# Методические рекомендации
# для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости
# (утв. Министерством здравоохранения и социального развития РФ 23 декабря 2009 г.)

## Обозначения и сокращения

**АВС** - антивирусные средства
**АРМ** - автоматизированное рабочее место
**ВТСС** - вспомогательные технические средства и системы
**ИСПДн** - информационная система персональных данных
**КЗ** - контролируемая зона
**ЛВС** - локальная вычислительная сеть
**МЭ** - межсетевой экран
**НСД** - несанкционированный доступ
**ОС** - операционная система
**ПДн** - персональные данные
**ПМВ** - программно-математическое воздействие
**ПО** - программное обеспечение
**ПЭМИН** - побочные электромагнитные излучения и наводки
**САЗ** - система анализа защищенности
**СЗИ** - средства защиты информации
**СЗПДн** - система (подсистема) защиты персональных данных
**СОВ** - система обнаружения вторжений
**ТКУИ** - технические каналы утечки информации
**УБПДн** - угрозы безопасности персональных данных
**ФСТЭК России** - Федеральная служба по техническому и экспортному контролю

## Определения

**Автоматизированная система** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** - подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Биометрические персональные данные** - сведения, которые характеризуют физиологические особенности человека, и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

**Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** - исполняемый программный код или

интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** - программа, предназначенная для осуществления несанкционированного доступа и/или воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** - возможность получения информации и ее использования.

**Закладочное устройство** - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** - присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** - электрический сигнал, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных (ИСПДн)** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Источник угрозы безопасности информации** - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** - пространство (территория, здание, часть здания,

помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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

**Межсетевой экран** - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и/или выходящей из информационной системы.

**Нарушитель безопасности персональных данных** - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**Недекларированные возможности** - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор (персональных данных)** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и/или осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Перехват (информации)** - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и

обработку информативных сигналов.

**Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Политика "чистого стола"** - комплекс организационных мероприятий, контролирующих отсутствие записи ключей и атрибутов доступа (паролей) на бумажные носители и хранения их вблизи объектов доступа.

**Пользователь информационной системы персональных данных** - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и/или блокировать аппаратные средства.

**Программное (программно-математическое) воздействие** - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Раскрытие персональных данных** - умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Ресурс информационной системы** - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Специальные категории персональных данных** - персональные данные, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технические средства информационной системы персональных данных** - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы

звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

**Технический канал утечки информации** - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**Угрозы безопасности персональных данных** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Учреждение** - учреждения здравоохранения, социальной сферы, труда и занятости.

**Уязвимость** - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## Введение

В настоящее время, на территории Российской Федерации осуществляется государственное регулирование в области обеспечения безопасности персональных данных (далее - ПДн). Правовое регулирование вопросов обработки ПДн осуществляется в соответствии с Конституцией Российской Федерации и международными договорами Российской Федерации, на основании вступившего в силу с 2007 года Федерального закона от 27.07.2006 г. N 152-ФЗ "О персональных данных" и принятых во исполнение его положений, нормативно-правовых актов и методических документов.

ГАРАНТ:

Согласно Федеральному закону от 27 июля 2006 г. N 152-ФЗ (в редакции Федерального закона от 23 декабря 2010 г. N 359-ФЗ) информационные системы персональных данных, созданные до 1 января 2011 г., должны быть приведены в соответствие с установленными требованиями не позднее 1 июля 2011 г.

В силу требований указанного Федерального закона "О персональных данных" все информационные системы персональных данных (далее - ИСПДн), созданные до введения его в действие, должны быть приведены в соответствие установленным требованиям не позднее 1 января 2010 года.

Настоящий документ представляет собой методические рекомендации, разъясняющие руководителям учреждений Минздравсоцразвития, в которых эксплуатируются ИСПДн, последовательность действий для приведения ИСПДн в соответствие с законодательством.

Цели методических рекомендаций:

- описание единого подхода к обеспечению безопасности персональных данных и приведению ИСПДн учреждений Минздравсоцразвития в соответствие с ФЗ-152 "О персональных данных";
- предоставление руководителям учреждений Минздравсоцразвития типовых решений по организации защиты ИСПДн;
- составление для учреждений программы работ по приведению ИСПДн в соответствие с ФЗ-152 "О персональных данных";
- планирование проведения первоочередных мероприятий по защите ПД в сжатые сроки - до 1 января 2010 г.;
- предоставление инструментов для снижения и оптимизации финансовых и трудовых затрат при приведении учреждений в соответствие с требованиями ФЗ-152 "О персональных данных".

Методические рекомендации содержат набор типовых шаблонов организационно-распорядительных документов, а также детальные инструкции по их заполнению.

Данные Методические рекомендации разработаны на основании Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" с учетом действующих нормативных документов ФСТЭК и ФСБ России по защите информации.

## 1. Основные обязанности учреждений здравоохранения, эксплуатирующих ИСПДн

Все учреждения и организации системы здравоохранения, социальной сферы, труда и занятости (далее - Учреждения) обязаны обеспечивать защиту персональных данных во внедряемых информационных системах с момента их ввода в эксплуатацию.

В отношении действующих информационных систем, обрабатывающих персональные данные, Учреждения обязаны осуществить ряд мероприятий:

- провести их классификацию с оформлением соответствующего акта;
- до 01.01.2010 реализовать комплекс мер по защите персональных данных в соответствии с перечисленными правовыми актами и методическими документами;
- провести оценку соответствия ИСПДн требованиям безопасности в форме сертификации (аттестации) или декларирования соответствия.

## 2. Основные мероприятия по приведению ИСПДн Учреждений в соответствие с ФЗ-152 "О персональных данных"

Каждое Учреждение, эксплуатирующее ИСПДн, должно выполнить до 1 января 2010 года следующие действия:

1) Разработать и утвердить внутри учреждения приказ о защите персональных данных (см. Приложение 1).

2) Разработать и утвердить внутри учреждения приказ о подразделении по защите персональных данных (см. Приложение 2).

3) Разработать и утвердить внутри учреждения приказ о назначении ответственных лиц за обработку персональных данных (см. Приложение 3).

4) Разработать и утвердить внутри учреждения Концепцию информационной безопасности и Политику информационной безопасности.

5) Разработать и утвердить внутри учреждения приказ о проведении внутренней проверки (см. Приложение 7). Результат оформить в виде отчета (см. Приложение 8).

6) Определить состав и категории обрабатываемых персональных данных (см. раздел 3 на стр. 20 настоящих рекомендаций). Результат оформить в виде перечня ПДн (см. Приложение 6).

7) Осуществить классификацию действующих информационных систем, обрабатывающих персональные данные (см. раздел 4 настоящих рекомендаций). Результат оформить в виде акта классификации (см. Приложение 9).

8) Разработать и утвердить внутри учреждения положение о разграничении прав доступа к обрабатываемым персональным данным (см. Приложение 10).

9) Адаптировать модель угроз к конкретной ИСПДн учреждения (см. Методику составления частной модели угроз). Результат оформить в виде Модели угроз (см. Приложение 11).

10) Разработать и утвердить план мероприятий по защите ПДн (см. Приложение 12). Необходимо учесть, что план мероприятий может быть пересмотрен через 6 месяцев ввиду опубликования новых пояснений по ФЗ-152 со стороны регуляторов.

11) Зарегистрироваться в качестве оператора персональных данных - подготовить и направить уведомление в территориальный орган Россвязькомнадзора - уполномоченный орган по защите прав субъектов персональных данных (см. Приложение 25).

12) Назначить ответственных за обеспечение безопасности персональных данных и подготовить должностные инструкции сотрудников, обрабатывающих ПДн, в составе:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности;
- Инструкция пользователя при работе с ИСПДн;
- Инструкция пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций.

13) Разработать и утвердить порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ (см. Приложение 13).

14) Разработать и утвердить план внутренних проверок состояния защиты ПДн (см. Приложение 14).

15) Разработать и утвердить журнал учета обращений субъектов ПДн о выполнении их законных прав (см. Приложение 16).

16) Разработать и утвердить перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним (см. Приложение 21).

17) Разработать и утвердить электронный журнал обращений пользователей информационной системы к ПДн (см. Приложение 24)

18) Провести необходимые технические мероприятия для обеспечения защиты ПДн при их обработке в ИСПДн (см. раздел 6 на стр. 70). В их состав входят:

а) Обязательные технические мероприятия.

б) Технические мероприятия, выполняемые, при выделении дополнительного финансирования.

19) Декларировать соответствие или провести аттестационные (сертификационные) испытания ИСПДн (см. раздел 8 на стр. 86).

В следующих главах настоящих методических рекомендаций будут даны конкретные рекомендации по выполнению каждого пункта.

## 3. Рекомендации по инвентаризации и категорированию персональных данных, обрабатываемых в ИСПДн Учреждений

Для проведения классификации информационных систем Учреждений необходимо провести мероприятия по сбору и анализу исходных данных по информационной системе и обрабатываемых в ней ПДн, а также провести их инвентаризацию.

ПДн - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных). Применительно к информационным системам Минздравсоцразвития это могут быть следующие сведения:

- ФИО пациента;
- паспортные данные;
- год месяц, дата и место рождения;
- адрес;
- семейное, социальное, имущественное положение;
- образование;
- диагноз, сведения и заключения о состоянии здоровья;
- полис ОМС;
- оказанные медицинские услуги и другие.

Перечень персональных данных можно найти в Приложении "Перечень персональных данных, подлежащих защите".

При проведении обследования информационных систем учреждения по критериям наличия указанной информации руководством принимается решение об обработке в данной информационной системе персональных данных. Решение принимается на основании Отчета о результатах проведения внутренней проверки.

Для правильной классификации информационной системы учреждения важно правильно определить категорию обрабатываемых в информационной системе персональных данных - $X_{пд}$. Определяются следующие категории обрабатываемых в информационной системе персональных данных ($X_{пд}$):

- категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

- категория 4 - обезличенные и/или общедоступные персональные данные.

К персональным данным позволяющим идентифицировать человека относятся такие данные, которые позволяют установить личность человека. Например, на основании только фамилии, имени и отчества нельзя точно установить личность, т.к. существуют полные однофамильцы. Но если в ИСПДн помимо ФИО обрабатываются также данные об адресе проживания, паспортные данные, биометрические данные (фотографическое изображение), данные о месте работы и т.д., то уже на основании их можно выделить конкретного человека.

Обезличенными данными в этом случае, являются данные, на основании которых нельзя идентифицировать субъекта персональных данных.

В категорию дополнительной информации входит любая другая информация, которую можно получить, обратившись к записи персональных данных: информация о доходах, должность, материальном положении и др.

Помимо данных категорий персональных данных, существуют также:

- специальные категории персональных данных - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных;

- биометрические персональные данные - сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию;

В ИСПДн Учреждений обрабатываются преимущественно специальные категории ПД - данные о состоянии здоровья субъектов.

В процессе классификации для снижения затрат на создание СЗПДн и оптимизации класса ИСПДн необходимо рассмотреть и по возможности использовать следующие инструменты:

1) Сегментация. Физическая или логическая сегментация ИСПДн по классам обрабатываемой информации, выделение сегментов сети, в которых происходит автоматизированная обработка персональных данных. Данные работы можно провести с помощью соответствующей настройки существующих в учреждении сертифицированных межсетевых экранов (МСЭ).

2) Обезличивание. Введение в процесс обработки персональных данных процедуры обезличивания существенно упростит задачи по защите персональных данных. Обезличивание можно провести путем нормализации баз данных. После выполнения обезличивания защите будет подлежать (по требованиям регулирующих документов) лишь справочник, позволяющий выполнить обратное преобразование.

3) Разделение ПД на части. В этом случае возможно уменьшение количества субъектов ПДн, обрабатываемых в системе. Это может быть достигнуто, например, за счет использования таблиц перекрестных ссылок в базах данных.

4) Абстрагирование ПДн. Зачастую на некоторых участках обработки или сегментах сети персональные данные можно сделать менее точными, например, путем группирования общих характеристик. При грамотном использовании такой прием позволит без ущерба для основной деятельности снизить класс ИСПДн.

5) Постановка требований поставщикам и разработчикам типовых систем обработки персональных данных, используемых в учреждениях. Включение требований наличия в составе закупаемых информационных систем средств, обеспечивающих защиту персональных данных в соответствии с Законом, позволит снизить затраты на приобретение дополнительных средств защиты.

Для реализации этих методов необходимо обратиться к поставщикам и

разработчикам вашей информационной системы и ее элементов. Особое внимание следует уделить специальному ПО и штатному ПО, дорабатываемому под ваши нужды штатными программистами-разработчиками или сторонними организациями. Правильно спроектированное программное обеспечение и базы данных могут существенно помочь в обеспечении безопасности персональных данных.

## 4. Рекомендации по классификации ИСПДн Учреждений, выбору модели угроз и нарушителя

Классификация ИСПДн Учреждений должна осуществляться непосредственно самими Учреждениями в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" в зависимости от категории и количества обрабатываемых данных.

Классификация ИСПДн производится на основании Отчета о результатах проведения внутренней проверки и оформляется соответствующим Актом классификации информационной системы персональных данных.

Чтобы правильно классифицировать ИС, Учреждения должны следующие действия:

1) Провести сбор и анализ исходных данных по ИС, а именно:

- выделить категорию обрабатываемых в информационной системе персональных данных - Хпд;
- определить объем обрабатываемых персональных данных (количество субъектов персональных данных, чьи персональные данные обрабатываются в информационной системе) - Хнпд;
- выявить характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- определить структуру информационной системы;
- выявить наличие подключений информационной системы к сетям связи общего пользования и/или сетям международного информационного обмена;
- определить режим обработки персональных данных;
- определить режим разграничения прав доступа пользователей информационной системы;
- определить местонахождение технических средств информационной системы.

Далее, на основе исходных данных необходимо вычислить следующие категории (Хпд):

| Хнпд\Хпд | 3 | 2 | 1 |
|---|---|---|---|
| категория 4 | К4 | К4 | К4 |
| категория 3 | К3 | К3 | К2 |
| категория 2 | К3 | К2 | К1 |
| категория 1 | К1 | К1 | К1 |

Все ИСПДн подразделяются на типовые и специальные. К типовым системам относятся системы, в которых требуется обеспечить только свойство конфиденциальности персональных данных. Все остальные системы относятся к специальным. Например, если в ИСПДн нужно обеспечить целостность ПДн, то такая ИСПДн будет специальной.

Типовым ИСПДн могут быть присвоены следующие классы:

- **класс 1 (К1)** - информационные системы, для которых нарушения могут привести к значительным негативным последствиям для субъектов персональных данных;

- **класс 2 (К2)** - информационные системы, для которых нарушения могут привести к негативным последствиям для субъектов персональных данных;

- **класс 3 (К3)** - информационные системы, для которых нарушения могут привести к незначительным негативным последствиям для субъектов персональных данных;

- **класс 4 (К4)** - информационные системы, для которых нарушения не приводят к негативным последствиям для субъектов персональных данных.

Однако в Учреждениях все ИСПДн будут отнесены к специальным, поскольку обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных, а также потому, что, как правило, помимо конфиденциальности требуется обеспечить свойство целостности ПДн. Класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных по результатам анализа исходных данных.

Вместе с тем, для специальных систем, тем не менее, необходимо вычислять класс К1-К4 так, как если бы эта система была типовая. Классификация специальных систем по аналогии с типовыми нужна для того, чтобы в дальнейшем можно было спроектировать систему защиты ИСПДн учреждения, поскольку в документах ФСТЭК России защита для любых систем строится с учетом их класса и модели угроз.

Модель угроз ИСПДн Учреждения зависит от используемых в учреждении технологических решений (однопользовательский/многопользовательский режим работы, подключение к ЛВС, подключение к сети Интернет, использование технологии удаленного доступа) и от функционального назначения конкретной ИСПДн.

Модель угроз строится на основании Методики составления частной модели угроз. Для каждой ИСПДн нужно составить свою модель угроз.

2) Присвоить информационной системе соответствующий класс и его документально оформить. Результаты классификации информационных систем оформляются соответствующим актом (см. Приложение 9). Для каждой ИСПДн нужно составить свой акт классификации.

3) Для дальнейшего проектирования системы защиты ПДн (далее - СЗПД) необходимо документально оформить частную модель угроз, на основе которой была произведена классификация ИСПДн. Частная модель угроз для специальной ИСПДн не должна содержать угрозы, реализация которых для данной ИСПДн маловероятна. Исключение из модели маловероятных угроз существенно снизит затраты на реализацию механизмов защиты на дальнейших этапах работ.

## 5. Рекомендации по выполнению организационных мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн Учреждений

Данные организационные мероприятия являются обязательными для выполнения всеми Учреждениями, эксплуатирующими ИСПДн, и могут быть выполнены специалистами учреждений без привлечения сторонних организаций и без выделения дополнительного финансирования со стороны Минздравсоцразвития. Для правильного выполнения организационных мероприятий и разработке документов необходимо использовать шаблоны, представленные в Приложении, а также использовать инструкции по их заполнению.

Перечень возможных дополнительных организационных мероприятий представлен в Плане мероприятий по обеспечению защиты ПДн. Дополнительные мероприятия (помимо представленных ниже) должны вводиться приказом по учреждению или в качестве инструкции о соблюдении режима безопасности в порядке, утвержденном в учреждении.

### 5.1. Рекомендации по разработке Положения о защите персональных данных

Положение о защите персональных данных, самый первый и самый важный нормативно-организационный документ. Положение вводится приказом и устанавливает нижестоящие документы по обеспечению режима обработки и защиты ПДн.

Пример приказа о введении Положения о защите персональных данных.

Положение должно:

1) Быть оформлено в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утверждено Руководителем Учреждения.

3) В приказе должен быть указан сотрудник ответственный за контроль исполнения приказа.

Ответственным сотрудником может быть Руководитель Учреждения, лицо, отвечающее за обеспечение режима безопасности, или любой другой сотрудник, на которого возложен контроль за выполнение приказа.

### 5.2. Рекомендации по разработке Положения о подразделении по защите информации

Положение о подразделении по защите информации, определяет лица, ответственные за обеспечение безопасности, а так же организационные и технические мероприятия по достижению безопасности. Положение вводится приказом и устанавливает нижестоящие документы по обеспечению защиты ПДн.

Пример приказа о введении Положения о подразделении по защите информации.

Положение должно:

1) Быть оформлено в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утверждено Руководителем Учреждения.

3) В приказе должно быть указано лицо (сотрудник) или подразделение, ответственное за обеспечение безопасности персональных данных. Если в Учреждении нет отдела или специалиста, занимающегося защитой информации, то его следует назначить из числа доверенных лиц. Ответственным за обеспечение безопасности ПДн может быть назначен руководитель отдела информационных технологий или любой другой сотрудник.

4) В Приказе должен быть установлен срок, до которого необходимо провести внутреннюю проверку. Проверка проводится на основании Приказа о проведении внутренней проверки.

5) В приказе должен быть указан сотрудник ответственный за контроль исполнения приказа.

Ответственным сотрудником может быть Руководитель Учреждения, лицо, отвечающее за обеспечение режима безопасности, или любой другой сотрудник, на

которого возложен контроль за выполнение приказа.

### 5.3. Рекомендации по разработке Приказа о назначении ответственных лиц за обработку ПДн

Приказ о назначении ответственных лиц за обработку ПДн, определяет уровень доступа и ответственность лиц участвующих в обработке ПДн. Положение вводится приказом и устанавливает нижестоящие документы по обеспечению режима обработки ПДн.

Пример Приказа о назначении ответственных лиц за обработку ПДн.

Приказ должен:

1) Быть оформлен в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утвержден Руководителем Учреждения, на основании Отчета о результатах проведения внутренней проверки.

Дата введения приказа, должна быть последующей после проведения внутренней проверки и принятия отчета о проведении внутренней проверки.

3) В приказе должен быть указан сотрудник ответственный за контроль исполнения приказа.

Ответственным сотрудником может быть Руководитель Учреждения, лицо, отвечающее за обеспечение режима безопасности или проведение внутренней проверки, или любой другой сотрудник, на которого возложен контроль за выполнение приказа.

### 5.4. Рекомендации по разработке Концепции информационной безопасности

Концепция информационной безопасности, определяет принципы обеспечения безопасности.

Пример Концепции информационной безопасности.

Концепция должна:

1) Быть оформлена в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утверждена Руководителем Учреждения.

3) При выявлении положений, специфичных для обработки ПДн в конкретном Учреждении, они должны быть добавлены в Концепцию.

### 5.5. Рекомендации по разработке Политики информационной безопасности

Политика информационной безопасности, определяет категории конкретных мероприятий по обеспечению безопасности ПДн.

Пример Политики информационной безопасности.

Политика должна:

1) Быть оформлена в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утверждена Руководителем Учреждения.

3) В соответствующем разделе Политики, должен быть уточнен перечень групп пользователей, обрабатывающих ПДн. Группы пользователей, их права, уровень доступа и информированность должны быть отражены так, как это отражается рабочим

порядком в Учреждении.

### 5.6. Рекомендации по разработке Перечня персональных данных, подлежащих защите

Перечень персональных данных содержит перечисление объектов защиты для каждой ИСПДн.

Пример Перечня персональных данных, подлежащих защите.

Перечень должен:

1) Быть оформлен в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утвержден Руководителем Учреждения на основании Отчета о результатах проведения внутренней проверки.

Дата введения Перечня, должна быть последующей после проведения внутренней проверки и принятия отчета о проведении внутренней проверки.

3) Перечень составляется для каждой выявленной ИСПДн.

4) В пунктах 2.6 ("Каналы информационного обмена и телекоммуникации и далее для всех ИСПДн") и 2.7 ("Объекты и помещения, в которых размещены компоненты ИСПДн") примера Перечня и далее для всех ИСПДн должны быть явно указаны каналы передачи и помещения.

ГАРАНТ:

По-видимому, в тексте предыдущего абзаца допущена опечатка. Имеются в виду пункты 2.5 и 2.6 Приложения 6

5) Состав перечня должен быть уточнен в соответствии с реалиями конкретного Учреждения.

### 5.7. Рекомендации по разработке Приказа о проведении внутренней проверки

Приказ о проведении внутренней проверки определяет положение о проведении внутренней проверки.

Пример Приказа о проведении внутренней проверки.

Приказ должен:

1) Быть оформлен в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утвержден Руководителем Учреждения.

3) В приказе должен быть установлен срок проведения проверки.

4) В приказе должен быть указан состав комиссии по классификации ИСПДн. В состав комиссии рекомендуется включить ответственного за обеспечение безопасности, руководителей отделов, чьи подразделения участвуют в обработке персональных данных, технических специалистов, обеспечивающих поддержку технических средств. Также к участию в комиссии в качестве консультантов можно привлекать специалистов сторонних организаций.

5) В приказе должен быть указан сотрудник ответственный за контроль исполнения приказа.

Ответственным сотрудником может быть Руководитель Учреждения, лицо, отвечающее за обеспечение режима безопасности или проведение внутренней проверки, или любой другой сотрудник, на которого возложен контроль за выполнение

приказа.

### 5.8. Рекомендации по разработке Отчета о результатах проведения внутренней проверки

Отчет о результатах проведения внутренней проверки описывает текущее состояние режимов обработки и защиты ПДн.

Пример Отчета о результатах проведения внутренней проверки.

Отчет должен:

1) Быть утвержден руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником.

2) Отчет составляется на основании приказа о проведении внутренней проверки.

3) В отчете указывается место и адрес Учреждения, где проводится проверка. Если проверка проводится также в филиалах, это тоже должно быть указано.

4) В отчете должны быть перечислены названиях всех выявленных ИСПДн.

5) Для каждой выявленной ИСПДн должен быть выделен раздел в отчете.

6) Для каждой ИСПДн должна быть определена ее структура, для которой определяются ее технические и эксплуатационные характеристики, режимы обработки ПДн и характеристики безопасности (см. раздел 4 на стр. 24).

| | |
|---|---|
| Заданные характеристики безопасности персональных данных | Типовая информационная система/специальная информационная система |
| Структура информационной системы | Автоматизированное рабочее место/Локальная информационная система/Распределенная информационная система |
| Подключение информационной системы к сетям общего пользования и/или сетям международного информационного обмена | Имеется/не имеется |
| Режим обработки персональных данных | Однопользовательская/многопользовательская система |
| Режим разграничения прав доступа пользователей | Система с разграничение# доступа/без разграничения доступа |
| Местонахождение технических средств информационной системы | Все технические средства находятся в пределах Российской Федерации/технические средства частично или целиком находятся за пределами Российской Федерации |
| Дополнительные# информация | К персональным данным предъявляется требование целостности и/или доступности |

Характеристики рекомендуется заполнять следующим образом:

- Все системы Учреждений являются специальными.
- Структура информационной системы может быть представлена как:
- Автоматизированное рабочее место, если вся обработка ПДн производится в рамках одного рабочего места.
- Локальная информационная система, если вся обработка ПДн производится в рамках одной локальной вычислительной сети.
- Распределенная информационная система, если обработка ПДн производится в

рамках комплекса автоматизированных рабочих мест и/или локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа. Т.е. элементы ИСПДн разнесены территориально, например, в ИСПДн включена сеть филиала, и связь между территориально удаленными элементами осуществляется по каналам сетей общего пользования и/или международного обмена.

- Подключение информационной системы к сетям общего пользования и/или сетям международного информационного обмена. Если ИСПДн или ее элементы имеют подключение к сети Интернет или другим сетям, вне зависимости обусловлено ли это служебной необходимостью - ИСПДн имеет подключение.

- Режим обработки персональных данных. Система является однопользовательской, если сотрудник обрабатывающий ПДн совмещает в себе функции администратора (осуществляет настройку и поддержку технических и программных средств) и оператора. Во всех других случаях ИСПДн является многопользовательской.

- Режим разграничения прав доступа пользователей. Если в системе все пользователи (администраторы, операторы, разработчики) обладают одинаковым набором прав доступа или осуществляют вход под единой учетной записью, а вход под другими учетными записями не осуществляется, то ИСПДн не имеет системы разграничения прав доступа. Во всех других случаях ИСПДн имеет систему разграничения прав доступа.

- Местонахождение технических средств информационной системы. Все ИСПДн Учреждений находятся на территории Российской Федерации.

- Дополнительная информация. К ИСПДн Учреждений предъявляются требования целостности. Если также должно обеспечиваться требование доступности, то необходимо внести соответствующие изменения.

7) Для каждой ИСПДн должен быть определен перечень обрабатываемых персональных данных, а также состав объектов защиты. Примерный состав обрабатываемых персональных данных и объектов защиты описан в Перечне персональных данных, подлежащих защите.

8) На основании состава персональных данных должен быть сделан вывод о категории обрабатываемых персональных данных ($X_{ПД}$) (см. раздел 4 на стр. 24).

9) Должен быть определен объем записей персональных данных ($X_{ПДН}$). В ИСПДн объем ПДн может принимать значение:

- 1 - в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

- 2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

- 3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

10) На основании категории персональных данных и их объема, ИСПДн присваивается класс (см. раздел 4 на стр. 24).

11) Для каждой ИСПДн должна быть нарисована конфигурация ИСПДн -

схематичное взаиморасположение элементов системы. Конфигурация может быть нарисована в любом графическом редакторе.

При составлении конфигурации могут использоваться следующие условные обозначения:

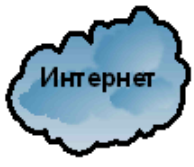
– Группа пользователей ИСПДн.

– АРМ пользователей ИСПДн.

– Сервер, например, почтовый, файловый, proxy сервер, сервер приложений и другие.

– Сервер баз данных.

– Межсетевой экран.



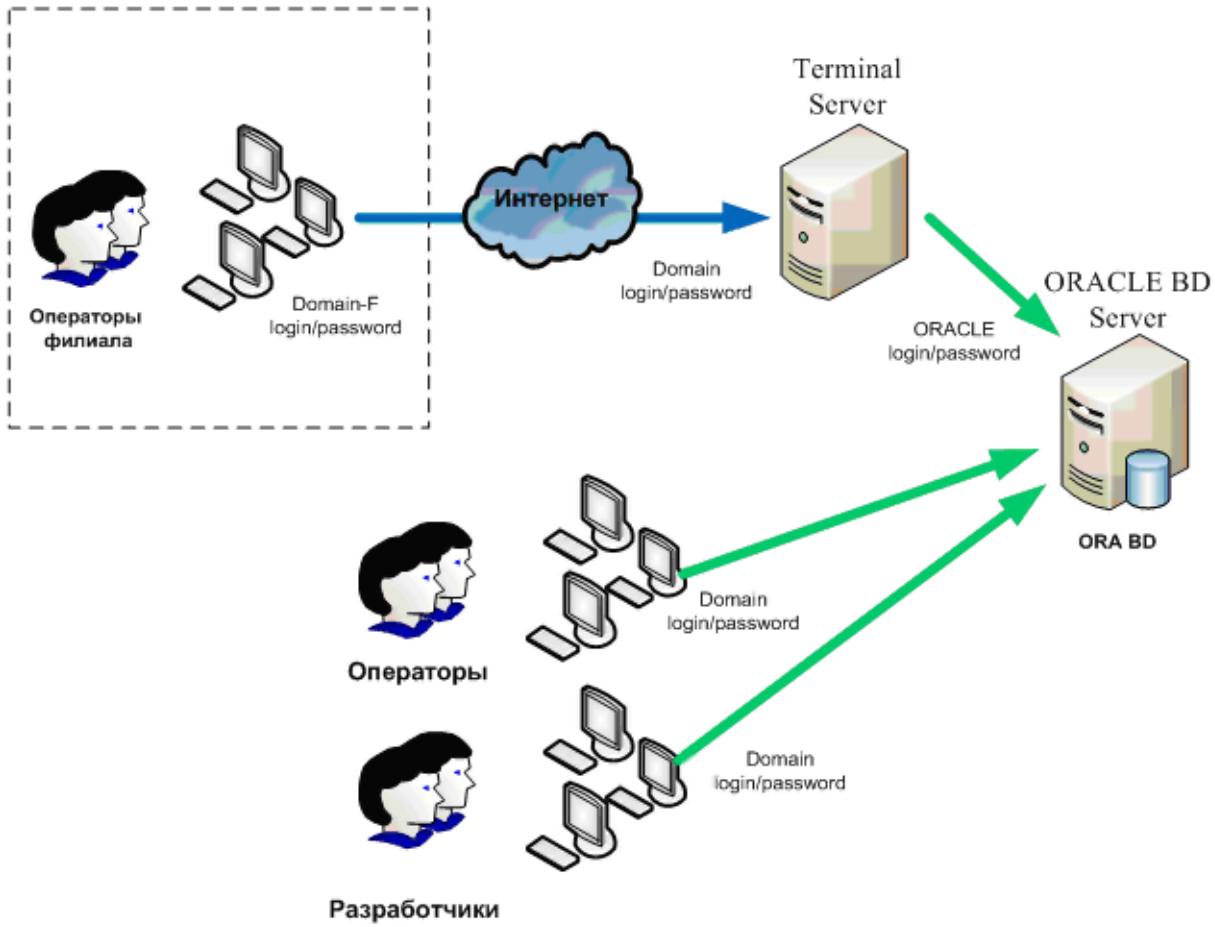

– Сеть общего доступа и / или международного обмена, например, Интернет.

– Направление информационного взаимодействия.

Пример конфигурации ИСПДн приведен на рисунке 1. Здесь показана ИСПДн, основным элементом которой является сервер баз данных ORACLE. К БД ORACLE осуществляют доступ Операторы и Разработчики ИСПДн, авторизуясь под своими

доменными учетными записями в домене Domain.

К БД ORACLE также имеют удаленный доступ Операторы филиала. Удаленный доступ организуется по сети общего пользования и международного обмена - Интернету. Операторы филиала вначале авторизуются в своем домене Domain-F, подключаются по сети Интернет к терминальному серверу Terminal Server, авторизуясь на нем под учетной записью основного домена Domain. Затем Операторы филиала авторизуются в БД ORACLE.



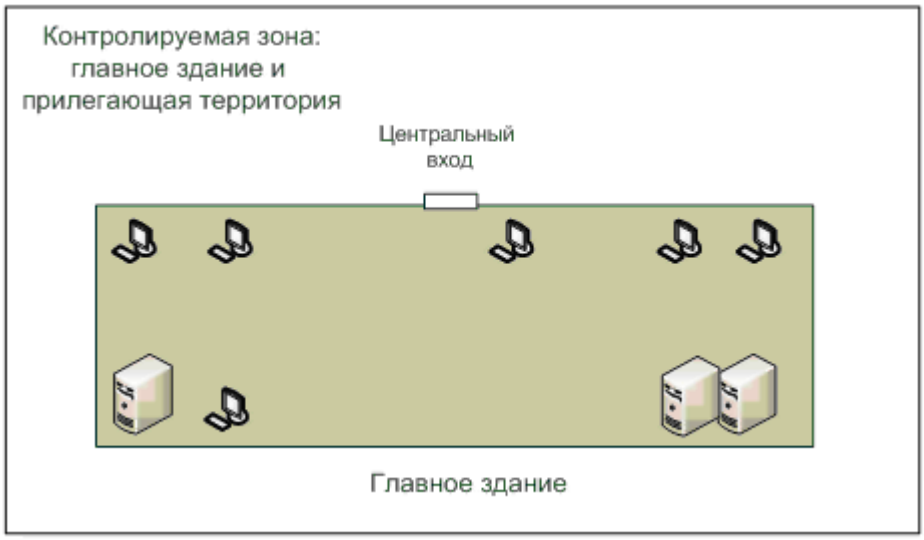

12) Для каждой ИСПДн должно быть нарисовано территориальное расположение ИСПДн относительно контролируемой зоны. Расположение ИСПДн относительно контролируемой зоны может быть нарисовано в любом графическом редакторе.

При составлении конфигурации могут использоваться следующие условные обозначения:

– АРМ пользователей ИСПДн.

– Серверы ИСПДн.

Пример расположение ИСПДн относительно контролируемой зоны приведен на рисунке 2.




13) Для каждой ИСПДн должна быть описана структура обработки ПДн. Структура обработки должна включать всю последовательность шагов по вводу ПДн, их обработке, передаче в другие ИСПДн и другим процессам. Структура обработки ПДн может быть описана как в текстовом, так и в графическом виде.

Пример описания структуры ИСПДн:

1) Сотрудник Регистратуры авторизуется на своем рабочем месте в ОС Windows XP в домене.

2) Сотрудник авторизуется в программе Медиалог.

3) Сотрудник вносит в программу данные из больничной карты пациента.

4) Данные хранятся на сервере MS SQL Server.

14) Для каждой ИСПДн должны быть определены группы пользователей участвующие в обработке ПДн. Список групп берется из Политики информационной безопасности. Для всех групп должен быть определен перечень прав и уровень доступа. Все это необходимо отразить в Матрице доступа.

**Таблица 1** - Пример матрицы доступа

| Группа | Уровень доступа к ПДн | Разрешенные | Сотрудники отдела |
|---|---|---|---|

| | | действия | |
|---|---|---|---|
| Администраторы ИСПДн | Обладают полной информацией о системном и прикладном программном обеспечении ИСПДн.<br><br>Обладают полной информацией о технических средствах и конфигурации ИСПДн.<br><br>Имеют доступ ко всем техническим средствам обработки информации и данным ИСПДн.<br><br>Обладают правами конфигурирования и административной настройки технических средств ИСПДн. | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение | Отдел информационных технологий |
| Администратор безопасности | Обладает правами Администратора ИСПДн.<br><br>Обладает полной информацией об ИСПДн.<br><br>Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.<br><br>Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение | Петров П.П. |
| Операторы ИСПДн с правами записи | Обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение | Отдел регистратуры |

| | | | |
|---|---|---|---|
| | | - использование<br>- уничтожение | |
| Операторы ИСПДн с правами чтения | Обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн. | - использование | Сотрудники call-центра |

15) Для каждой ИСПДн должен быть определен поименный список сотрудников, участвующих в обработке.

16) Для каждой ИСПДн должны быть определены угрозы безопасности персональных данных. Список угроз безопасности определяется на основании Методических рекомендаций по составлению модели угроз, раздел 7.4.

17) Для каждой ИСПДн должны быть определены имеющиеся технические меры защиты. Должны быть описаны все меры защиты как штатного ПО (операционные системы и программы), так и специально установленных систем безопасности (перечень возможных специальных систем безопасности описан в Политике информационной безопасности, раздел 4).

**Таблица 2** - Пример описания технических средств защиты

| Элемент ИСПДн | Программное средство обработки ПДн | Установленные средства защиты |
|---|---|---|
| АРМ пользователя | ОС Windows XP<br><br>Браузер | Средства ОС:<br>- управление и разграничение доступа пользователей;<br>- регистрация и учет действий с информацией.<br><br>Антивирус НАЗВАНИЕ<br>- регистрация и учет действий с информацией;<br>- обеспечение целостности данных;<br>- обнаружение вторжений. |
| АРМ администратора | ОС Windows XP<br><br>Клиент приложения | Средства ОС:<br>- управление и разграничение доступа пользователей;<br>- регистрация и учет действий с информацией.<br><br>Антивирус НАЗВАНИЕ<br>- регистрация и учет действий с информацией;<br>- обеспечение целостности данных;<br>- обнаружение вторжений. |
| Сервер приложений | OS Windows Server 2007 | Средства ОС:<br>- управление и разграничение доступа пользователей; |

| | | |
|---|---|---|
| | | - регистрация и учет действий с информацией;<br>- обеспечение целостности данных.<br><br>Антивирус НАЗВАНИЕ<br>- регистрация и учет действий с информацией;<br>- обеспечение целостности данных;<br>- производить обнаружений# вторжений. |
| СУБД | БД ORACLE | Средства БД<br>Средства ОС:<br>- управление и разграничение доступа пользователей;<br>- регистрация и учет действий с информацией;<br>- обеспечение целостности данных.<br>- обнаружение вторжений. |
| Граница ЛВС | | Межсетевой экран:<br>- управление и разграничение доступа пользователей;<br>- регистрацию и учет действий с информацией;<br>- обеспечение целостности данных.<br>- обнаружение вторжений. |
| Каналы передачи | | СКЗИ НАЗВАНИЕ<br>Средства СКЗИ:<br>- управление и разграничение доступа пользователей;<br>- регистрация и учет действий с информацией;<br>- обеспечение целостности данных. |

18) Для каждой ИСПДн должны быть определены имеющиеся организационные меры защиты. Перечень возможных организационных мер представлен в Плане мероприятий по обеспечению защиты ПДн.

19) Для каждой ИСПДн должны быть определены необходимые меры по снижению опасности актуальных угроз. Анализ актуальности угроз производится на основании Методических рекомендаций по составлению модели угроз, раздел 10.

Перечень возможных организационных мер представлен в Плане мероприятий по обеспечению защиты ПДн.

### 5.9. Рекомендации по разработке Акта классификации информационной системы персональных данных

Акт классификации информационной системы персональных данных, определяет структуру ИСПДн и режим обработки ПДн. Акт классификации составляется для каждой выявленной ИСПДн и прилагается к Уведомлению об обработке.

Пример Акта классификации информационной системы персональных данных.

Акт должен:

1) Утверждаться Председателем комиссии по классификации.

2) Для каждой ИСПДн должна быть определена ее структура, в которой определяются характеристики режима обработки (см. раздел 4 на стр. 24).

| | |
|---|---|
| Категория обрабатываемых персональных данных | X_ПД: 1/2/3/4 |
| Объем обрабатываемых персональных данных | X_ПДН: 1/2/3 |
| Заданные характеристики безопасности персональных данных | Типовая информационная система/специальная информационная система |
| Структура информационной системы | Автоматизированное рабочее место/Локальная информационная система /Распределенная информационная система |
| Подключение информационной системы к сетям общего пользования и/или сетям международного информационного обмена | Имеется/не имеется |
| Режим обработки персональных данных | Однопользовательская/многопользовательская система |
| Режим разграничения прав доступа пользователей | Система с разграничение# доступа/без разграничения доступа |
| Местонахождение технических средств информационной системы | Все технические средства находятся в пределах Российской Федерации/технические средства частично или целиком находятся за пределами Российской Федерации |
| Дополнительные# информация | К персональным данным предъявляется требование целостности и/или доступности |
| Тип информационной системы персональных данных: | Специальная |

Характеристики рекомендуется заполнять следующим образом:

- Категория обрабатываемых персональных данных ($X_{ПД}$). Определяется исходя из особенностей персональных данных, порядок категорирования которых описан в разделе 4.

- Должен быть определен объем записей персональных данных ($X_{ПДН}$). В ИСПДн объем ПДн может принимать значение:

- 1 - в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

- 2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

- 3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов

персональных данных в пределах конкретной организации.

- Структура информационной системы. ИС является:

- Автоматизированным рабочим местом, если вся обработка ПДн производится в рамках одного рабочего места.

- Локальной информационной системой, если вся обработка ПДн производится в рамках одной локальной вычислительной сети.

- Распределенной информационной системой, если обработка ПДн производится в рамках комплекса автоматизированных рабочих мест и/или локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа. Т.е. элементы ИСПДн разнесены территориально, например, в ИСПДн включена сеть филиала, и связь между территориально удаленными элементами осуществляется по каналам сетей общего пользования и/или международного обмена.

- Подключение информационной системы к сетям общего пользования и/или сетям международного информационного обмена. Если ИСПДн или ее элементы имеют подключение к Интернету или другим сетям, вне зависимости обусловлено ли это служебной необходимостью или нет, то ИСПДн имеет подключение.

- Режим обработки персональных данных. Система является однопользовательской, если сотрудник обрабатывающий ПДн совмещает в себе функции администратора (осуществляет настройка# и поддержку технических и программных средств) и оператора. Во всех других случаях ИСПДн является многопользовательской.

- Режим разграничения прав доступа пользователей. Если в системе все пользователи (администраторы, операторы, разработчики) обладают одинаковым набором прав доступа или осуществляют вход под единой учетной записью и вход под другими учетными записями не осуществляется, то ИСПДн не имеет системы разграничения прав доступа. Во всех других случаях ИСПДн имеет систему разграничения прав доступа.

- Местонахождение технических средств информационной системы. Все ИСПДн Учреждений находятся на территории Российской Федерации.

- Дополнительная информация. К ИСПДн Учреждений предъявляются требования целостности. Если также должно обеспечиваться требование доступности, то необходимо внести соответствующие изменения.

- Тип информационной системы персональных данных. Все ИСПДн учреждения являются специальными.

3) На основании полученных данных каждой ИСПДн должен быть присвоен класс.

Пример присвоения класса:

На основании полученных данных и в соответствии с моделью угроз персональных данных (для специальных информационных систем) информационной системе персональных данных "АИС Регистратура" присвоен класс К3.

4) Акт должен быть подписан всеми членами комиссии.

### 5.10. Рекомендации по разработке Положения о разграничении прав доступа к обрабатываемым персональным данным

Положение о разграничении прав доступа к обрабатываемым персональным данным определяет список лиц ответственных за обработку ПДн и уровень их доступа.

Пример Положения о разграничении прав доступа к обрабатываемым персональным данным.

Положение должно:

1) Быть оформлено в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утверждено Руководителем Учреждения, на основании Отчета о результатах проведения внутренней проверки.

Дата введения Положения, должна быть последующей после проведения внутренней проверки и принятия отчета о проведении внутренней проверки.

3) В Приложениях к Положению для каждой ИСПДн должен быть представлен список групп пользователей участвующих в обработке. Список групп пользователей берется из Отчета о результатах проведения внутренней проверки.

4) В Приложениях к Положению для каждой ИСПДн должен быть представлен поименный список сотрудников ответственных за обработку ПДн. Список групп пользователей берется из Отчета о результатах проведения внутренней проверки.

### 5.11. Рекомендации по разработке Модели угроз безопасности персональных данных

Модель угроз безопасности персональных данных определяет перечень актуальных угроз.

Модель угроз разрабатывается на основании Методики составления модели угроз.

Пример Модели угроз безопасности персональных данных.

Модель угроз должна:

1) Быть утверждена Руководителем Учреждения, на основании Отчета о результатах проведения внутренней проверки.

Дата принятия Модели угроз, должна быть последующей после проведения внутренней проверки и принятия отчета о проведении внутренней проверки.

2) Быть составлена в соответствии с Методикой составления ЧМУ в учреждениях Минздравсоцразвития.

3) В Модели должны быть перечислены названиях всех выявленных ИСПДн.

4) Для каждой выявленной ИСПДн должен быть выделен раздел в Модели.

5) Для каждой ИСПДн должна быть определена ее структура, в которой определяются характеристики режима обработки (см. раздел 4).

| | |
|---|---|
| Заданные характеристики безопасности персональных данных | Типовая информационная система/специальная информационная система |
| Структура информационной системы | Автоматизированное рабочее место/Локальная информационная система/Распределенная информационная система |
| Подключение информационной системы к сетям общего пользования и/или сетям международного информационного обмена | Имеется/не имеется |
| Режим обработки персональных данных | Однопользовательская/многопользовательская система |
| Режим разграничения прав доступа пользователей | Система с разграничением доступа/без разграничения доступа |
| Местонахождение технических | Все технические средства находятся в |

| | |
|---|---|
| средств информационной системы | пределах Российской Федерации/технические средства частично или целиком находятся за пределами Российской Федерации |
| Дополнительные информация | К персональным данным предъявляется требование целостности и/или доступности |

Характеристики рекомендуется заполнять следующим образом:

- Все системы Учреждений являются специальными.
- Структура информационной системы может быть представлена как:
- Автоматизированное рабочее место, если вся обработка ПДн производится в рамках одного рабочего места.
- Локальная информационная система, если вся обработка ПДн производится в рамках одной локальной вычислительной сети.
- Распределенная информационная система, если обработка ПДн производится в рамках комплекса автоматизированных рабочих мест и/или локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа. Т.е. элементы ИСПДн разнесены территориально, например, в ИСПДн включена сеть филиала, и связь между территориально удаленными элементами осуществляется по каналам сетей общего пользования и/или международного обмена.
- Подключение информационной системы к сетям общего пользования и/или сетям международного информационного обмена. Если ИСПДн или ее элементы имеют подключение к Интернету или другим сетям, вне зависимости обусловлено ли это служебной необходимостью или нет, то ИСПДн имеет подключение.
- Режим обработки персональных данных. Система является однопользовательской, если сотрудник обрабатывающий ПДн совмещает в себе функции администратора (осуществляет настройка# и поддержку технических и программных средств) и оператора. Во всех других случаях ИСПДн является многопользовательской.
- Режим разграничения прав доступа пользователей. Если в системе все пользователи (администраторы, операторы, разработчики) обладают одинаковым набором прав доступа или осуществляют вход под единой учетной записью и вход под другими учетными записями не осуществляется, то ИСПДн не имеет системы разграничения прав доступа. Во всех других случаях ИСПДн имеет систему разграничения прав доступа.
- Местонахождение технических средств информационной системы. Все ИСПДн Учреждений находятся на территории Российской Федерации.
- Дополнительная информация. К ИСПДн Учреждений предъявляются требования целостности. Если также должно обеспечиваться требование доступности, то необходимо внести соответствующие изменения.

6) Для каждой ИСПДн должен быть определен перечень обрабатываемых персональных данных, а так же состав объектов защиты. Примерный состав обрабатываемых персональных данных и объектов защиты описан в Перечне персональных данных, подлежащих защите.

7) На основании состава персональных данных должен быть сделан вывод о категории обрабатываемых персональных данных ($X_{ПД}$) (см. раздел 4).

8) Должно быть определен объем записей персональных данных ($X_{ПДН}$). В ИСПДн объем ПДн может принимать значение:

- 1 - в информационной системе одновременно обрабатываются персональные

данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

- 2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

- 3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

9) Для каждой ИСПДн должна быть нарисована конфигурация ИСПДн - схематичное взаиморасположение элементов системы. Конфигурация может быть нарисована в любом графическом редакторе.

При составлении конфигурации могут использоваться следующие условные обозначения:

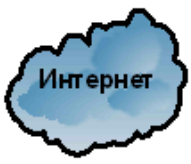
– Группа пользователей ИСПДн.

– АРМ пользователей ИСПДн.

– Сервер, например, почтовый, файловый, proxy сервер, сервер приложений и другие.

– Сервер баз данных.

– Межсетевой экран.




– Сеть общего доступа и/или международного обмена, например, Интернет.

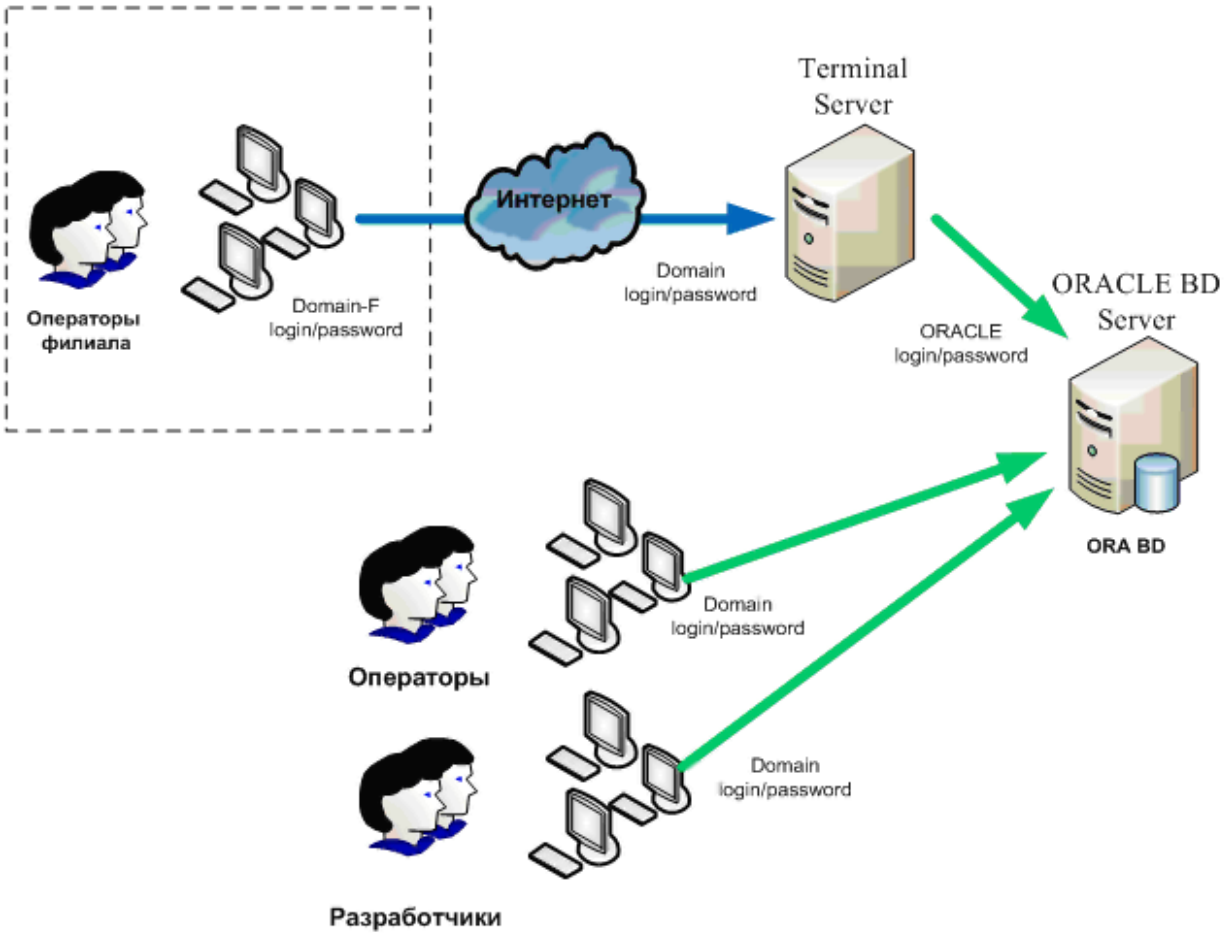
– Направление информационного взаимодействия.

Пример конфигурации ИСПДн приведен на рисунке 1. Здесь показана ИСПДн, основным элементом которой является сервер баз данных ORACLE. К БД ORACLE осуществляют доступ Операторы и Разработчики ИСПДн, авторизуясь под своими

доменными учетными записями в домене Domain.

К БД ORACLE так же имеют удаленный доступ Операторы филиала. Удаленный доступ организуется по сети общего пользования и международного обмена - Интернету. Операторы филиала вначале авторизуются в своем домене Domain-F, подключаются через Интернет к терминальному серверу Terminal Server, авторизуясь на нем под учетной записью основного домена Domain. Затем Операторы филиала авторизуются в БД ORACLE.

Пример конфигурации ИСПДн приведен на рисунке 3.



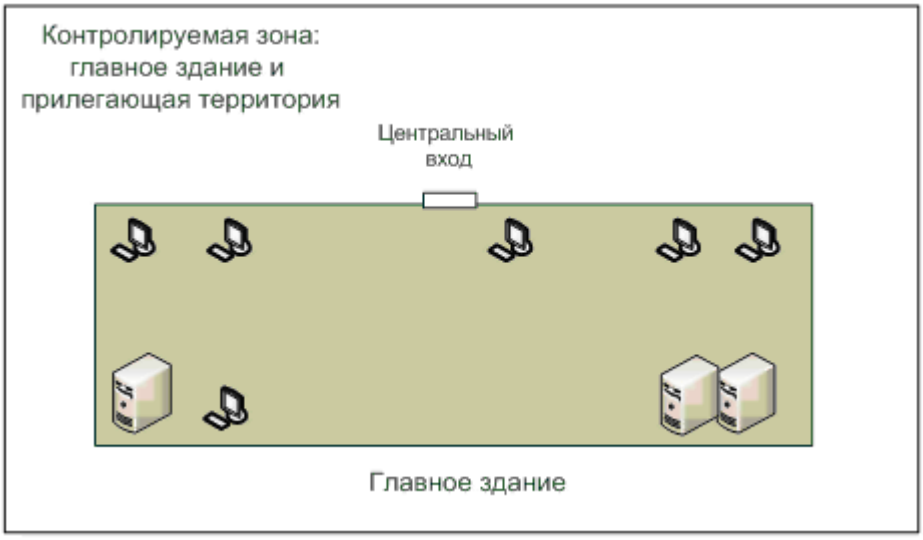

10) Для каждой ИСПДн должно быть нарисовано территориальное расположение ИСПДн относительно контролируемой зоны. Расположение ИСПДн относительно контролируемой зоны может быть нарисовано в любом графическом редакторе.

При составлении конфигурации могут использоваться следующие условные обозначения:

– АРМ пользователей ИСПДн.

– Сервера ИСПДн.

Пример расположение ИСПДн относительно контролируемой зоны приведен на рисунке 4.




11) Для каждой ИСПДн должна быть описана структура обработки ПДн. Структура обработки должна включать всю последовательность шагов по вводу ПДн, их обработке, передаче в другие ИСПДн и другим процессам. Структура обработки ПДн может быть описана как в текстовом, так и в графическом виде.

Пример описания структуры ИСПДн:

1) Сотрудник Регистратуры авторизуется на своем рабочем месте в ОС Windows XP в домене.

2) Сотрудник авторизуется в программе Медиалог.

3) Сотрудник вносит в программу данные из больничной карты пациента.

4) Данные хранятся на сервере MS SQL Server.

12) Для каждой ИСПДн должны быть определены группы пользователей участвующие в обработке ПДн. Список групп берется из Политики информационной безопасности. Для всех групп должен быть определен перечень прав и уровень доступа. Все это необходимо отразить в Матрице доступа.

Пример Матрицы доступа:

| Группа | Уровень доступа к ПДн | Разрешенные | Сотрудники отдела |
|---|---|---|---|

| | | действия | |
|---|---|---|---|
| Администраторы ИСПДн | Обладают полной информацией о системном и прикладном программном обеспечении ИСПДн.<br><br>Обладают полной информацией о технических средствах и конфигурации ИСПДн.<br><br>Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.<br><br>Обладают правами конфигурирования и административной настройки технических средств ИСПДн. | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение | Отдел информационных технологий |
| Администратор безопасности | Обладает правами Администратора ИСПДн.<br><br>Обладает полной информацией об ИСПДн.<br><br>Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.<br><br>Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение | Петров П.П. |
| Операторы ИСПДн с правами записи | Обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение | Отдел регистратуры |

| | | | |
|---|---|---|---|
| | | - использование<br>- уничтожение | |
| Операторы ИСПДн с правами чтения | Обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн. | - использование | Сотрудники call-центра |

13) Для каждой ИСПДн должен быть определен поименный список сотрудников, участвующих в обработке.

14) Для каждой ИСПДн должен быть дополнен список внутренних нарушителей (см. раздел 1.6 Модели угроз) в соответствии с уточненным списком групп в Политике информационной безопасности.

15) Для каждой ИСПДн должен быть определен исходный уровень защищенности, по параметрам:

| Позиция | Технические и эксплуатационные характеристики | Уровень защищенности |
|---|---|---|
| 1 | По территориальному размещению | |
| 2 | По наличию соединения с сетями общего пользования | |
| 3 | По встроенным (легальным) операциям с записями баз персональных данных | |
| 4 | По разграничению доступа к персональным данным | |
| 5 | По наличию соединений с другими базами ПДн иных ИСПДн | |
| 6 | По уровню (обезличивания) ПДн | |
| 7 | По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки | |

16) Для каждой ИСПДн должны быть определены вероятности реализации угроз безопасности персональных данных (на основании Методических рекомендаций по составлению модели угроз раздел 8.5).

17) Для каждой ИСПДн должна быть определена реализуемость угроз безопасности персональных данных (на основании Методических рекомендаций по составлению модели угроз раздел 9).

18) Для каждой ИСПДн должна быть определена опасность реализации угроз безопасности персональных данных (на основании Методических рекомендаций по составлению модели угроз раздел 10).

19) Для каждой ИСПДн должна быть определена актуальность угроз безопасности персональных данных (на основании Методических рекомендаций по составлению модели угроз раздел 11).

20) Для каждой ИСПДн должны быть определены необходимые меры по снижению опасности актуальных угроз. Перечень возможных организационных мер представлен в Плане мероприятий по обеспечению защиты ПДн.

21) Для каждой ИСПДн должны быть составлена обобщенная таблица Модели угроз (на основании Методических рекомендаций по составлению модели угроз - Приложения).

22) На основании полученных данных для каждой ИСПДн должно быть сделано заключение о классификации ИСПДн и необходимости аттестации.

Пример Заключения:

В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20, на основании категории и объема обрабатываемых персональных данных - ИСПДн "АИС Регистратура" классифицируется, как специальная ИСПДн класса К3.

Аттестация ИСПДн "АИС Регистратура" не требуется.

### 5.12. Рекомендации по разработке Плана мероприятий по обеспечению защиты ПДн

План мероприятий по обеспечению защиты ПДн определяет перечень мероприятий обеспечения безопасности.

Пример Плана мероприятий по обеспечению защиты ПДн.

План должен:

1) Быть оформлен в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утвержден руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником, на основании Отчета о результатах проведения внутренней проверки.

Дата введения Плана, должна быть последующей после проведения внутренней проверки и принятия отчета о проведении внутренней проверки.

3) В Плане должен быть уточнен список мероприятий по обеспечению безопасности ПДн с учетом уже имеющихся мероприятий. Не обязательно внедрять все мероприятия (особенно в части технических мер, за исключением случаев описанных в разделе 0).

4) Обобщенный список мероприятий содержит:

| Мероприятие | Периодичность | Исполнитель/ Ответственный |
|---|---|---|
| **ИСПДн 1** | | |
| **Организационные мероприятия** | | |
| Первичная внутренняя проверка | Разовое<br>срок до 01.01.2010 г. | |
| Определение перечня ИСПДн | Разовое<br>срок до | |
| Определение обрабатываемых ПДн и объектов защиты | Разовое<br>срок до | |
| Определение круга лиц участвующих в обработке ПДн | Разовое<br>срок до | |
| Определение ответственности лиц участвующих в обработке | Разовое<br>срок до | |
| Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей | Разовое<br>срок до | |
| Назначение ответственного за безопасность ПДн | Разовое<br>срок до | |

| | | |
|---|---|---|
| Введение режима защиты ПДн | Разовое<br>срок до | |
| Утверждение Концепции информационной безопасности | Разовое<br>срок до | |
| Утверждение Политики информационной безопасности | Разовое<br>срок до | |
| Собрание коллегиального органа по классификации ИСПДн | Разовое<br>срок до | |
| Классификация всех выявленных ИСПДн | Разовое<br>срок до | |
| Первичный анализ актуальности УБПДн | Разовое<br>срок до | |
| Установление контролируемой зоны вокруг ИСПДн | Разовое<br>срок до | |
| Выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц, не допущенных к обработке ПДн | Разовое<br>срок до | |
| Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн. | Разовое<br>срок до | |
| Организация порядка резервного копирования защищаемой информации на твердые носители | Разовое<br>срок до | |
| Организация порядка восстановления работоспособности технических средств, ПО, баз данных с подсистем СЗПДн | Разовое<br>срок до | |
| Введение в действие инструкции по порядку формирования, распределения и применения паролей | Разовое<br>срок до | |
| Организация информирования и обучения сотрудников о порядке обработки ПДн | Разовое<br>срок до | |
| Организация информирования и обучения сотрудников о введенном режиме защиты ПДн | Разовое<br>срок до | |
| Разработка должностных инструкций о порядке обработки ПДн и обеспечении введенного режима защиты | Разовое<br>срок до | |
| Разработка инструкций о порядке работы при подключении к сетям общего пользования и/или международного обмена | Разовое<br>срок до | |
| Разработка инструкций о действии в случае возникновения внештатных ситуаций | Разовое<br>срок до | |
| Разработка положения о внесении изменения в штатное программное обеспечение элементов ИСПДн | Разовое<br>срок до | |
| Разработка положения о порядке внесения изменений в программное обеспечение собственной разработки или штатное ПО, | Разовое<br>срок до | |

| | | |
|---|---|---|
| специально дорабатываемое собственными разработчиками или сторонними организациями.<br>Положение должно включать в себя техническое задание на изменения, технический проект, приемо-сдаточные испытания, акт о введении в эксплуатацию. | | |
| Организация журнала учета обращений субъектов ПДн | Разовое<br>срок до | |
| Организация перечня по учету технических средств и средств защиты, а так же документации к ним | Разовое<br>срок до | |
| **Физические мероприятия** | | |
| Организация постов охраны для пропуска в контролируемую зону | Разовое<br>срок до | |
| Внедрение технической системы контроля доступа в контролируемую зону и помещения (по электронным пропускам, токену, биометрическим данным и т.п.) | Разовое<br>срок до | |
| Внедрение технической системы контроля доступа к элементам ИСПДн (по электронным пропускам, токену, биометрическим данным и т.п.) | Разовое<br>срок до | |
| Внедрение видеонаблюдения | Разовое<br>срок до | |
| Установка дверей на входе в помещения с аппаратными средствами ИСПДн | Разовое<br>срок до | |
| Установка замков на дверях в помещениях с аппаратными средствами ИСПДн | Разовое<br>срок до | |
| Установка жалюзи на окнах | Разовое<br>срок до | |
| Установка решеток на окнах первого и последнего этажа здания | Разовое<br>срок до | |
| Установка системы пожаротушения в помещениях, где расположены элементы ИСПДн | Разовое<br>срок до | |
| Установка систем кондиционирования в помещениях, где расположены аппаратные средства ИСПДн | Разовое<br>срок до | |
| Установка систем бесперебойного питания на ключевые элементы ИСПДн | Разовое<br>срок до | |
| Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн | Разовое<br>срок до | |
| **Технические (аппаратные и программные) мероприятия** | | |
| Внедрение единого хранилища зарегистрированных действий пользователей с ПДн | Разовое<br>срок до | |

| | | |
|---|---|---|
| Внедрение специальной подсистемы управления доступом, регистрации и учета (НАЗВАНИЕ) | Разовое<br>срок до | |
| Внедрение антивирусной защиты (НАЗВАНИЕ) | Разовое<br>срок до | |
| Внедрение межсетевого экранирования (НАЗВАНИЕ) | Разовое<br>срок до | |
| Внедрение подсистемы анализа защищенности (НАЗВАНИЕ) | Разовое<br>срок до | |
| Внедрение подсистемы обнаружения вторжений (НАЗВАНИЕ) | Разовое<br>срок до | |
| Внедрение криптографической защиты (НАЗВАНИЕ) | Разовое<br>срок до | |
| **Контролирующие мероприятия** | | |
| Создание журнала внутренних проверок и поддержание его в актуальном состоянии | Ежемесячно | |
| Контроль над соблюдением режима обработки ПДн | Еженедельно | |
| Контроль над соблюдением режима защиты | Ежедневно | |
| Контроль над выполнением антивирусной защиты | Еженедельно | |
| Контроль за соблюдением режима защиты при подключении к сетям общего пользования и/или международного обмена | Еженедельно | |
| Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн | Ежегодно | |
| Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн | Еженедельно | |
| Контроль за обеспечением резервного копирования | Ежемесячно | |
| Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз | Ежегодно | |
| Поддержание в актуальном состоянии нормативно-организационных документов | Ежемесячно | |
| Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО специально дорабатываемое собственными разработчиками или сторонними организациями. | Ежемесячно | |

5) В случае уточнения мероприятий обеспечения безопасности, вследствие специфики обеспечения безопасности конкретного Учреждения, соответствующие изменения должны быть внесены в План.

### 5.13. Рекомендации по разработке Порядка резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет принципы обеспечения целостности и доступности ПДн.

Пример Порядка резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

Положение должно:

1) Быть оформлено в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утверждено руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником.

3) В Положении должны быть указаны сотрудники, ответственные за реагирование на инциденты безопасности.

Ответственным сотрудником может быть администратор ИСПДн или любой другой сотрудник.

4) В Положении должны быть указаны сотрудники ответственные за контроль обеспечения мероприятий по предотвращению инцидентов безопасности.

Ответственным сотрудником может быть лицо, отвечающее за обеспечение режима безопасности, или любой другой сотрудник.

### 5.14. Рекомендации по разработке Плана внутренних проверок

План внутренних проверок содержит периодичность проведения внутренних проверок.

Пример Плана внутренних проверок.

План должен быть утвержден руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником.

### 5.15. Рекомендации по разработке Журнала по учету мероприятий по контролю состояния защиты ПДн

Журнал по учету мероприятий по контролю состояния защиты ПДн содержит результаты выполненных мероприятий по безопасности.

Пример Журнала по учету мероприятий по контролю состояния защиты ПДн.

Журнал должен:

1) Быть утвержден руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником.

2) В журнале отражается, название мероприятия, дата проведения, исполнитель и результат мероприятия.

Пример заполнения журнала:

| Мероприятие | Дата | Исполнитель | Результат |
|---|---|---|---|
| Проверка осведомленности пользователей о режиме защиты ПДн | 01.01.2010 | Иванов А.А. | |

| | | | |
|---|---|---|---|
| Переход на новую версию СУБД ORACLE | 01.01.2010 | Сидоров С.С. | Установлена СУБД ORACLE версии 10 |
| Плановый аудит информационной безопасности | 01.01.2010 | ЗАО "Практика Безопасности" | Аналитический отчет |
| Установлена система контроля доступа в помещение серверной по электронному пропуску | 01.01.2010 | ЗАО "Ромашка" | |
| Введена охрана контролируемой зоны | 01.01.2010 | ЧОП "Снежинка" | |
| Составлены акты классификации ИСПДн | 01.01.2010 | Иванов А.А. Сидоров С.С. | |
| Проверка антивирусной защиты | 01.01.2010 | Сидоров С.С. | Еженедельная проверка - нарушений не обнаружено |
| Осуществлено плановое резервное копирование обрабатываемых персональных данных | 01.01.2010 | Сидоров С.С. | Носители N 3-5 |

### 5.16. Рекомендации по разработке Журнала учета обращений субъектов ПДн о выполнении их законных прав

Журнал учета обращений субъектов ПДн о выполнении их законных прав, содержит список обращений субъектов ПДн.

Пример Журнала учета обращений субъектов ПДн о выполнении их законных прав.

Журнал должен:

1) Быть утвержден руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником.

2) В Журнале отражается ФИО субъекта, дата обращения и цель обращения.

Пример заполнения журнала:

| N | ФИО | Дата | Цель |
|---|---|---|---|
| | Иванов И.И. | 01.10.2010 | Информирование |
| | Сидоров С.С. | 01.10.2010 | Прекращение обработки |
| | Петров П.П. | 01.10.2010 | Уточнение ПДн |

### 5.17. Рекомендации по разработке Инструкции администратора ИСПДн

Инструкция администратора ИСПДн определяет должностные обязанности администратора ИСПДн.

Пример Инструкции администратора ИСПДн.

Инструкция должна:

1) Быть утверждена Руководителем Учреждения, ответственным за обеспечение безопасности ПДн или руководителем отдела.

2) В Инструкции должно быть указано лицо, которому непосредственно подчиняется Администратор ИСПДн.

3) В случае уточнения обязанностей администратора ИСПДн, вследствие специфических особенностей Учреждения, в Инструкцию должны быть внесены соответствующие изменения.

### 5.18. Рекомендации по разработке Инструкции пользователя ИСПДн

Инструкция пользователя ИСПДн определяет должностные обязанности всех пользователей ИСПДн.

Пример Инструкции пользователя ИСПДн.

Инструкция должна:

1) Быть утверждена Руководителем Учреждения, ответственным за обеспечение безопасности ПДн или руководителем отдела.

2) В случае уточнения обязанностей пользователя ИСПДн, вследствие специфических особенностей Учреждения, в Инструкцию должны быть внесены соответствующие изменения.

### 5.19. Рекомендации по разработке Инструкции администратора безопасности ИСПДн

Инструкция администратора безопасности ИСПДн определяет должностные обязанности администратора безопасности ИСПДн.

Пример Инструкции администратора безопасности ИСПДн.

Инструкция должна:

1) Быть утверждена руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником.

2) В Инструкции должно быть прописано лицо, которому непосредственно подчиняется Администратор Безопасности ИСПДн.

3) В случае уточнения обязанностей Администратора безопасности ИСПДн, вследствие специфических особенностей Учреждения, в Инструкцию должны быть внесены соответствующие изменения.

### 5.20. Рекомендации по разработке Инструкции пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций

Инструкция пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций определяет порядок действий в случае возникновения внештатных ситуаций.

Пример Инструкции пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций.

Инструкция должна:

1) Инструкция утверждается Руководителем Учреждения, ответственным за обеспечение безопасности ПДн или руководителем отдела.

2) В случае уточнения мер по ликвидации внештатных ситуаций, вследствие специфических особенностей Учреждения, в Инструкцию должны быть внесены соответствующие изменения.

### 5.21. Рекомендации по разработке Перечня по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним

Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним содержит перечень настроек средств защиты и документации к ним.

Пример Перечня по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним.

Перечень должен:

1) Быть утвержден руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником.

2) Перечень заполняется для каждой выявленной ИСПДн.

3) В Перечне содержится описание настроек технических средств защиты и документации к ним. Описание настроек технических средств выполняется в соответствие с общим (Политика информационной безопасности раздел 4) или уточненным списком (Политика информационной безопасности - Приложение) характеристик.

Пример заполнения Перечня:

| Техническое средство | Эксплуатационная информация | Техническая документация |
|---|---|---|
| Антивирус<br>НАЗВАНИЕ<br><br>версия | Антивирус настроен на:<br>- резидентный антивирусный мониторинг;<br>- ежедневное антивирусное сканирование;<br>- скрипт-блокирование;<br>- автоматизированное обновление антивирусных баз с периодичностью _____.<br>- ...<br>- ...<br>- ...<br><br>Ключи и атрибуты доступа хранятся у _____ в _____ (сейф, криптографически защищенный носитель и т.п.) | Журнал настроек Межсетевого экрана хранится у _____ |
| Межсетевой экран<br>НАЗВАНИЕ<br><br>версия | Межсетевой экран настроен на:<br>- фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;<br>- регистрацию и учет запрашиваемых сервисов прикладного уровня:<br>-<br>-<br>-<br>-<br>- блокирования доступа | Инструкция по установке и настройке от производителя.<br><br>Журнал настроек Межсетевого экрана хранится у _____ |

| | | |
|---|---|---|
| | неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату. Ключи и атрибуты доступа хранятся у _____ в _____ (сейф, криптографически защищенный носитель и т.п.) | |

4) В перечне можно отражать ключи и атрибуты доступа к техническим средствам ИСПДн. В таком случае доступ к Перечню должен быть ограничен, а сам перечень защищен физическими (хранение в сейфе) и/или техническими (шифрование) средствами.

### 5.22. Рекомендации по разработке Технического задания на разработку системы обеспечения безопасности информации объекта вычислительной техники учреждения

Техническое задание на разработку системы обеспечения безопасности информации объекта вычислительной техники учреждения определяет требования к системе защиты персональных данных.

Пример Технического задания на разработку системы обеспечения безопасности информации объекта вычислительной техники учреждения.

Техническое задание должно:

1) Быть оформлено в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утверждено Руководителем Учреждения или руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником.

3) Техническое задание может быть изменено с учетом специфики конкретного Учреждения.

### 5.23. Рекомендации по разработке Эскизного проекта на создание системы обеспечения безопасности информации объекта

Эскизный проект на создание системы обеспечения безопасности информации объекта определяет принципы построения системы защиты персональных данных.

Пример Эскизного проекта на создание системы обеспечения безопасности информации объекта.

Эскизный проект должен:

1) Быть утвержден Руководителем Учреждения или руководителем подразделения ответственного за обеспечение режима безопасности или специально уполномоченным сотрудником.

2) Эскизный проект может быть изменен с учетом специфики конкретного Учреждения.

### 5.24. Рекомендации по разработке Положения об Электронном журнале обращений пользователей информационной системы к ПДн

Положение об Электронном журнале обращений пользователей информационной системы к ПДн определяет порядок регистрации действий пользователей ИСПДн при обработке ПДн. Положение вводится приказом.

Пример Положения об Электронном журнале обращений пользователей информационной системы к ПДн.

Положение должно:

1) Быть оформлено в соответствии с внутренним порядком документооборота Учреждения.

2) Быть утверждено Руководителем Учреждения.

3) Электронный журнал представляет совокупность записей штатных средств обработки ПДн (операционных систем, прикладного ПО) или специально установленных систем управления доступом, регистрации и учета (Политика информационной безопасности раздел 4) о событиях выполняемых пользователями (лог-файлы).

4) Записи о событиях должны храниться в технических средствах или собираться в едином хранилище специально установленных систем управления доступом, регистрации и учета.

5) Записи о событиях должны резервироваться в соответствии с Порядком резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

### 5.25. Рекомендации по разработке уведомления в территориальный орган Россвязькомнадзора

Уведомление в территориальный орган Россвязькомнадзора, является заявкой на получение статуса оператора персональных данных.

Пример Уведомления об обработке.

Уведомление должно быть оформлено в соответствии с рекомендациями Россвязькомнадзора по заполнению Уведомления.

## 6. Рекомендации по выполнению технических мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн Учреждений

Технические мероприятия могут быть разделены на 2 типа:

- Обязательные технические мероприятия.
- Технические мероприятия, выполняемые при выделении дополнительного финансирования.

Перечень возможных дополнительных технических мероприятий представлен в Плане мероприятий по обеспечению защиты ПДн.

### 6.1. Обязательные технические мероприятия

Для всех типов ИСПДн обязательным является установка антивирусной защиты на все элементы ИСПДн (рабочие станции, файловые сервера, сервера приложений).

Для ИСПДн, имеющих информационную структуру локальной или распределенной информационной системы и имеющих подключение к сетям общего пользования и/или международного обмена (Интернету), также необходимым является установка межсетевого экрана на границе сети. Для ИСПДн, имеющих информационную структуру автоматизированного рабочего места, установка межсетевого экрана не обязательна.

Для всех ИСПДн, осуществляющих передачу в другие ИСПДн по сетям общего пользования и/или международного обмена, необходимо установить систему криптозащиты.

### 6.2. Технические мероприятия, выполняемые, при выделении дополнительного финансирования

В соответствии с руководящими документами ФСТЭК России, мероприятия по защите ПДн при их обработке в ИСПДн Учреждений от НСД, включают в себя:

1) Организацию управлением доступом;
2) Организацию защиты от программно математических воздействий (ПМВ)
3) Организацию регистрации и учета;
4) Обеспечение целостности;
5) Контроль отсутствия недекларированных возможностей (НДВ);
6) Антивирусную защиту;
7) Обеспечение безопасного межсетевого взаимодействия ИСПД;
8) Анализ защищенности;
9) Обнаружение вторжений;

Решение о проведении данных технических мероприятий должно приниматься на основании:

- Класса ИСПДн.
- Предписаний Россвязькомнадзора по результата# проверки.
- При наличии дополнительного финансирования.

Прежде чем проводить данные технические мероприятия, проанализируйте Модель угроз безопасности персональных данных. ИСПДн Учреждений имеют мало актуальных угроз безопасности персональных данных. Опасность реализации большинства угроз можно снизить организационными и обязательными техническими мерами (см. п. 6.1).

В случае необходимости внедрения вышеперечисленных технических мер, необходимо:

1) Уточнить у поставщика наличие сертификата ФСТЭК России на устанавливаемое средство.
2) Уточнить у поставщика функционал внедряемого средства в соответствии с Требованиями к СЗПДн, приведенными в таблице 3 применительно к классу ИСПДн.

**Таблица 3** - Требования к системе защиты персональных данных

| N | Требования к системе защиты персональных данных | К3 | К2 | К1 |
|---|---|---|---|---|
| I | В подсистеме управления доступом: | | | |
| 1 | Реализовать идентификацию и проверку подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов; | + | + | + |
| 2 | Реализовать идентификацию терминалов, технических средств обработки ПДн, узлов ИСПДн, компьютеров, каналов связи, внешних устройств ИСПДн по их логическим именам (адресам, номерам); | - | + | + |
| 3 | Реализовать идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам; | - | + | + |
| 4 | Реализовать контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа; | - | + | + |
| 5 | При наличии подключения ИСПДн к сетям общего пользования должно применяться межсетевое экранирование. | Не ниже 5-го уровня защищенности | Не ниже 4-го уровня защищенности | Не ниже 3-го уровня защищенности |
| 6 | Для обеспечения безопасного межсетевого взаимодействия в ИСПДн для разных классов необходимо использовать МЭ | Не ниже 5-го уровня защищенности | Не ниже 4-го уровня защищенности | Не ниже 3-го уровня защищенности |
| II | Средство защиты от программно математических воздействий (ПМВ): | | | |
| 1 | Реализовать идентификацию и аутентификацию субъектов доступа при входе в средство защиты от программно математических воздействий (ПМВ) и перед выполнением ими любых операций по управлению функциями средства защиты от ПМВ по паролю (или с использованием иного механизма аутентификации) условно-постоянного действия длиной не менее шести буквенно-цифровых символов; | + | + | + |
| 2 | Осуществлять контроль любых действий субъектов доступа по управлению функциями средства защиты от | + | + | + |

| | | | | |
|---|---|---|---|---|
| | ПМВ только после проведения его успешной аутентификации; | | | |
| 3 | Предусмотреть механизмы блокирования доступа к средствам защиты от ПМВ при выполнении устанавливаемого числа неудачных попыток ввода пароля; | + | + | + |
| 4 | Необходимо проводить идентификацию файлов, каталогов, программных модулей, внешних устройств, используемых средств защиты от ПМВ; | + | + | + |
| III | В подсистеме регистрации и учета: | | | |
| 1 | Осуществлять регистрацию входа (выхода) субъекта доступа в систему (из системы), либо регистрацию загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы; | + | + | + |
| 2 | Проводить учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку); | + | + | + |
| 3 | Проводить регистрацию входа/выхода субъектов доступа в средство защиты от ПМВ, регистрацию загрузки и инициализации этого средства и ее программного останова. В параметрах регистрации указывается время и дата входа/выхода субъекта доступа в средство защиты от ПМВ или загрузки/останова этого средства, а также идентификатор субъекта доступа, инициировавшего данные действия; | + | + | + |
| 4 | Проводить регистрацию событий проверки и | + | + | + |

| | | | | |
|---|---|---|---|---|
| | обнаружения ПМВ. В параметрах регистрации указываются время и дата проверки или обнаружения ПМВ, идентификатор субъекта доступа, инициировавшего данные действия, характер выполняемых действий по проверке, тип обнаруженной вредоносной программы (ВП), результат действий средства защиты по блокированию ПМВ; | | | |
| 5 | Проводить регистрацию событий по внедрению в средство защиты от ПМВ пакетов обновлений. В параметрах регистрации указываются время и дата обновления, идентификатор субъекта доступа, инициировавшего данное действие версия и контрольная сумма пакета обновления; | + | + | + |
| 6 | Проводить регистрацию событий запуска/завершения работы модулей средства защиты от ПМВ. В параметрах регистрации указываются время и дата запуска/завершения работы, идентификатор модуля, идентификатор субъекта доступа, инициировавшего данное действие, результат запуска/завершения работы; | + | + | + |
| 7 | Должна проводиться регистрация событий управления субъектом доступа функциями средства защиты от ПМВ. В параметрах регистрации указываются время и дата события управления каждой функцией, идентификатор и спецификация функции, идентификатор субъекта доступа, инициировавшего данное действие, результат действия; | + | + | + |
| 8 | Проводить регистрацию событий попыток доступа программных средств к модулям средства защиты от ПМВ или специальным ловушкам. В параметрах регистрации указываются время и дата попытки доступа, идентификатор модуля, идентификатор и спецификация модуля средства защиты от ПМВ (специальной | + | + | + |

| | | | | |
|---|---|---|---|---|
| | ловушки), результат попытки доступа; | | | |
| 9 | Проводить регистрацию событий отката для средства защиты от ПМВ. В параметрах регистрации указываются время и дата события отката, спецификация действий отката, идентификатор субъекта доступа, инициировавшего данное действие, результат действия; | + | + | + |
| 10 | Обеспечить защиту данных регистрации от их уничтожения или модификации нарушителем; | + | + | + |
| 11 | Реализовать механизмы сохранения данных регистрации в случае сокращения отведенных под них ресурсов; | + | + | + |
| 12 | Реализовать механизмы просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров; | + | + | + |
| 13 | Проводить автоматический непрерывный мониторинг событий, которые могут являться причиной реализации ПМВ (создание, редактирование, запись, компиляция объектов, которые могут содержать ВП). | + | + | + |
| 14 | Реализовать механизм автоматического анализа данных регистрации по шаблонам типовых проявлений ПМВ с автоматическим их блокированием и уведомлением администратора безопасности; | + | + | + |
| 15 | Проводить несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации; | + | + | + |
| 16 | Осуществлять регистрацию входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы. | - | + | + |
| 17 | Осуществлять регистрацию выдачи печатных (графических) документов на "твердую" копию. В параметрах регистрации указываются (дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи - логическое имя (номер) внешнего устройства, краткое содержание | - | + | + |

| | | | | |
|---|---|---|---|---|
| | (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ; | | | |
| 18 | Осуществлять регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный - несанкционированный), | - | + | + |
| 19 | Осуществлять регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная - несанкционированная), идентификатор субъекта доступа, спецификация защищаемого файла; | - | + | + |
| 20 | Осуществлять регистрацию попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная - несанкционированная), идентификатор субъекта доступа, спецификация защищаемого объекта - логическое имя (номер); | - | + | + |

| | | | | |
|---|---|---|---|---|
| 21 | Проводить учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку); | - | + | + |
| 22 | Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютеров и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов, информации); | - | + | + |
| IV | В подсистеме обеспечения целостности: | | | |
| 1 | Обеспечить целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ; | + | + | + |
| 2 | Осуществлять физическую охрану ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации; | + | + | + |
| 3 | Проводить периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД; | + | + | + |
| 4 | должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности; | + | + | + |

| | | | | |
|---|---|---|---|---|
| 5 | Проводить проверку целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм; | + | + | + |
| 6 | Обеспечить возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности; | + | + | + |
| 7 | Реализовать механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм; | + | + | + |
| 8 | Проводить резервное копирование ПДн на отчуждаемые носители информации; | - | + | + |
| V | В подсистеме антивирусной защиты: | | | |
| 1 | Проводить автоматическую проверку на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа; | + | + | + |
| 2 | Реализовать механизмы автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения; | + | + | + |
| 3 | Регулярно выполнять (при первом запуске средств защиты ПДн от ПМВ и с устанавливаемой периодичностью) проверка на предмет наличия в них ВП; | + | + | + |
| 4 | Должна инициироваться автоматическая проверка ИСПДн на предмет наличия ВП при выявлении факта ПМВ; | + | + | + |
| 5 | Реализовать механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, | + | + | + |

| | | | | |
|---|---|---|---|---|
| | содержащих ВП. | | | |
| 6 | Дополнительно в ИСПДн должен проводиться непрерывный автоматический мониторинг информационного обмена с внешней сетью с целью выявления ВП. | + | + | + |
| VI | Контроль отсутствия НДВ в ПО СЗИ | | | |
| 1 | Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации - СЗИ, в том числе и встроенных в общесистемное и прикладное программное обеспечение - ПО), должен быть обеспечен соответствующий уровень контроля отсутствия в нем НДВ (не декларированных возможностей). | + | + | + |
| VII | Обнаружение вторжений в ИСПДн | | | |
| | Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ). | + | + | + |
| 1 | Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа | + | - | - |
| 2 | Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа и методы выявления аномалий | - | + | + |
| VIII | Защита ИСПДн от ПЭМИН | | | |
| 1 | Для обработки информации необходимо использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ | + | + | + |

| | | | | |
|---|---|---|---|---|
| | 29216-91, ГОСТ Р 50948-2001, ГОСТ Р 50949-2001, ГОСТ Р 50923 96, СанПиН 2.2.2.542-96). | | | |
| IX | Оценка соответствия ИСПДн требованиям безопасности ПДн | | | |
| 1 | Провести обязательную сертификацию (аттестацию) по требованиям безопасности информации; | - | + | + |
| 2 | Декларировать соответствие или обязательную сертификацию (аттестацию) по требованиям безопасности информации (по решению оператора); | + | - | - |

**Примечание:** Для ИСПДн 4 класса перечень мероприятий по защите ПДн определяется оператором в зависимости от ущерба, который может быть нанесен вследствие несанкционированного или непреднамеренного доступа к ПДн.

## 7. Рекомендации по применению программно-аппаратных средств защиты персональных данных в ИСПДн Учреждений

Все используемые в учреждениях и организациях системы здравоохранения, социальной сферы, труда и занятости России средства защиты информации должны быть сертифицированы в ФСТЭК России и входить в государственный реестр сертифицированных средств защиты информации. Актуальная копия реестра доступна в сети Интернет, по адресу: http://www.fstec.ru/_doc/reestr_sszi/_reestr_sszi.xls

### 7.1. Рекомендации по применению программно-аппаратных средств для подсистемы управления доступом

Подсистема управления доступом не является обязательной для всех типов ИСПДн (см. раздел 6.2). Выбор средств подсистемы управления доступом следует осуществлять на основании наличия сертификата ФСТЭК России.

### 7.2. Рекомендации по применению программно-аппаратных средств для подсистемы защиты от программно математических воздействий (ПМВ)

Подсистема защиты от программно математических воздействий не является обязательной для всех типов ИСПДн (см. раздел 6.2). Выбор средств подсистемы защиты от программно математических воздействий следует осуществлять на основании наличия сертификата ФСТЭК России.

### 7.3. Рекомендации по применению программно-аппаратных средств для подсистемы регистрации и учета

Подсистема регистрации и учета не является обязательной для всех типов ИСПДн (см. раздел 6.2). Выбор средств подсистемы регистрации и учета следует осуществлять на основании наличия сертификата ФСТЭК России.

### 7.4. Рекомендации по применению программно-аппаратных средств для подсистемы обеспечения целостности

Подсистема обеспечения целостности не является обязательной для всех типов ИСПДн (см. раздел 6.2). Выбор средств подсистемы обеспечения целостности следует осуществлять на основании наличия сертификата ФСТЭК России.

### 7.5. Рекомендации по применению программно-аппаратных средств для подсистемы контроля отсутствия недекларированных возможностей (НДВ)

Подсистема контроля отсутствия недекларированных возможностей не является обязательной для всех типов ИСПДн (см. раздел 6.2). Выбор средств подсистемы контроля отсутствия недекларированных возможностей следует осуществлять на основании наличия сертификата ФСТЭК России.

### 7.6. Рекомендации по применению программно-аппаратных средств для подсистемы антивирусной защиты

Подсистема антивирусной защиты является обязательной для всех типов ИСПДн. Выбор средств антивирусной защиты следует осуществлять на основании наличия сертификата ФСТЭК России.

Рекомендуется внедрение одного из следующих средств антивирусной защиты:

- Антивирус Касперского.
- Антивирус Dr. Web.

### 7.7. Рекомендации по применению программно-аппаратных средств для подсистемы обеспечения безопасного межсетевого взаимодействия ИСПДн

Подсистема обеспечения безопасного межсетевого взаимодействия является обязательной для ИСПДн, имеющих информационную структуру локальной или распределенной информационной системы и имеющих подключение к сетям общего пользования и/или международного обмена (Интернету). Для ИСПДн, имеющих информационную структуру автоматизированного рабочего места, установка межсетевого экрана не обязательна.

Выбор средств подсистемы обеспечения безопасного межсетевого взаимодействия следует осуществлять на основании наличия сертификата ФСТЭК России.

Рекомендуется внедрение одного из следующих межсетевых экранов защиты:

- Межсетевой экран ViPNet.
- Межсетевой экран "ЗАСТАВА-S".

### 7.8. Рекомендации по применению программно-аппаратных средств для подсистемы анализа защищенности

Подсистема анализа защищенности не является обязательной для всех типов ИСПДн (см. раздел 6.2). Выбор средств подсистемы анализа защищенности следует осуществлять на основании наличия сертификата ФСТЭК России.

### 7.9. Рекомендации по применению программно-аппаратных средств для подсистемы обнаружения вторжений

Подсистема обнаружения вторжений не является обязательной для всех типов ИСПДн (см. раздел 6.2). Выбор средств подсистемы обнаружения вторжений следует осуществлять на основании наличия сертификата ФСТЭК России.

## 8. Рекомендации по проведению аттестационных испытаний и по декларированию соответствия для ИСПДн Учреждений

После реализации организационно-технических мероприятий по приведению ИСПДн в соответствие с требованиями Закона, учреждения и организации Минздравсоцразвития России должны провести аттестационные испытания (аттестацию проводит контролирующий орган или специально уполномоченный контролирующим органом лицензиат) или составить декларацию соответствия ИСПДн классу.

1) Аттестация ИСПДн обязательна для систем К1, К2. Аттестационные испытания проводятся организациями, имеющими необходимые лицензии ФСТЭК России, и состоят из следующих этапов:

а) Анализ ИСПДн учреждения, изучение вновь принятых решений по обеспечению безопасности информации и включают проверку:

- организационно-технических мероприятий по обеспечению безопасности ПДн;
- защищенности информации от утечек по техническим каналам (ПЭМИН);
- защищенности информации от НСД.

б) По результатам аттестационных испытаний принимается решение о выдаче "Аттестата соответствия" информационной системы заявленному классу по требованиям безопасности информации. Аттестат выдается сроком на 3 года.

2) Декларирование соответствия - это подтверждение соответствия характеристик ИСПДн предъявляемым к ней требованиям, установленным законодательством Российской Федерации, руководящими и нормативно-методическими документами ФСТЭК России и ФСБ России. Декларирование соответствия может осуществляться на основе собственных доказательств учреждения или на основании доказательств, полученных с участием привлеченных организаций, имеющих необходимые лицензии.

В случае проведения декларирования на основе собственных доказательств Учреждение самостоятельно формирует комплект документов, таких как техническая документация, другие документы и результаты собственных исследований, послужившие мотивированным основанием для подтверждения соответствия информационной системы персональных данных всем необходимым требованиям, предъявляемым к классу К3. Для информационных систем К4 оценка соответствия не регламентируется и осуществляется по решению учреждения.

Декларации о соответствии, полученные на основе собственных доказательств и с участием третьей стороны, имеют одинаковую юридическую силу. Также они имеют действие, аналогичное действию сертификата (аттестата) соответствия, и также действительны на территории всей страны и стран, признающих разрешительные документы системы ГОСТ Р в течение всего срока действия. Инструкция по составлению декларации см. в Приложении.

## Заключение

На основании данных Методических рекомендаций необходимо подготовить необходимый комплект документов (см. Приложение). Документы оформляются в соответствии с положениями раздела 5.

В случае возникновения вопросов по использованию данных методических рекомендаций обращайтесь по телефону Многоканального круглосуточного ежедневного Call-Центр Министерства здравоохранения и социального развития Российской федерации для специалистов учреждений здравоохранения, социальной сферы, труда и занятости по вопросам защиты информации:

8-800-100-3984 (звонок бесплатный).

## 9. Список использованных источников

Разработка Методических рекомендаций была осуществлена в соответствии со следующими нормативными документами:


1. Федеральный закон от 27 июля 2006 года N 152-ФЗ "О персональных данных"
2. Федеральный закон от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
3. Федеральный закон от 19 декабря 2005 года N 160-ФЗ "О ратификации Конвенции Совета Европы О защите физических лиц при автоматической обработке персональных данных"
4. Федеральный закон от 10 января 2002 года N 1-ФЗ "Об электронной цифровой подписи"
5. Указ Президента Российской Федерации от 12 мая 2009 года N 537 "О стратегии национальной безопасности Российской Федерации до 2020 года".
6. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 года N Пр-1895
7. Указ Президента Российской Федерации от 17 марта 2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"
8. Указ Президента Российской Федерации от 6 марта 1997 года N 188 "Об утверждении Перечня сведений конфиденциального характера"
9. Постановление Правительства Российской Федерации от 15 августа 2006 г. N 504 "О лицензировании деятельности по технической защите конфиденциальной информации"
10. Постановление Правительства Российской Федерации от 31 августа 2006 г. N 532 "О лицензировании деятельности по разработке и/или производству средств защиты конфиденциальной информации"
11. Постановление Правительства Российской Федерации от 26 июня 1995 года N 608 "О сертификации средств защиты информации"
12. Постановление Правительства Российской Федерации от 28 февраля 1996 года N 226 "О государственном учете и регистрации баз и банков данных"
13. Постановление Правительства Российской Федерации от 3 ноября 1994 года N 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти"
14. Постановление Правительства Российской Федерации от 17 ноября 2007 года N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"
15. Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.
16. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
17. Руководящий документ. Автоматизированные системы. Защита от

несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

18. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Председателем Гостехкомиссии России 25 июля 1997 г.

19. Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом Гостехкомиссии России от 4 июня 1999 г. N 114

20. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден приказом Гостехкомиссии России от 19 июня 2002 г. N 187 (часть 1, часть 2, часть 3)

21. Порядок проведения классификации информационных систем персональных данных. Утвержден приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20

22. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

23. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены Заместителем директора ФСТЭК России 15 февраля 2008 г.

24. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Утверждены Заместителем директора ФСТЭК России 15 февраля 2008 г.

25. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года N 149/5-144.

ГАРАНТ:

По-видимому, в тексте предыдущего абзаца допущена опечатка. Номер названного руководства следует читать как "149/54-144"

26. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года N 149/6/6-622

**Приложение 1**

## Шаблоны документов и инструкции по их заполнению

Учреждениям Минздравсоцразвития России в обязательном порядке необходимо самостоятельно или с привлечением лицензиатов ФСТЭК России разработать и утвердить следующие внутренние нормативные документы по защите персональных

данных:

1) Положение о защите персональных данных.
2) Положение о подразделении по защите информации.
3) Приказ о назначении ответственных лиц за обработку ПДн.
4) Перечень персональных данных, подлежащих защите.
5) Приказ о проведении внутренней проверки.
6) Отчет о результатах проведения внутренней проверки.
7) Акт классификации информационной системы персональных данных угроз для конкретной ИСПДн.
8) Положение о разграничении прав доступа к обрабатываемым персональным данным.
9) Модель угроз безопасности персональных данных угроз для конкретной ИСПДн.
10) План мероприятий по обеспечению защиты ПДн.
11) Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.
12) Должностные инструкции сотрудников, обрабатывающих ПДн:
- Должностная инструкция администратора ИСПДн.
- Инструкция пользователя ИСПДн.
- Должностная инструкция администратора безопасности ИСПДн.
- Инструкция пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций.
13) План внутренних проверок.
14) Журнал по учету мероприятий по контролю состояния защиты ПДн.
15) Журнал учета обращений субъектов ПДн о выполнении их законных прав.
16) Положение об Электронном журнале обращений пользователей информационной системы к ПДн.
17) Копия уведомления Роскомнадзора с исходящим номером и датой подписания

Для правильного выполнения технических мероприятий желательно иметь следующие документы:

1) Концепция информационной безопасности ИСПДн учреждения.
2) Политика информационной безопасности ИСПДн учреждения.
3) Техническое задание на разработку системы обеспечения безопасности ИСПДн.
4) Эскизный проект на создание системы обеспечения безопасности ИСПДн.

Настоящие методические рекомендации содержат шаблоны перечисленных выше основных требуемых внутренних нормативных документов по защите персональных данных. После учета специфики учреждения эти документы необходимо ввести в действие приказом по учреждению.

Директор Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации — О.В. Симаков

Согласовано
Начальник 2 управления ФСТЭК России — А.В. Куц
"22" декабря 2009 г.

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

# Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости

## Приложение 1

## Положение
## о защите персональных данных в информационных системах персональных данных учреждения здравоохранения, социальной сферы, труда и занятости (проект приказа)

СОГЛАСОВАНО

_____ _____ _____
подпись, дата
_____ _____ _____
подпись, дата
_____ _____ _____
подпись, дата

Москва 2009

**ПРИКАЗ**

"___" _____ 20__ г. г. _____ N_____

О проведении работ по защите персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости

В целях исполнения Федерального закона N 152-ФЗ от 27 июля 2006 года "О персональных данных" в учреждениях здравоохранения, социальной сферы, труда и занятости:

ПРИКАЗЫВАЮ:

1) Ввести в учреждении здравоохранения, социальной сферы, труда и занятости режим обработки персональных данных.

2) Назначить лица ответственные за обработку персональных данных в информационных системах персональных данных, перечисленных в Приказе о назначении ответственных лиц за обработку персональных данных.

3) Организовать доступ ответственных за обработку персональных данных в

информационных системах персональных данных, на основании прав перечисленных в Положении о разграничении прав доступа к обрабатываемым персональным данным.

4) Ввести в учреждении здравоохранения, социальной сферы, труда и занятости режим защиты персональных данных.

5) Осуществлять режим защиты персональных данных в отношении данных перечисленных в Перечне персональных данных, подлежащих защите.

6) Разработать и внедрить:

а) Журнал учета обращений субъектов ПДн о выполнении их законных прав.

б) Электронный журнал обращений пользователей информационной системы к ПДн.

в) Инструкцию администратора информационных систем персональных данных.

г) Инструкцию пользователя информационных систем персональных данных.

д) Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним.

7) Контроль за исполнением настоящего приказа возложить на _____.

ФИО _____ (_____)
(подпись) (ФИО)

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 2**

**Положение**
**о подразделении по защите персональных данных в информационных системах персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**
**(проект приказа)**

СОГЛАСОВАНО

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

Москва 2009

**ПРИКАЗ**

"___" _____ 20__ г. г. _____ N_____

О проведении работ по защите персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости

В целях исполнения Федерального закона N 152-ФЗ от 27 июля 2006 года "О персональных данных" в учреждениях здравоохранения, социальной сферы, труда и занятости:

ПРИКАЗЫВАЮ:

1) Назначить подразделение _____ ответственным за обеспечение защиты персональных данных, во главе с _____.

2) Осуществлять режим защиты персональных данных на основании принципов и положений:

а) Концепции информационной безопасности.

б) Политики информационной безопасности.

3) Осуществлять режим защиты персональных данных в отношении данных перечисленных в Перечне персональных данных, подлежащих защите.

4) Провести внутреннюю проверку, в срок до _____ г., на предмет:

а) Классификации информационных систем обработки данных.

б) Определения режима обработки персональных данных в информационной системе.

в) Установления круга лиц участвующих в обработке персональных данных.

г) Выявления угроз безопасности персональных данных.

5) Разработать и внедрить:

а) План мероприятий по обеспечению защиты персональных данных.

б) Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним.

в) План внутренних проверок.

г) Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

д) Инструкцию администратора безопасности информационных системах персональных данных.

е) Инструкцию пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций.

6) Контроль за исполнением настоящего приказа возложить на _____.

