123-ФЗ, от 25.07.2011 N 261-ФЗ) «О персональных данных»;

2.2.5 Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2.2.6 Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2.2.7 Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных.

2.2.8 Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.2.9 Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

2.2.10 Учет машинных носителей персональных данных.

2.2.11 Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.

2.2.12 Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.2.13 Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

2.2.14 Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

2.3 При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационной системе осуществляется:

- разработка для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;
- разработка на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;
- поэкземплярный учет используемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.

2.4 Описание принятых мер должно быть включено в уведомление, предусмотренное частью 1 статьи 22 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных».

2.5 Сведения предусмотренные пунктами 5, 7^1, 10 и 11 части 3 статьи 22 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» должны быть предоставлены в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор).

2.6 Обеспечение функционирования и безопасности информационной системы персональных данных возлагается на ответственного пользователя, имеющего необходимый уровень квалификации, назначаемого приказом оператора (далее – ответственный пользователь).

2.7 Ответственные пользователи должны иметь функциональные обязанности, разработанные в соответствии с настоящими Требованиями.

2.8 Лица, оформляемые на работу в качестве пользователей (ответственных пользователей), должны быть ознакомлены с настоящими Требованиями и другими документами, регламентирующими организацию и обеспечение безопасности персональных данных при их обработке в информационных системах, под расписку и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

2.9 В соответствии с требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и

установленным уровнем защищенности персональных данных, обрабатываемых в ИСПДн «Лабораторная диагностика» необходимо выполнение следующих требований:

- контроль за выполнением настоящих Требований организуется и проводится Коптяевым Игорем Александровичем, заместителем главного врача по медицинскому обслуживанию населения не реже 1 раза в 3 года;
- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение Главным врачом документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
- необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

2.10 При использовании в ИСПДн сертифицированных по требованиям безопасности информации средств защиты информации для обеспечения установленного уровня защищенности персональных данных применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты;
- средства защиты информации прошедшие проверку по 4 уровню контроля на отсутствие НДВ;
- межсетевые экраны не ниже 3 класса.

3. Мероприятия по обеспечению безопасности персональных данных от несанкционированного доступа при их обработке в информационной системе персональных данных

В состав мер по обеспечению безопасности ПДн, реализуемых в рамках СЗПДн с учетом актуальных угроз безопасности ПДн и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

В таблице 1 приведено содержание требуемых мер по обеспечению безопасности персональных данных:

Таблица 1. Содержание требуемых мер по обеспечению безопасности ПДн

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники
III. Ограничение программной среды (ОПС)	
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
IV. Защита машинных носителей персональных данных (ЗНИ)	
ЗНИ.1	Учет машинных носителей персональных данных
ЗНИ.2	Управление доступом к машинным носителям персональных данных
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.5	Мониторинг (просмотр, анализ) результатоврегистрации событий безопасности и реагирование на них
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VII. Обнаружение вторжений (СОВ)	
СОВ.1	Обнаружение вторжений
СОВ.2	Обновление базы решающих правил
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)	
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)
X. Обеспечение доступности персональных данных (ОДТ)	
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала
XII. Защита технических средств (ЗТС)	
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
XIV. Выявление инцидентов и реагирование на них (ИНЦ)	
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
ИНЦ.5	Принятие мер по устранению последствий инцидентов
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)	
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных