ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ
«ИВДЕЛЬСКАЯ ЦЕНТРАЛЬНАЯ РАЙОННАЯ БОЛЬНИЦА»
ПРИКАЗ

г. Ивдель **№ 476/2** **от 25.11.2015г.**

О работе с персональными данными пациентов
ГБУЗ СО «Ивдельская ЦРБ»

В соответствии с Положением об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119, постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

ПРИКАЗЫВАЮ:

1. Утвердить «Положение о работе с персональными данными пациентов государственного бюджетного учреждения здравоохранения Свердловской области «Ивдельская центральная районная больница» (прилагается);
2. Начальнику отдела кадров Некипеловой Г.Д. обеспечить ознакомление всех работников с настоящим приказом под роспись.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач ГБУЗ СО
«Ивдельская ЦРБ» ***С.А. Зигмантович***

УТВЕРЖДЕНО
Приказом главного врача
ГБУЗ СО «Ивдельская ЦРБ»
от 25.11.2015г. № 476/2

ПОЛОЖЕНИЕ
о работе с персональными данными пациентов государственного бюджетного учреждения здравоохранения Свердловской области «Ивдельская центральная районная больница»

1. Политика безопасности персональных данных

1.1. Введение

1.1.1. Общий обзор

1) Настоящее Положение о работе с персональными данными пациентов при их обработке в информационных системах персональных данных государственного бюджетного учреждения здравоохранения Свердловской области «Ивдельская центральная районная больница» (далее Положение) разработано в соответствии с ч. 1 ст. 23, ст. 24 Конституции Российской Федерации, Федеральным законом Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» и определяет порядок организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее ИСПДн) в государственном бюджетном учреждении здравоохранения Свердловской области «Ивдельская центральная районная больница» (далее Учреждение).
2) Перечень сотрудников, допущенных к работе с персональными данными в ИСПДн, определяется приказом главного врача ГБУЗ СО «Ивдельская центральная районная больница» (далее Руководитель).
3) Ответственность за обеспечение безопасности персональных данных и надлежащего режима работы ИСПДн возлагается на штатного сотрудника Учреждения приказом Руководителя.
4) Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

1.1.2. Область применения и цель положения

Положение распространяется на Субъектов персональных данных, являющихся лицами, обратившимися за медицинской помощью в ГБУЗ СО «Ивдельская центральная районная больница»;

Область применения положения:

а) помещения обработки и хранения персональных данных, принадлежащие организации;
б) аппаратные и программные средства, обеспечивающие обработку и хранение персональных данных;
в) хранилища носителей информации, содержащей персональные данные.

Цель данного положения:

1) определение основных принципов построения системы защиты персональных данных Учреждения;
2) определение основных мер защиты и областей ее внедрения для обеспечения выполнения Федерального законодательства, требования и рекомендаций национальных и международных стандартов в области информационной безопасности персональных данных.

1.1.3.Основные понятия и определения

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Инцидент информационной безопасности – событие, в результате наступления которого произошло разглашение конфиденциальной информации, нарушение работоспособности ИСПДн, внесение несанкционированных изменений, утечка или разглашение персональных данных клиентов и прочих событий, ведущих к нарушению прав и свобод граждан РФ.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

1.1.4.Понятие и состав персональных данных

1) В соответствии с пунктом 1 статьи 3 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» под персональными данными субъекта (далее Персональные данные) понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
2) Документами, содержащими персональные данные, являются:
   а) паспорт или иной документ, удостоверяющий личность;
   б) полис ОМС;
   в) история болезни;
   г) амбулаторная карта пациента;
   д) медицинские заключения о состоянии здоровья.
   е) другие документы, содержащие сведения, необходимые для оказания медицинских услуг.

1.1.5.Методы и способы защиты персональных данных

1) Методы и способы защиты персональных данных определяются в соответствии с постановлением Правительства Российской Федерации № 1119 от 01 ноября 2012 г., Приказом ФСТЭК России № 21 от 18 февраля 2013 г., Приказ ФСБ России № 378 от 10 июля 2014 г.
2) Системы защиты персональных данных должны соответствовать требованиям нормативных и руководящих документов ФСТЭК России, ФСБ России.
3) Под защитой персональных данных субъекта понимается комплекс мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.
4) Защита персональных данных субъекта осуществляется за счёт Учреждения в порядке, установленном федеральным законом.

5) Учреждение при защите персональных данных субъектов принимает все необходимые организационно-распорядительные, юридические и технические меры, в том числе:
   а) шифровальные (криптографические) средства;
   б) антивирусная защита;
   в) анализ защищённости;
   г) обнаружение и предотвращение вторжений;
   д) управления доступом;
   е) регистрация и учет;
   ж) обеспечение целостности.
6) Разработка нормативно-методических локальных актов, регулирующих защиту персональных данных.

1.2. Цели и принципы обеспечения безопасности

1.2.1. Цели обеспечения безопасности

Целью обеспечения безопасности являются:
1) организация непрерывного и защищенного процесса обработки, хранения, передачи информации, содержащей персональные данные;
2) защита прав и свобод граждан РФ, предоставляющих Учреждению свои персональные данные для обработки и хранения.

1.2.2. Принципы обеспечения безопасности

Информационная безопасность персональных данных:
а) основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов;
б) обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер (программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики информационной системы);
в) должна обеспечиваться на всех этапах обработки информации и во всех режимах функционирования;
г) должна предусматривать контроль эффективности средств защиты.

Информационная безопасность персональных данных должна основываться на следующих принципах:
1) Принцип системности - системный подход к защите компьютерных систем предполагает необходимость взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов при всех видах информационной деятельности и информационного проявления. При обеспечении информационной безопасности информационных систем необходимо учитывать все слабые и наиболее уязвимые места системы, а также характер, возможные объекты и направления атак на систему со стороны нарушителя, пути проникновения распределенной системы и НСД к информации;
2) Принцип комплексности - для обеспечения защиты имеется широкий спектр мер, методов и средств защиты компьютерных систем. Комплексное их использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающие все существующие каналы угроз и не содержащие слабых мест на стыках отдельных её компонентов;
3) Принцип непрерывности защиты – защита информации - это не разовое мероприятие и не конкретная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный направленный процесс предполагающий принятие соответствующих мер на всех этапах существования информационной системы. Разработка системы защиты должна вестись параллельно обработке самой защищаемой системы;
4) Разумная достаточность - важно правильно выбрать тот уровень защиты при котором затраты, риск и размер возможного ущерба были бы приемлемы и не создавали неудобств пользователю;
5) Гибкость системы защиты - часто приходится создавать систему защиты в условиях большой неопределенности, поэтому принятые меры и средства защиты особенно в начальный период их эксплуатации могут оказывать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения уровня варьирования защищенности средство защиты должно обладать

определенной гибкостью, особенно если средство необходимо установить на работающую систему не нарушая процесса её нормального функционирования;

6) Принцип простоты применения средств защиты - механизмы защиты должны быть интуитивно понятны и просты в применении. Применение средств защиты не должно быть связано со знанием каких либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.

1.3. Организация безопасности

1.3.1. Ответственность

За вопросы безопасности в Учреждении несут ответственность:

1) Руководитель Учреждения.
2) Лица, назначенные Руководителем из состава сотрудников, ответственные за организацию работ по защите персональных данных.
3) Лица, назначенные Руководителем из состава сотрудников, и допущенные к средствам обработки информации и хранилищам, содержащим персональные данные.
4) Непосредственно Субъект персональных данных отвечает за корректность своих данных, за соблюдение установленного порядка и мер по обеспечению безопасности ПДн и самолично отвечает за разглашение информации конфиденциального характера, ставшей известной ему.

Каждый из обозначенных людей (кроме Субъекта) несет ответственность за неразглашение и корректность обработки ПДн в соответствии с Кодексом об административных правонарушениях на территории Российской Федерации и Уголовным Кодексам Российской Федерации.

1.3.2. Направления политики обеспечения безопасности

Основными направлениями политики информационной безопасности являются:

1) Соблюдение прав и свобод граждан РФ;
2) Соблюдение юридических норм РФ;
3) Обеспечение безопасности (конфиденциальности) данных;
4) Обеспечение непрерывного и корректного процесса обработки персональных данных, сохранение их целостности, корректности и доступности.

1.3.3. Регистрация инцидентов безопасности

Любые инциденты безопасности, в которые входят:

1) факты попыток и успешной реализации несанкционированного доступа в системы обработки информации, в помещения обработки информации и к хранилищам информации;
2) факты сбоя или некорректной работы систем обработки информации;
3) факты сбоя или некорректной работы средств защиты информации;
4) факты разглашения информации, содержащей ПДн;
5) факты разглашения информации о методах и способах защиты и обработки информации, содержащей ПДн,

должны сообщаться сотрудниками Учреждения ответственному за обеспечение безопасности. По каждому сообщению ответственный должен регистрировать инцидент, который в дальнейшем должен проходить процедуру расследования Комиссией, назначенной Руководителем Учреждения.

1.3.4. Безопасность средств обработки

Безопасность средств обработки обеспечивается организационными и техническими средствами. Организационно осуществляется допуск сотрудников и третьих лиц (если того требует бизнес-процесс), при этом минимизируется круг лиц, имеющих доступ. Права доступа к информации назначаются исходя из их необходимости и достаточности.

Технически безопасность обеспечивается корректной настройкой средств обработки информации и установкой наложенных средств защиты информации. Все средства защиты информации должны пройти обязательную процедуру оценки соответствия требованиям безопасности ФСТЭК России и ФСБ России.

1.3.5. Безопасность связи

Каналы передачи данных должны обеспечивать безопасное соединение узлов сети Учреждения. Безопасность может обеспечиваться следующими мерами:

1) Сегментация сети на зоны обработки ПДн и демилитаризированные зоны посредством физического разделения или с помощью VLAN технологий;
2) Максимальное ограничение доступа и набора протоколов и портов зоны обработки ПДн к сетям общего пользования и сетям международного обмена посредством средств межсетевого экранирования;
3) Обеспечение сетей обработки ПДн, имеющих подключение к сетям общего пользования и сетям международного обмена, средствами обнаружения и предотвращения вторжений;
4) Систематический контроль состояния системы защиты средствами активного аудита;
5) При прохождении каналов связи вне контролируемой зоны необходимо обеспечивать шифрование передаваемой информации на таких участках.

1.3.6. Физическая безопасность

Физическая безопасность можно обеспечивать следующими средствами, исходя из достаточности и необходимости того или иного средства:

1) Организация разрешительной системы доступа в помещения хранения и обработки ПДн.
2) Использование систем контроля и управления доступом (СКУД).
3) Учет ключей, электронных ключей доступа (proximity card, touch memory).
4) Использование физической охраны.
5) Использование видеонаблюдения.
6) Конструктивное усиление окон, дверей, стен и иных преград для несанкционированного доступа.

1.4. Квалификация персонала

Сотрудники, участвующие в обработке ПДн, должны иметь соответствующее образование и квалификацию, позволяющие им корректно работать со средствами обработки информации. Не разрешается допуск лиц, не прошедших собеседование с руководителем подразделения на предмет проверки знаний по работе с средствами обработки, осуществляющего обработку ПДн.

1.5. Безопасность документов и носителей информации

Материальные носители информации должны храниться в сейфах или запираемых шкафах.

Все электронные носители информации должны быть промаркированы (возможно использование заводской маркировки) и перечислены в журнале учета. Выдача и сдача электронных носителей осуществляется под роспись пользователя носителя.

Виды бумажных носителей должны быть определены шаблонами.

Организация работ по защите персональных данных

1.6. Создание комиссии по организации работ по защите персональных данных

1.6.1. Создание комиссии

Для организации работ по защите информации создается комиссия в составе:

а) председатель комиссии из состава руководства организации;
б) члены комиссии.

Состав лиц комиссии и ее создание оформляется «Приказом о создании комиссии для организации работ по защите персональных данных».

В состав комиссии должны входить следующие сотрудники:

а) ответственный за организацию работ по защите ПДн;
б) ответственный за обеспечение безопасности ПДн;
в) ответственный за обеспечение работы систем обработки ПДн.

1.6.2. Функциональные обязанности Комиссии

На членов Комиссии возлагаются следующие обязанности:

а) определения уровня защищенности (классификация) ИСПДн;
б) визирование организационно-распорядительных документов Учреждения в области защиты персональных данных;
в) согласование проектных документов ИСПДн и СЗПДн;
г) контроль состава, функций, состояний ИСПДн и СЗПДн;

д) визирование актов изменения состава, функций, состояний ИСПДн и СЗПДн.

1.7. Сотрудники, ответственные за обработку и обеспечение защиты персональных данных

1.7.1. Состав и порядок назначения лиц, ответственных за организацию и обеспечение защиты ПДн

Лица, ответственные за организацию и обеспечение защиты ПДн назначаются из состава сотрудников Учреждения. Они могут быть выделены либо как штатные единицы, либо выполнять функции (см. п. 2.2.2-2.2.4), назначенные приказами (или иному внутреннему нормативному акту) Руководителя:

а) Приказ о назначении ответственного за организацию и обеспечение защиты ПДн;
б) Приказ о назначении ответственного за обеспечение безопасности ПДн;
в) Приказ о назначении ответственного за технические средства обработки ПДн.

В должностной инструкции указанных лиц должны присутствовать обязательства по неразглашению информации, прямо и косвенно касающейся персональных данных:

1) ПДн гражданина РФ;
2) сведения о средствах обработки и защиты ПДн;
3) сведения об организации и обеспечению защиты ПДн.

1.7.2. Функциональные обязанности ответственного за организацию защиты ПДн

Ответственный должен выполнять следующий минимальный перечень функций:

1) руководит выполнением работ по технической защите информации в организации;
2) организует проведение классификации информационных ИСПДн, выявление угроз безопасности информации и технических каналов утечки информации, аттестации ИСПДн, применению сертифицированных средств защиты информации;
3) организует разработку организационно-распорядительных документов в области защиты информации;
4) разрабатывает предложения для включения в планы и программы работ по защите информации;
5) участвует в работах по внедрению новых средств защиты информации;
6) содействует распространению в организации передового опыта и внедрению современных организационно-технических мер, средств и способов защиты информации;
7) организует мероприятия по предотвращению утечки информации ограниченного доступа должностными лицами организаций, выполняющих работы, связанные со сведениями, составляющими государственную тайну и (или) содержащими иную информацию ограниченного доступа, при использовании открытых каналов связи;
8) осуществляет контроль выполнения требований нормативных правовых актов и иных документов по защите информации;
9) организует работы по определению потребности в средствах защиты информации, их заказу, получению и распределению;
10) участвует в подборе и расстановке специалистов;
11) организует работу по аттестации, обучению, профессиональной переподготовке и повышению квалификации специалистов в области защиты информации.

1.7.3. Функциональные обязанности ответственного за обеспечение безопасности ПДн

Ответственный должен выполнять следующий минимальный перечень функций:

1) выполняет работы по внедрению специальных технических и программно-математических средств защиты информации;
2) обеспечение организационных и инженерно-технических мер защиты ИСПДн;
3) разрабатывает планы и графики работ по техническому обслуживанию и ремонту электронного оборудования технических средств защиты информации и повышению эффективности его использования;
4) участвует в проверке, приемке и освоении вновь вводимых в эксплуатацию технических средств защиты информации;
5) ведет учет неисправностей, поломок и аварий оборудования технических средств защиты информации, анализирует причины и определяет направления их устранения;
6) изучает режимы работы оборудования технических средств защиты информации и условия его эксплуатации;

7) выполняет работы по эксплуатации, обслуживанию и ремонту средств технической защиты информации;
8) разрабатывает предложения по доработке (модернизации) оборудования технических средств защиты информации, повышающие его надежность, долговечность и эффективность применения;
9) составляет заявки на приобретение оборудования технических средств защиты информации, запасного имущества, принадлежностей и материалов к нему, ремонт неисправных устройств;
10) организует хранение и списание оборудования и средств защиты информации, не подлежащих дальнейшему использованию по назначению;
11) устанавливает разграничение полномочий пользователей и порядок доступа к информационным ресурсам, порядок использования основных и вспомогательных технических средств и систем;
12) проводит контроль выполнения работниками организации работ согласно перечню мероприятий по обеспечению безопасности информации;
13) ведет учет нештатных ситуаций; информирует руководство и уполномоченных работников службы безопасности об инцидентах и попытках несанкционированного доступа к информации, элементам автоматизированных систем управления по результатам функционирования и контроля систем технической защиты информации;
14) осуществляет администрирование сервисами и механизмами безопасности автоматизированных систем управления, комплексами и средствами технической защиты информации и контроля;
15) готовит предложения по совершенствованию технологических мер защиты информации;
16) контролирует работы по установке, модернизации и профилактике аппаратных и программных средств; созданию, учету, хранению и использованию резервных и архивных копий массивов данных и электронных документов;
17) контролирует работы по внесению изменений в программно-аппаратную конфигурацию автоматизированных систем управления и их соответствие требованиям обеспечения безопасности информации;
18) ведет учет носителей информации, осуществляет их хранение, прием, выдачу ответственным исполнителям, контролирует правильность их использования.

1.7.4.Функциональные обязанности ответственного за технические средства обработки ПДн

Функции могут быть совмещены с функциями системного администратора Учреждения.
Ответственный должен выполнять следующий минимальный перечень функций:

1) участвует в работах по внедрению специальных технических и программно-математических средств защиты информации;
2) разрабатывает планы и графики работ по техническому обслуживанию и ремонту электронного оборудования средств обработки ПДн и повышению эффективности его использования;
3) участвует в проверке, приемке и освоении вновь вводимых в эксплуатацию средств обработки ПДн;
4) ведет учет неисправностей, поломок и аварий оборудования средств обработки ПДн, анализирует причины и определяет направления их устранения;
5) изучает режимы работы оборудования средств обработки ПДн и условия его эксплуатации;
6) выполняет работы по эксплуатации, обслуживанию и ремонту средств обработки ПДн;
7) разрабатывает предложения по доработке (модернизации) оборудования средств обработки ПДн, повышающие его надежность, долговечность и эффективность применения;
8) составляет заявки на приобретение оборудования средств обработки ПДн, запасного имущества, принадлежностей и материалов к нему, ремонт неисправных устройств;
9) организует хранение и списание оборудования средств обработки ПДн, не подлежащих дальнейшему использованию по назначению;
10) ведет учет нештатных ситуаций; информирует руководство и уполномоченных работников службы безопасности об инцидентах и попытках несанкционированного доступа к информации, элементам автоматизированных систем управления;
11) осуществляет администрирование сервисами и механизмами средств обработки ПДн;
12) прекращает работы при несоблюдении установленной технологии обработки информации и невыполнении требований информационной безопасности;

13) контролирует работы по установке, модернизации и профилактике аппаратных и программных средств; созданию, учету, хранению и использованию резервных и архивных копий массивов данных и электронных документов;
14) принимает участие в работах по внесению изменений в программно-аппаратную конфигурацию автоматизированных систем управления.

1.8. Порядок внедрения новых информационных ресурсов, содержащих персональные данные

1.8.1. Определение перечня персональных данных. Согласие субъекта ПДн на обработку

На начальном этапе внедрения новой ИСПДн определяется перечень обрабатываемых ПДн (далее Перечень). Каждый элемент Перечня должен быть элементарным (то есть не должен быть объединением других элементов, например, элемент «ФИО и паспорт» на самом деле состоит из двух элементов списка: ФИО, паспорт) и оформлен в виде пункта документа «Перечень персональных данных, обрабатываемых в Учреждения» с указанием обоснования и цели обработки и закреплен внутренним нормативным актом «Приказ об утверждении перечня персональных данных».

Учреждение должно проводить обоснованную обработку ПДн: каждому элементу Перечня должно быть приведено обоснование.

Далее определяется согласия субъекта на обработку его ПДн.

Согласие должно содержать следующие данные:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
4) цель обработки персональных данных;
5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
9) подпись субъекта персональных данных.

1.8.2. Уведомление о начале обработки персональных данных в Роскомнадзор России

С помощью Перечня (см. п. 2.3.1) определяется необходимость отправки уведомления в Роскомнадзор России. Отправка не требуется если обработка ПДн ведется на одном из следующих основаниях:

1) обработка в соответствии с трудовым законодательством;
2) договорные отношения;
3) обработка общедоступных данных;
4) обработка только ФИО Субъекта;
5) сбор данных, собираемых для однократных пропусков.
6) включенных в ИСПДн, имеющие статус государственных информационных систем персональных данных;
7) обработка без использования средств автоматизации.

В иных случаях через Портал персональных данных Роскомнадзора России оформляется уведомление в электронном виде.

1.8.3. Определение списка лиц, имеющих доступ к обработке персональных данных

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Круг лиц, имеющих доступ к ПДн, должен быть достаточным для выполнения непрерывной и бессбойной обработки персональных данных, и при этом быть максимально ограниченным для снижения рисков утечки информации.

Список может представлять собой перечень структурных подразделений непосредственно собирающих и обрабатывающих персональные данные с обязательным указанием третьих лиц, имеющих доступ к ПДн (Приложение №2), либо перечень конкретных лиц, осуществляющих сбор и обработку.

Список должен содержать следующие данные:

1) ФИО/Должность лица;
2) Помещения;
3) Ресурс ПДн;
4) Дата получения доступа;
5) Роспись в уведомлении о доступе;
6) Дата прекращения доступа;
7) Роспись в уведомлении о прекращении доступа ,–

и должен быть утвержден соответствующим приказом.

1.8.4. Определение контролируемой зоны и помещений обработки персональных данных

Контролируемая зона - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Контролируемая зона может ограничиваться периметром охраняемой территории частично, охраняемой территорией, охватывающей здания и сооружения, в которых проводятся закрытые мероприятия, частью зданий, комнатой, кабинетом, в которых проводятся закрытые мероприятия. Контролируемая зона может устанавливаться размером больше, чем охраняемая территория, при этом она должна обеспечивать постоянный контроль за неохраняемой частью территории.

Территория контролируемой зоны определяется Приказом (или иным внутренним нормативным актом) Руководителя (Приложение №9).

Помещениями обработки персональных данных являются все помещения на территории Контролируемой зоны Учреждения, в которых содержатся:

1) сервера обработки ПДн;
2) системы хранения данных, содержащих ПДн;
3) системы резервного копирования систем обработки и хранения ПДн;
4) системы защиты информации;
5) станции ввода, обработки, просмотра ПДн.

Перечень помещений обработки персональных данных определяется Приказом (или иным внутренним нормативным актом) Руководителя.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

1.8.5. Определение прав доступа лиц, имеющих доступ к обработке персональных данных

Права доступа лиц, имеющих доступ к обработке персональных данных, определяются в необходимом и достаточном объеме для осуществления обработки. Предоставление прав реализуется ответственным за обеспечение безопасности персональных данных. Объем необходимых прав определяется ответственным за организацию работ по защите персональных данных по устному согласованию с руководителем подразделения, осуществляющего обработку ПДн.

1.8.6. Определение прав доступа лиц, имеющих доступ к сопровождению систем защиты и обработки персональных данных

Права доступа лиц, имеющих доступ к сопровождению систем защиты и обработки персональных данных, определяются из соображений разделения ролей обеспечения безопасности персональных данных и обеспечения работы систем обработки персональных данных.

Роль обеспечения безопасности должна реализовывать следующие функции:

1) Аудит доступа (организационный и инструментальный).
2) Назначение прав доступа.
3) Установка и удаление из системы СЗИ.
4) Управление настройками СЗИ.

Роль обеспечения работы систем обработки персональных данных должна реализовывать следующие функции:

1) Установка и удаление средств обработки ПДн.
2) Управление настройками средств обработки ПДн.
3) Установка и удаление вспомогательных средств обработки ПДн и не связанных с обработкой систем.
4) Управление настройками вспомогательных средств обработки ПДн и не связанных с обработкой систем.

Права доступа регламентируются соответствующими внутренним нормативным актом: матрицей доступа.

1.9. Проектирование системы защиты персональных данных

1.9.1. Определение угроз безопасности персональным данным

В соответствии с постановлением Правительства Российской Федерации № 1119 от 01 ноября 2012 г., Приказом ФСТЭК России №21 от 18 февраля 2013г. требуется разработать «Модель угроз безопасности персональным данным» на каждую ИСПДн.

Модель угроз разрабатывается в соответствии с РД «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России. Оценка рисков должна производится как совокупная экспертная оценка специалистов по обеспечению безопасности и специалистов по обеспечению работы систем обработки данных.

1.9.2. Классификация информационной системы персональных данных

Классификация проводится Комиссией (см. п. 2.1).

По результатам анализа исходных данных уровень защищенности (класс) информационной системы персональных данных определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами.

1.9.3. Выбор средств защиты персональных данных

Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

На территории РФ единственной формой оценки соответствия является сертификация на соответствие требованиям безопасности информации ФСТЭК России и ФСБ России.

Выбранные СЗИ должны обеспечивать нейтрализацию всех угроз, выявленных в модели угроз безопасности персональным данным.

Перечень внедренных СЗИ и СКЗИ должен быть отражен в журналах, ведущихся ответственным за обеспечение безопасности персональных данных (Приложение № 3, 4).

1.9.4. Оценка соответствия системы защиты требованиям по информационной безопасности

Оценка соответствия внедренной системы защиты проводится с использованием сертифицированных в системе сертификации ФСТЭК России инструментальных средств с оформлением заключения о готовности системы защиты или проведении аттестационных испытаний с привлечением лицензиата ФСТЭК России.

В случае аттестации, при успешных испытаниях выдается официальный Аттестат соответствия ИСПДн требованиям по безопасности информации.

Обеспечение безопасности персональных данных

1.10. Информационные ресурсы, содержащие персональные данные

Информационные ресурсы, содержащие персональные данные, должны быть обособлены и не пересекаться с информационными ресурсами систем обработки иных систем. Обособление должно обеспечиваться организационными мерами, мерами физической защиты и средствами защиты информации.

Информационные ресурсы создаются для обработки, хранения, передачи информации, содержащей ПДн и объединенных одной целью обработки.

1.10.1. Передача персональных данных

Под передачей персональных данных субъекта понимается распространение информации по каналам связи и на материальных носителях.

При передаче персональных данных работники Учреждения должны соблюдать следующие требования:

Не сообщать персональные данные субъекта в коммерческих целях. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи не допускается.

Осуществлять передачу персональных данных субъектов в пределах Учреждения в соответствии с настоящим Положением, нормативно-технологической документацией и должностными инструкциями.

Разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей.

Передавать персональные данные субъекта представителям субъекта в порядке, установленном законодательством и нормативно-технологической документацией и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

1.10.2. Хранение и использование персональных данных

Под хранением персональных данных понимается существование записей в информационных системах и на материальных носителях.

Персональные данные субъектов обрабатываются и хранятся в информационных системах, а также на бумажных носителях в Учреждении.

Хранение персональных данных субъекта может осуществляться не дольше, чем этого требуют цели обработки, если иное не предусмотрено федеральными законами.

1.10.3. Сроки хранения персональных данных

Сроки хранения персональных данных пациентов регламентированы Перечнем форм первичной медицинской документации учреждений здравоохранения.

1.11. Порядок предоставления доступа к информационным ресурсам, содержащим персональные данные

1.11.1. Порядок предоставления доступа

Порядок предоставления доступа сотрудникам, осуществляющим обработку ПДн, должен быть регламентирован внутренним нормативным актом (см. п. 2.3.3).

На каждую ИСПДн должна быть разработана «Инструкция по учету лиц, допущенных к работе с персональными данными», матрица доступа, «Инструкция пользователя по обработке персональных данных».

В общем виде порядок доступа новых сотрудников должен осуществляться по следующей схеме:

1) Принимаемый сотрудник в соответствии с занимаемой должностью и Приказом о списке лиц, имеющих доступ к обработке ПДн (см. п. 2.3.3) наделяется правом доступа к обработке ПДн;
2) Сотрудник ознакамливается с «Приказом о списке лиц, имеющих доступ к обработке ПДн», «Обязательством о неразглашении информации конфиденциального характера» Положениями и Инструкциями по работе с персональными данными и ставит отметки об ознакомлении в «Журнале инструктажа персонала»;
3) Сотрудник расписывается в «Журнале учета лиц, имеющих доступ к обработке ПДн», получая доступ к соответствующим информационным ресурсам.

1.11.2. Порядок прекращения доступа

В общем виде порядок прекращения доступа сотрудников (в связи с увольнением или иным причинам отсутствия необходимости обработки ПДн, используя конкретный информационный ресурс) должен расписаться в «Журнале учета лиц, имеющих доступ к обработке ПДн», указав дату прекращения доступа.

1.12. Аудит безопасности систем обработки персональных данных

1.12.1. Виды аудита

Аудит безопасности производится ответственным за обеспечение безопасности персональных данных регулярно, а также в ситуациях, требующих проведения расследования инцидента, связанного с нарушением информационной безопасности.

Ответственный должен руководствоваться инструкциями и правилами (Приложения №5-12):

а) Правила парольной защиты.
б) Правила антивирусной защиты.
в) Правила обновления общесистемного и прикладного программного обеспечения ИСПДн.
г) Порядок работы с электронным журналом обращений пользователей информационной системы к ПДн.
д) Порядок предоставления информации.
е) Порядок расследования инцидентов безопасности.
ж) Порядок приостановки предоставления доступа к ПДн в случае обнаружения нарушений порядка их обработки.
з) Инструкция по организации резервирования и восстановления.

Аудит состоит из пассивных и активных мер контроля.

1.12.2. Протоколирование и пассивный аудит

Протоколирование и пассивный аудит предназначены для осуществления контроля за наиболее критичными компонентами сети, включающими в себя серверы приложений, баз данных и прочие сетевые серверы, межсетевые экраны, рабочие станции управления сетью и т.п. Компоненты этой подсистемы осуществляют протоколирование, централизованный сбор и анализ событий, связанных с безопасностью (включая предоставление доступа, попытки аутентификации, изменение системных политик и пользовательских привилегий, системные сбои и т.п.). Они включают в себя как средства защиты информации, так и встроенные средства, имеющиеся в составе ОС, СУБД, приложений и т.п. осуществляющие обработку ПДн и предназначенные для регистрации событий безопасности. Все данные аудита поступают на выделенный сервер аудита, где осуществляется их хранение и обработка.

Подсистема пассивного аудита безопасности выполняет следующие основные функции:

а) отслеживание событий, влияющих на безопасность системы;
б) регистрация событий, связанных с безопасностью в журнале аудита;
в) выявление нарушений безопасности, путем анализа данных журналов аудита ответственным за обеспечение безопасности ПДн в фоновом режиме.

Средства протоколирования и аудита должны применяться на всех рубежах защиты в следующем объеме:

1) На рубеже защиты внешнего периметра должны протоколироваться следующие события:
   а) информация о состоянии внешнего маршрутизатора, МЭ, сервера удаленного доступа, модемов;
   б) действия внешних пользователей по работе с внутренними информационными ресурсами;
   в) действия внутренних пользователей по работе с внешними информационными ресурсами;
   г) попытки нарушения правил разграничения доступа на МЭ;
   д) действия администраторов МЭ;
2) На рубеже защиты серверов и рабочих станций средствами подсистем аудита безопасности ОС должно обеспечиваться протоколирование всех системных событий, связанных с безопасностью, включая удачные и неудачные попытки регистрации пользователей в системе, доступ к системным ресурсам, изменение политики аудита и т. п.;
3) На уровне приложений должна обеспечиваться регистрация событий, связанных с их функционированием, средствами этих приложений.

Эффективность функционирования системы пассивного аудита безопасности определяется следующими основными свойствами этой системы:

а) наличие средств аудита, обеспечивающих возможность выборочного контроля любых происходящих в системе событий, связанных с безопасностью;

б) наличие средств централизованного управления журналами аудита, политикой аудита и централизованного анализа данных аудита по всем контролируемым системам;
в) непрерывность контроля над критичными компонентами ЛВС во времени.

1.12.3. Активный аудит

Активный аудит безопасности предназначен для автоматического выявления нарушений безопасности критичных компонентов ИСПДн и реагирования на них в режиме реального времени. К числу критичных компонентов ИСПДн, с наибольшей вероятностью подверженных атакам со стороны злоумышленников, относится внешний защищенный шлюз в сеть Интернет, сервер удаленного доступа, серверная группа и рабочие станции управления сетью.

Для сбора информации и реагирования на инциденты используются сертифицированные средства анализа защищенности сетей, операционных систем.

Анализатор сетевого трафика должен обнаруживать известные типы сетевых атак при подключении к сетям международного обмена.

Анализ защищенности должен проводиться путем эмуляции действий возможного злоумышленника по осуществлению удаленных атак, а также средства системного уровня, и предназначенные для анализа параметров конфигурации операционных систем и приложений, выявления уязвимостей, коррекции конфигурационных параметров и контроля изменения состояния операционных систем и приложений.

Средства анализа защищенности системного и прикладного уровней предназначены для решения следующих основных задач:

1) анализ параметров конфигурации операционных систем и приложений по шаблонам с целью выявления уязвимостей, связанных с их некорректной настройкой, определения уровня защищенности контролируемых систем и соответствия политике безопасности организации;
2) коррекция конфигурационных параметров операционных систем и приложений;
3) контроль изменения состояния операционных систем и приложений, осуществляемый на основе мгновенных снимков их параметров и атрибутов файлов.

Средства контроля защищенности системного уровня должны выполнять проверки привилегий пользователей, политик управления паролями и регистрационных записей пользователей, параметров подсистемы резервного копирования, командных файлов, параметров системы электронной почты, настройки системных утилит и т.п.

1.13. Расследование инцидентов информационной безопасности

1.13.1. Порядок регистрации

Источником информации об инциденте информационной безопасности может служить следующее:

1) сообщения работников, пациентов Учреждения, направленные в Учреждение в виде сообщений по электронной почте, служебных записок, писем, заявлений и т.д.;
2) уведомления/сообщения органов осуществляющих контроль или надзор за деятельностью Учреждения;
3) данные, полученные на основании анализа журналов СЗПДн.

При получении сообщения об инциденте информационной безопасности по электронной почте или по телефонному звонку необходимо убедиться в достоверности полученной информации (например путем совершения «обратного» звонка по указанным в сообщении телефонам, проверки данных указанных в подписи сообщения или названных при звонке).

Сотрудник, получивший информацию об инциденте, должен сообщить об этом ответственному за обеспечение безопасности ПДн. Ответственный за обеспечение безопасности сообщает об инциденте ответственному за организацию безопасности и начальнику подразделения, в котором случился инцидент.

Все инциденты информационной безопасности должны регистрироваться в журнале регистрации нештатных ситуаций (Приложение №13). Журнал инцидентов информационной безопасности должен постоянно актуализироваться.

1.13.2. Порядок разбора

Разбором инцидентов информационной безопасности занимается Комиссия (см. п. 2.1).

После сбора информации ответственным за обеспечение безопасности по инциденту Комиссия анализирует все данные об обстоятельствах инцидента (электронные письма, логи информационных систем, показания сотрудников и др.).

Комиссия обязана установить имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лица, виновные в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению.

По окончании разбора инцидента информационной безопасности комиссией оформляется отчет, в котором указываются основные «контрольные точки» инцидента.

Отчет предоставляется Руководителю Учреждения. В конце отчета указывается причина возникновения инцидента и предложения по недопущению подобных инцидентов в будущем.

После окончания расследования Комиссия принимает решение о наказании виновных лиц и согласовывает решение с Руководителем.

1.14. Предоставление информации по обращению субъекта персональных данных

Все обращения субъектов ПДн регистрируются в «Журнале регистрации обращений субъектов персональных данных» (Приложение №14).

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;
2) правовые основания и цели обработки персональных данных;
3) цели и применяемые оператором способы обработки персональных данных;
4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
6) сроки обработки персональных данных, в том числе сроки их хранения;
7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 г. N 152-ФЗ «О персональных данных»;
8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
10) иные сведения, предусмотренные Федеральным законом от 27.07.2006 г. N 152-ФЗ «О персональных данных» или другими федеральными законами.

Приложение № 1
Журнал учета лиц,
допущенных к работе с
персональными данными

ЖУРНАЛ

УЧЕТА ЛИЦ, ДОПУЩЕННЫХ К РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

ИНВ. № _____

Начат: «____» _____ 20___ г.

Окончен: «____» _____ 20___ г.

На _____ листах

№ п/п	Ф.И.О.	Должность	Сведения о допуске к персональным данным			Сведения о прекращении допуска к персональным данным		
			наименование ИСПДн / неавтоматизированная обработка	дата утверждения «Списка…»	дата и подпись допускаемого лица	дата утверждения «Списка…» или дата приказа об увольнении	номер приказа об увольнении	дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн
1	2	3	4	5	6	7	8	9

Приложение № 2
Журнал учета СЗИ

ЖУРНАЛ

УЧЕТА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ,
ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ
ИНВ. № _____

Начат: «___» _____ 20__г.

Окончен: «___» _____ 20__г.

На _____ листах

Номер п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание
1	2	3	4	5	6	7

Приложение № 3
Журнал учета СКЗИ

ЖУРНАЛ

УЧЕТА СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ,
ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ
ИНВ. № _____

Начат: «___» _____ 20__г.

Окончен: «___» _____ 20__г.

На _____ листах

№ п.п.	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых докумен-тов	Номера экземпляров (криптографичес-кие номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводи-тельного письма	Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к кото-рым подклю-чены крипто-средства	Дата изъятия (уничто-жения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Приложение № 4
Правила парольной защиты

ПРАВИЛА ПАРОЛЬНОЙ ЗАЩИТЫ

1. Общие положения

Целью применения и реализации Правил парольной защиты является недопущение утечки ПДн, а также их несанкционированной модификации или уничтожения и действует для всех пользователей и администраторов ИСПДн оператора.

Правила парольной защиты регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль над действиями пользователей при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение безопасности ПДн.

Личные пароли должны генерироваться и распределяться централизованно либо создаваться пользователями ИСПДн самостоятельно с учетом следующих требований:

- пароль должен быть не менее 6-ти символов;
- в числе символов пароля ***обязательно должны присутствовать*** буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от значений 24-х предыдущих паролей;
- максимальный срок действия пароля пользователя составляет 90 дней;
- минимальный срок действия пароля пользователя составляет 2 дня;
- пользователь не имеет права сообщать личный пароль другим лицам.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

При наличии, в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п., технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение ответственному за обеспечение безопасности ПДн. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже двух раз в квартал.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой на основании письменного указания начальника отдела.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) ответственного за обеспечение безопасности ПДн.

2. Контроль

Контроль за действиями пользователей ИСПДн при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственного за обеспечение безопасности в организации.

Приложение № 5
Правила антивирусной защиты

ПРАВИЛА АНТИВИРУСНОЙ ЗАЩИТЫ

1. Общие требования

Правила антивирусной защиты определяют требования к организации защиты ИСПДн от разрушающего воздействия вредоносных программ и устанавливают ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

Целью защиты ИСПДн от вредоносных программ является предотвращение и нейтрализация негативных воздействий вредоносных программ на средства вычислительной техники.

К использованию в ИСПДн допускаются только лицензионные и сертифицированные ФСТЭК или ФСБ России по требованиям безопасности информации средства защиты от вредоносных программ.

Установка и начальная настройка средств защиты от вредоносный программ в ИСПДн осуществляется представителями организации – лицензиата ФСТЭК России, впоследствии – ответственным за обеспечение безопасности ПДн.

Ответственный за обеспечение безопасности ПДн должен организовывать осуществление периодического обновления сигнатур средств защиты от вредоносных программ и контроль их работоспособности не реже чем один раз в неделю.

Пользователи ИСПДн обязаны руководствоваться в работе настоящими правилами антивирусной защиты и «Инструкцией пользователя ИСПДн...».

2. Применение средств защиты от вредоносных программ

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с ответственным за обеспечение безопасности ПДн, если он назначен на объекте) должен провести внеочередной антивирусный контроль своего персонального компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу персонального компьютера;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение безопасности ПДн;
- провести «лечение» или удаление зараженных файлов.

3. Ответственность

Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями Настоящих Правил возлагается на ответственного за обеспечение безопасности ПДн.

Ответственность за проведение мероприятий антивирусной защиты ИСПДн и соблюдение требований Настоящих Правил возлагается на ответственного за обеспечение безопасности в организации и всех пользователей ИСПДн.

Приложение № 6
Правила обновления
общесистемного и прикладного
программного обеспечения ИСПДн

ПРАВИЛА ОБНОВЛЕНИЯ ОБЩЕСИСТЕМНОГО И ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИСПДн

1. Общие положения

В системе управления ИСПДн оператора должна обеспечиваться и регламентироваться деятельность, связанная с установкой нового оборудования, либо его компонентов, патчей, а также обновлений операционных систем (далее – ОС) и других приложений.

Тестирование нового оборудования и обновлений программного обеспечения (далее – ПО) не должно осуществляться на ресурсах действующей информационной инфраструктуры.

Правила и порядок обновления ПО, ОС и приложений в целях информационной безопасности ИСПДн направлены на защиту ресурсов от:

- нарушения штатной работы информационных ресурсов и сервисов;
- разрушения;
- нарушения штатного функционирования оборудования;
- несанкционированной модификации;
- несанкционированного копирования.

2. Правила управления обновлениями ПО ИСПДн в информационной инфраструктуре оператора.

- Отслеживание появления новых уязвимостей в используемой ОС, появление патчей, изготовленных производителями с целью устранения указанных уязвимостей, должно регламентироваться и производиться в плановом порядке;
- Установке патчей должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от вновь устанавливаемых патчей;
- В случае обнаружения негативного воздействия, устанавливаемого патча на штатное функционирование информационной инфраструктуры, данный патч устанавливаться не должен;
- Установке новых версий ПО или внесению изменений и дополнений в действующее ПО должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного ПО;
- Установка протестированных патчей может быть произведена только на основании решения ответственного за обеспечение безопасности ПДн;
- Установка новых версий ПО или внесение изменений и дополнений в действующее ПО может быть произведено только по согласованию с ответственным за обеспечение безопасности ПДн;
- Применение организационно-технических и/или аппаратно-программных решений может быть произведено только по согласованию с ответственным за обеспечение безопасности ПДн.

3. Контроль

Контроль за выполнением требований Настоящих Правил должен осуществлять ответственный за обеспечение безопасности в организации.

Приложение № 7
Порядок работы
с электронным журналом
обращений пользователей
информационной системы к ПДн

ПОРЯДОК РАБОТЫ С ЭЛЕКТРОННЫМ ЖУРНАЛОМ ОБРАЩЕНИЙ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ К ПДн

1. Общие положения

Правила и порядок протоколирования и анализа (аудита) значимых событий в ИСПДн, направлены на превентивную фиксацию и изучение действий субъектов и объектов в ИСПДн.

Все события, происходящие в ОС, ИСПДн, других критических приложений и СЗИ должны протоколироваться в специальные электронные журналы аудита.

Аудит событий, зафиксированных в указанных электронных журналах, должен анализироваться в плановом порядке на постоянной основе.

2. Настройки безопасности систем аудита

Электронные журналы аудита должны записываться и вестись в автоматизированном режиме.

Настройки журналов аудита должны однозначно интерпретировать все значимые события ИСПДн.

Электронные журналы аудита не должны быть доступны на чтение, уничтожение и модификацию пользователям ИСПДн.

Электронные журналы аудита не должны быть доступны на уничтожение и модификацию администраторам ИСПДн.

Электронные журналы аудита должны быть доступны на чтение и архивирование сотруднику, выполняющему функции ответственного за обеспечение безопасности ПДн.

Размер каждого электронного журнала составляет 16 Мб. Затирание старых событий журнала происходит по необходимости по мере заполнения журнала.

3. Контроль

Контроль выполнения положений и требований порядка работы с электронным журналом обращений пользователей информационной системы к ПДн должен осуществлять ответственный за обеспечение безопасности в организации.

Приложение № 8
Порядок предоставления информации

ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ИНФОРМАЦИИ ОРГАНАМ ГОСУДАРСТВЕННОЙ ВЛАСТИ И МЕСТНОГО САМОУПРАВЛЕНИЯ, ФИЗИЧЕСКИМ И ЮРИДИЧЕСКИМ ЛИЦАМ

1. Общие положения

Оператор должен предоставлять информацию, содержащую ПДн субъекта, третьим лицам только с письменного согласия субъекта ПДн за исключением случаев, предусмотренных частью 2 статьи 9 Федерального Закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Информация, содержащая ПДн субъекта и предоставляемая третьим лицам, должна быть достоверной и не избыточной, по отношению к целям, заявленным этими лицами, при сборе ПДн.

При передаче обработки ПДн другому лицу на основании договора, оператор должен зафиксировать в нем обязанность указанного лица в обеспечении конфиденциальности ПДн и безопасности данных при их обработке.

2. Трансграничная передача данных

При трансграничной передаче ПДн оператор должен руководствоваться положениями статьи 12 Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных».

Приложение № 9
Порядок расследования
инцидентов безопасности

ПОРЯДОК ПРОВЕДЕНИЯ СЛУЖЕБНОГО РАССЛЕДОВАНИЯ НАРУШЕНИЙ РЕЖИМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИСПДн

1. Общие положения

Данный порядок устанавливает правила классификации нарушений информационной безопасности и процедуры служебного расследования (назначения, проведения и выработки выводов) для определения уровня защищенности ИСПДн оператора и мер по возможному предотвращению инцидентов информационной безопасности.

2. Классификация инцидентов информационной безопасности

Нарушения режима информационной безопасности и их последствия классифицируются по значимости на:

- Нарушения I категории.
- Нарушения II категории.
- Нарушения III категории.

Служебное расследование назначается по нарушениям I и II категорий.

3. Перечень инцидентов информационной безопасности

Инциденты I категории, к каковым относятся нарушения, повлекшие за собой разглашение (утечку) защищаемых ПДн и/или утрату содержащих их отчуждаемых носителей, уничтожение (искажение) ИСПДн, выведение из строя технических и программных средств, а именно:

- подбор административного пароля (успешный);
- несанкционированная реконфигурация параметров ИСПДн;
- утрата или кража резервной копии базы ПДн;
- необоснованная передача массивов ПДн;
- умышленное нарушение работоспособности ИСПДн;
- несанкционированный доступ к ПДн ИСПДн;
- несанкционированное внесение изменений в ИСПДн;
- умышленное заражение компьютеров и серверов ИСПДн вирусами;
- проведение работ с ИСПДн, повлекшее за собой необратимую потерю данных.

Инциденты II категории, к каковым относятся: нарушения, в результате которых возникают предпосылки к разглашению (утечке) защищаемых ПДн, утрате содержащих их отчуждаемых носителей, уничтожению (искажению) ИСПДн, выведению из строя технических и программных средств, а именно:

- ошибка при входе в ИСПДн (набор не назначенного пароля, более трех раз подряд, периодически);
- несанкционированное (неоднократное) оставление включенного ПК;
- перезагрузка компьютера, при сбоях в работе ПК, (неоднократная) в т.ч. аварийная (неоднократная) перезагрузка, путем нажатия кнопки RESET;
- утрата учтенного отчуждаемого съемного носителя;
- попытка входа под чужим именем, паролем, многократная неудачная;
- попытка входа под чужим именем пользователя, паролем, удачная;
- несанкционированная очистка журналов аудита;
- несанкционированное копирование ПДн на внешние носители;
- несанкционированная установка (удаление) ПО ИСПДн;
- несанкционированное изменение конфигурации ПО ИСПДн;
- попытка получения прав администратора на локальном ПК (увеличения собственных прав, получение прав на отладку программ) удачная и неудачная;

– попытка получения прав администратора в домене или на удаленной машине удачная и неудачная;
– неумышленное заражение локального или сетевого ПК компьютерными вирусами;
– несанкционированное использование сканирующего ПО;
– несанкционированное использование анализаторов протоколов (снифферов);
– несанкционированный просмотр, вывод на печать и т.п. ПДн.

Инциденты III категории, к каковым относятся нарушения, не несущие признаков нарушений I и II категорий, а именно:
– ошибка при входе в ИСПДн (набор неправильного пароля, сетевого имени более трех раз подряд, не периодическая);
– попытка неудачного доступа к ПДн ИСПДн (периодическая);
– перевод времени на ПК;
– выполнение собственных производственных обязанностей на компьютере в неразрешенное время;
– перезагрузка компьютера, при сбоях в работе ПК, (однократная) в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;
– нецелевое использование корпоративных ресурсов (печать, Internet, mail, и т.п.).

4. Назначение и проведение служебного расследования

Служебное расследование назначается по нарушениям I и II категорий.

Состав комиссии, а также сроки проведения служебного расследования назначаются распоряжением сотрудника, ответственного за обеспечение безопасности персональных данных, по каждому отдельному факту нарушения или по факту группы нарушений.

Служебное расследование может быть инициировано на основании устного заявления, докладной или служебной записки любого сотрудника оператора по выявленному отдельному факту нарушения, либо по факту группы нарушений.

5. Состав комиссии для проведения служебного расследования

В состав комиссии входят лица, назначенные приказом главного врача «О создании комиссии для организации работы по защите персональных данных».

В случае необходимости Председатель комиссии может привлекать к работе:
– администраторов управления информатизации и телекоммуникаций;
– непосредственного начальника нарушителя;
– экспертов из других подразделений;
– привлеченных специалистов организаций-лицензиатов.

6. Члены комиссии имеют право:

Требовать документального подтверждения факта нарушений информационной безопасности ИСПДн оператора.

Устанавливать причины допущенных нарушений любым из способов, не противоречащим законодательству РФ.

Брать письменные объяснения по поводу выявленных нарушений у любого сотрудника оператора.

7. Ответственность.

Ответственность за выявление и классификацию инцидента информационной безопасности, требующего проведения процедуры служебного расследования несет ответственный за обеспечение безопасности ПДн.

Ответственность за назначение процедуры служебного расследования несет руководитель организации.

Ответственность за проведение процедуры служебного расследования несет сотрудник, ответственный за обеспечение безопасности персональных данных в ИСПДн оператора.

Ответственность за содержание, обоснованность, актуализацию Настоящего Порядка, а также надлежащее выполнение его положений несет ответственный за обеспечение безопасности ПДн.

8. Оформление результатов работы комиссии

Результаты работы Комиссии должны быть оформлены в виде аналитического экспертного заключения на имя руководителя, ответственного за обеспечение безопасности персональных данных, с предложениями по необходимым организационным выводам, а также по расширению или дополнению «Примерного перечня нарушений».

Результатом работы Комиссии должен стать АКТ, в котором изложены:

- Документальное подтверждение факта нарушений информационной безопасности ИСПДн оператора;
- установленные причины выявленных нарушений в ИСПДн оператора;
- сформированные предложения по устранению причин выявленных инцидентов информационной безопасности в ИСПДн оператора»;
- предложения по расширению (дополнению) «Перечня инцидентов информационной безопасности».

Приложение № 10
Порядок приостановки
предоставления доступа к ПДн
в случае обнаружения нарушений
порядка их обработки

ПОРЯДОК ПРИОСТАНОВКИ ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПДн В СЛУЧАЕ ОБНАРУЖЕНИЯ НАРУШЕНИЙ ПОРЯДКА ИХ ОБРАБОТКИ

1. Общие положения

Целью установления Настоящего Порядка является предотвращение утечки и несанкционированного доступа к ПДн при выявлении нарушений режима безопасности при обработке и/или чтении ПДн в ИСПДн.

Работа с ПДн должна приостанавливаться только при обнаружении нарушений I и/или II категорий.

2. Действие должностных лиц в случае обнаружения нарушений

Сотрудник, обнаруживший нарушения при работе с ПДн обязан сообщить об этом своему непосредственному руководителю.

Сотрудник, ответственный за обеспечение безопасности персональных данных в ИСПДн оператора, обязан:

- установить категорию выявленного нарушения;
- при установлении I или II категории нарушения инициировать проведение служебного расследования;
- оповестить все отделы и сотрудников, работающих с ПДн о прекращении доступа к ресурсам ИСПДн на время проведения служебного расследования.

Все отделы и сотрудники, работающие с ПДн обязаны:

- временно (на время проведения служебного расследования) приостановить свою деятельность по работе с ИСПДн;
- содействовать проведению служебного расследования.

Работа с ПДн может возобновляться только после устранения всех выявленных нарушений, их последствий;

Информация о возможности возобновления работы с ИСПДн должна доводиться до всех заинтересованных подразделений лицом, установившим запрет на работы в ИСПДн.

Приложение № 11
Инструкция по организации
резервирования и восстановления

Инструкция по организации резервирования и восстановления программного обеспечения, баз персональных данных информационных систем персональных данных в «государственном бюджетном учреждении здравоохранения Свердловской области «Ивдельская центральная районная больница»

1. Общие требования

1.1. Настоящая инструкция разработана в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации № 1119 от 01 ноября 2012 г., с целью обеспечения возможности незамедлительного восстановления персональных данных (далее – ПДн), модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2. Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных (далее – ИСПДн) государственного бюджетного учреждения здравоохранения Свердловской области «Ивдельская центральная районная больница» (далее – оператор).

2. Резервируемое общесистемное и специальное программное обеспечение, программное обеспечение средств защиты информации и базы персональных данных

2.1. Необходимо осуществлять резервное копирование актуальной информации и данных, используемых для полного восстановления БД, содержащих персональные данные.

2.2. Резервное копирование осуществляется во внешнее хранилище (сервер резервного копирования, ЖМД, ГМД, CD-ROM, USB накопитель).

2.3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль в соответствии с инструкцией по антивирусной защите.

3. Порядок резервирования и хранения резервных копий (ответственный за резервирование, периодичность)

3.1 Ежедневно, по окончанию работы с ПДн на ПЭВМ, должно осуществляться резервное копирование актуальных ПДн во внешнее хранилище, создавая тем самым резервный электронный архив актуальных ПДн.

3.2 Еженедельно, в пятницу, по окончании рабочего дня, должно осуществляться полное копирование данных, необходимых для восстановления работы БД, содержащих ПДн, во внешнее хранилище.

3.3 Электронные носители, на которые осуществляется резервное копирование актуальных ПДн и их копии должны быть поставлены на соответствующий учет.

3.4 Электронные носители, на которые осуществляется резервное копирование актуальных ПДн, должны храниться в специально оборудованном для хранения месте, обеспечивающем сохранность этих носителей.

3.5 Ответственность за организацию резервного копирования в ИСПДн в соответствии с требованиями настоящей Инструкции возлагается сотрудника, ответственного за обеспечение безопасности персональных данных в ИСПДн оператора.

3.6 Ответственность за проведение мероприятий резервного копирования в ИСПДн и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности ПДн и всех пользователей ИСПДн.

4. Порядок восстановления работоспособности ИСПДн

4.1 В случае потери работоспособности ИСПДн, должно быть обеспечено ее восстановление из резервной копии. Восстановление из резервной копии осуществляется в соответствии с документацией, прилагающейся к системе резервного копирования ПО.

Приложение № 12
Порядок уничтожения носителей,
содержащих персональные данные

Порядок уничтожения носителей персональных данных в государственном бюджетном учреждении здравоохранения Свердловской области «Ивдельская центральная районная больница»

1. Работа с бумажными носителями (документами)

1.2.Виды и периоды уничтожения бумажных носителей, содержащих персональные данные (далее – документов).

№ п/п	Документ	Срок хранения	Действия по окончании срока хранения
1.			Уничтожение
2.			Уничтожение

По окончании срока хранения документы, указанные в п. 1.2, уничтожаются путём измельчения на мелкие части, исключающие возможность последующего восстановления информации или сжигаются.

2. Работа с машиночитаемыми носителями

2.1 Виды и периоды уничтожения персональных данных, хранимых в электронном виде («файлах») на жестком диске компьютера (далее - НЖМД) и машиночитаемых носителях: компакт дисках (далее – CD-R/RW, DVD-R/RW в зависимости от формата), дискетах 3,5“ 1.4Mb (далее – FDD).

№ п/п	Информация, вид носителя	Срок хранения	Действия по окончании срока хранения
			Уничтожение носителя; удаление файла с НЖМД
			Уничтожение носителя
			Повторное использование или уничтожение носителя

По окончании указанных в п. 2.1 сроков хранения, машиночитаемые носители, подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления и дальнейшего использования. Это достигается путём деформирования, нарушения единой целостности носителя или его сжигания. Подлежащие уничтожению файлы с персональными данными, удаляются средствами автоматизированного комплекса, использующегося для обработки персональных данных.

В случае допустимости повторного использования носителя формата FDD, CD-RW, DVD-RW, применяется программное удаление («затирание») содержимого диска путём его форматирования с последующей записью новой информации на данный носитель.

3. Порядок оформления документов об уничтожении носителей

В ходе процедуры уничтожения носителей необходимо присутствие членов экспертной комиссии, осуществляющей уничтожение персональных данных и иной конфиденциальной информации.

В ГБУЗ СО «Ивдельская центральная районная больница» уничтожение носителей, содержащих персональные данные осуществляет экспертная комиссия, утверждённая приказом главного врача.

Персональный состав экспертной комиссии по уничтожению носителей, содержащих персональные данные, определяется приказом главного врача

Комиссия составляет и подписывает соответствующий акт об уничтожении носителей персональных данных.

Приложение № 12
Журнал учета
нештатных ситуаций

ЖУРНАЛ

УЧЕТА НЕШТАТНЫХ СИТУАЦИЙ ИСПДН, ВЫПОЛНЕНИЯ ПРОФИЛАКТИЧЕСКИХ РАБОТ,
УСТАНОВКИ И МОДИФИКАЦИИ ПРОГРАММНЫХ СРЕДСТВ НА КОМПЬЮТЕРАХ ИСПДН
ИНВ. № _____

Начат: «___» _____ 20__г.

Окончен: «___» _____ 20__г.

На _____ листах

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи	ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)
1	2	3	4	5	6	7

Приложение № 13
Журнал регистрации
обращений субъектов

ЖУРНАЛ

УЧЕТА ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ВОПРОСАМ
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ИНВ. № _____

Начат: «____» _____ 20___ г.

Окончен: «____» _____ 20___ г.

На _____ листах

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или об отказе в ее предоставлении	Дата передачи / отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8