ФИО _____ (_____)
(подпись) (ФИО)

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ

_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 3**

**Приказ**
**о назначении ответственных за обработку персональных данных в информационных системах персональных данных учреждения здравоохранения, социальной сферы, труда и занятости (проект приказа)**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |

Москва 2009

**ПРИКАЗ**

"___" _____ 20__ г. г. _____ N_____

О проведении работ по защите персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости

В целях исполнения Федерального закона N 152-ФЗ от 27 июля 2006 года "О персональных данных" в учреждениях здравоохранения, социальной сферы, труда и занятости:

ПРИКАЗЫВАЮ:

1) Назначить ответственных за обработку персональных данных в информационных системах персональных данных.
2) Список лиц ответственных за обработку персональных данных должен быть определен на основании Отчета по результатам внутренней проверки.
3) Осуществлять доступ лиц ответственных за обработку персональных данных на основании Положения о разграничении прав доступа к обрабатываемым персональным данным.
4) Разработать и внедрить инструкции пользователей, осуществляющих обработку персональных данных в информационных системах персональных данных.

5) Осуществлять регистрацию обращений субъектов персональных данных в Журнале учета обращений субъектов персональных данных о выполнении их законных прав.

6) Контроль за исполнением настоящего приказа возложить на _____.

ФИО _____ (_____)
(подпись) (ФИО)

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 4**

**Концепция**
**информационной безопасности информационных систем персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

Москва 2009

**Определения**

В настоящем документе используются следующие термины и их определения.

**Автоматизированная система** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** - подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и

информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Биометрические персональные данные** - сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

**Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** - возможность получения информации и ее использования.

**Закладочное устройство** - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных (ИСПДн)** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Информационные технологии** - процессы, методы поиска, сбора, хранения,

обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Источник угрозы безопасности информации** - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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

**Межсетевой экран** - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**Недекларированные возможности** - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу),

обезличивание, блокирование, уничтожение персональных данных.

**Общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор (персональных данных)** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Технические средства информационной системы персональных данных** - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

**Перехват (информации)** - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Политика "чистого стола"** - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

**Пользователь информационной системы персональных данных** - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

**Программное (программно-математическое) воздействие** - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Раскрытие персональных данных** - умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных

данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Ресурс информационной системы** - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Специальные категории персональных данных** - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технический канал утечки информации** - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**Угрозы безопасности персональных данных** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Учреждение** - учреждения здравоохранения, социальной сферы, труда и занятости.

**Уязвимость** - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## Обозначения и сокращения

**АВС** - антивирусные средства
**АРМ** - автоматизированное рабочее место

**ВТСС** - вспомогательные технические средства и системы
**ИСПДн** - информационная система персональных данных
**КЗ** - контролируемая зона
**ЛВС** - локальная вычислительная сеть
**МЭ** - межсетевой экран
**НСД** - несанкционированный доступ
**ОС** - операционная система
**ПДн** - персональные данные
**ПМВ** - программно-математическое воздействие
**ПО** - программное обеспечение
**ПЭМИН** - побочные электромагнитные излучения и наводки
**САЗ** - система анализа защищенности
**СЗИ** - средства защиты информации
**СЗПДн** - система (подсистема) защиты персональных данных
**СОВ** - система обнаружения вторжений
**ТКУИ** - технические каналы утечки информации
**УБПДн** - угрозы безопасности персональных данных

## Введение

Настоящая Концепция информационной безопасности ИСПДн учреждения здравоохранения, социальной сферы, труда и занятости (Далее - Учреждения), разработана Министерством здравоохранения и социального развития РФ, является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности Учреждения.

Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в Учреждениях, при обработке информации вообще, и персональных данных в частности.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) Учреждения. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Учреждений, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и

защиту информации.

Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн Учреждения;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;
- координации деятельности структурных подразделений Учреждения при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн Учреждения.

Область применения Концепции распространяется на все учреждения здравоохранения, социальной сферы, труда и занятости, эксплуатирующие технические и программные средства ИСПДн, в которых осуществляется автоматизированная обработка ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

Правовой базой для разработки настоящей Концепции служат требования действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных (ПДн).

## 1 Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) Учреждения, в соответствии с Перечнем ИСПДн. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Эти меры призваны обеспечить:

- конфиденциальность информации (защита от несанкционированного ознакомления);

- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

- доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

Стадии создания СЗПДн включают:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;

- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;

- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) предусмотренных Политикой информационной безопасности ИСПДн следующих организационно-распорядительных документов:

- План мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн;

- План мероприятий по контролю обеспечения защиты ПДн;

- Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;

- Должностная инструкция администратора ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

- Должностная инструкция администратора безопасности ИСПДн;

- Должностная инструкция пользователя ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

- Инструкция на случай возникновения внештатной ситуации;

- Рекомендации по использованию программных и аппаратных средств защиты информации.

Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн Учреждения.

## 2 Задачи СЗПДн

Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

Для достижения основной цели система безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

а) к информации, циркулирующей в ИСПДн;

б) средствам вычислительной техники ИСПДн;

в) аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

- регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;
- защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;
- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
- своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

## 3 Объекты защиты

### 3.1 Перечень информационных систем

В Учреждении _____ производится обработка персональных данных в информационных система обработки персональных данных (ИСПДн).

Перечень ИСПДн определяется на основании Отчета по результатам внутренней проверки.

### 3.2 Перечень объектов защиты

Объектами защиты являются - информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащие защите, определен в Перечне персональных данных, подлежащих защите в ИСПД.

Объекты защиты включают:

1) Обрабатываемая информация.
2) Технологическая информация.
3) Программно-технические средства обработки.
4) Средства защиты ПДн.
5) Каналы информационного обмена и телекоммуникации.
6) Объекты и помещения, в которых размещены компоненты ИСПДн.

## 4 Классификация пользователей ИСПДн

Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник Учреждения, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

Пользователи ИСПДн делятся на три основные категории:

1) Администратор ИСПДн. Сотрудники Учреждения, которые занимаются настройкой, внедрением и сопровождением системы. Администратор ИСПДн обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

2) Программист-разработчик ИСПДн. Сотрудники Учреждения или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик ИСПДн обладает следующим уровнем доступа:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

3) Оператор ИСПДн. Сотрудники подразделений Учреждения участвующих в процессе эксплуатации ИСПДн. Оператор ИСПДн обладает следующим уровнем доступа:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

Категории пользователей должны быть определены для каждой ИСПДн. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей определенными в Политике информационной безопасности.

Все выявленные группы пользователей отражаются в Отчете по результатам внутренней проверки. На основании Отчета определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Матрице доступа в Положении о разграничении прав доступа к обрабатываемым персональным данным.

## 5 Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности ПДн ИСПДн Учреждения и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;

- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

### 5.1 Законность

Предполагает осуществление защитных мероприятий и разработку СЗПДн Учреждения в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал ПДн ИСПДн Учреждения должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиты ПДн.

### 5.2 Системность

Системный подход к построению СЗПДн Учреждения предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн Учреждения.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

### 5.3 Комплексность

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы

для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

### 5.4 Непрерывность защиты ПДн

Защита ПДн - не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

### 5.5 Своевременность

Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

### 5.6 Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

### 5.7 Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

### 5.8 Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа "все, что не разрешено, запрещено".

Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

### 5.9 Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн Учреждения, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

### 5.10 Гибкость системы защиты ПДн

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

### 5.11 Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

### 5.12 Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат

при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

### 5.13 Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

### 5.14 Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Учреждения.

### 5.15 Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

## 6 Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных.

### 6.1 Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

### 6.2 Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

### 6.3 Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;

- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;

- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне Учреждения в целом;

- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Эти правила определяют:

- какова область применения политики безопасности ПДн;

- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а так же их установить ответственность;

- кто имеет права доступа к ПДн;

- какими мерами и средствами обеспечивается защита ПДн;

- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

- определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;

- определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;

- организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

В организационные меры должны состоять из:

- регламента доступа в помещения ИСПДн;

- порядок допуска сотрудников к использованию ресурсов ИСПДн Учреждения;

- регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;

- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;

- инструкций пользователей ИСПДн (администратора ИСПДн, администратора безопасности, оператора ИСПДн);

- инструкция пользователя при возникновении внештатных ситуаций.

### 6.4 Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи

и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

### 6.5 Аппаратно-программные средства защиты ПДн

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн Учреждения;
- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании принципов (раздел 5) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;
- каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- в ИСПДн Учреждения разработка и отладка программ осуществляется за пределами ИСПДн, на испытательных стендах;
- все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства Учреждения;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).
- специалистами Учреждения осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

## 7 Контроль эффективности системы защиты ИСПДн Учреждения

Контроль эффективности СЗПДн должен осуществляется на периодической

основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

## 8 Сферы ответственности за безопасность ПДн

Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является руководитель Учреждения. Руководитель может делегировать часть полномочий по обеспечению безопасности персональных данных.

Сфера ответственности руководителя включает следующие направления обеспечения безопасности ПДн:

- Планирование и реализация мер по обеспечению безопасности ПДн;
- Анализ угроз безопасности ПДн;
- Разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;
- Контроль защищенности ИТ инфраструктуры Компании от угроз ИБ путем;
- Обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;
- Предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты (раздел 3), с этими организациями должно быть заключено "Соглашение о конфиденциальности", либо "Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн". Подготовка типовых вариантов этих соглашений осуществляется совместно с Юридическим отделом.

## 9 Модель нарушителя безопасности

Под нарушителем в Учреждении понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты (раздел 3).

Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

- внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование

ИСПДн;

- внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Классификация нарушителей представлена в Модели угроз безопасности персональных данных каждой ИСПДн.

## 10 Модель угроз безопасности

Для ИСПДн Учреждения выделяются следующие основные категории угроз безопасности персональных данных:

1) Угрозы от утечки по техническим каналам.

2) Угрозы несанкционированного доступа к информации:

- Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.

- Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

- Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

- Угрозы преднамеренных действий внутренних нарушителей.

- Угрозы несанкционированного доступа по каналам связи.

Описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности персональных данных каждой ИСПДн.

## 11 Механизм реализации Концепции

Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;

- постановлений Правительства Российской Федерации;

- руководящих, организационно-распорядительных и методических документов ФСТЭК России;

- потребностей ИСПДн в средствах обеспечения безопасности информации.

## 12 Ожидаемый эффект от реализации Концепции

Реализация Концепции безопасности ПДн в ИСПДн позволит:

- оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

- разработать распорядительные и нормативно-методические документы применительно к ИСПДн;

- провести классификацию и сертификацию ИСПДн;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;
- обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИСПДн и создаст условия для ее дальнейшего совершенствования.

## 13 Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

1. Федеральный закон от 27.07.2006 г. N 152-ФЗ "О персональных данных" (далее - ФЗ "О персональных данных"), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
2. "Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденное Постановлением Правительства РФ от 17.11.2007 г. N 781.
3. "Порядок проведения классификации информационных систем персональных данных", утвержденный совместным Приказом ФСТЭК России N 55, ФСБ России N 86 и Мининформсвязи РФ N 20 от 13.02.2008 г.
4. "Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", утвержденное Постановлением Правительства РФ от 15.09.2008 г. N 687.
5. "Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных", утвержденные Постановлением Правительства РФ от 06.07.2008 г. N 512.
6. Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:
7. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)
8. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)
9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)
10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 14.02.08 г. (ДСП)

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ

_____

_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 5**

**Политика информационной безопасности информационных систем персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____<br>подпись, дата | _____ |
| _____ | _____<br>подпись, дата | _____ |
| _____ | _____<br>подпись, дата | _____ |

Москва 2009

**Определения**

В настоящем документе используются следующие термины и их определения.

**Автоматизированная система** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** - подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Биометрические персональные данные** - сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

**Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему

распространению и самовоспроизведению.

**Вредоносная программа** - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** - возможность получения информации и ее использования.

**Закладочное устройство** - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных (ИСПДн)** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Источник угрозы безопасности информации** - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

**Конфиденциальность персональных данных** - обязательное для соблюдения

оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

**Межсетевой экран** - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**Недекларированные возможности** - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор (персональных данных)** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Технические средства информационной системы персональных данных** - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические

средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

**Перехват (информации)** - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Политика "чистого стола"** - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

**Пользователь информационной системы персональных данных** - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

**Программное (программно-математическое) воздействие** - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Раскрытие персональных данных** - умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Ресурс информационной системы** - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Специальные категории персональных данных** - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технический канал утечки информации** - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**Угрозы безопасности персональных данных** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Учреждение** - учреждения здравоохранения, социальной сферы, труда и занятости.

**Уязвимость** - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## Обозначения и сокращения

**АВС** - антивирусные средства
**АРМ** - автоматизированное рабочее место
**ВТСС** - вспомогательные технические средства и системы
**ИСПДн** - информационная система персональных данных
**КЗ** - контролируемая зона
**ЛВС** - локальная вычислительная сеть
**МЭ** - межсетевой экран
**НСД** - несанкционированный доступ
**ОС** - операционная система
**ПДн** - персональные данные
**ПМВ** - программно-математическое воздействие
**ПО** - программное обеспечение
**ПЭМИН** - побочные электромагнитные излучения и наводки
**САЗ** - система анализа защищенности
**СЗИ** - средства защиты информации
**СЗПДн** - система (подсистема) защиты персональных данных

**СОВ** - система обнаружения вторжений
**ТКУ И** - технические каналы утечки информации
**УБПДн** - угрозы безопасности персональных данных

## Введение

Настоящая Политика информационной безопасности учреждения (далее - Политика) здравоохранения, социальной сферы, труда и занятости (Далее - Учреждения), разработана Министерством здравоохранения и социального развития РФ, является официальным документом.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности ИСПД Учреждения.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", на основании:

- "Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденных Заместителем директора ФСТЭК России от 15.02.2008 г.,
- "Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. N 149/6/6-662.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Учреждения.

## 1 Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в Перечне персональных данных,

подлежащих защите.

Состав ИСПДн подлежащих защите, представлен в Отчете о результатах проведения внутренней проверки.

Эта Политика информационной безопасности была утверждена руководителем Учреждения _____ и введена в действие приказом N ____ от xx.xx.xxxx.

## 2 Область действия

Требования настоящей Политики распространяются на всех сотрудников Учреждения (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

## 3 Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

- Отчета о результатах проведения внутренней проверки;
- Перечня персональных данных, подлежащих защите;
- Акта классификации информационной системы персональных данных;
- Модели угроз безопасности персональных данных;
- Положения о разграничении прав доступа к обрабатываемым персональным данным;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчета о результатах проведения внутренней проверке, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- Сервера приложений;
- СУБД;
- Граница ЛВС;
- Каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;

- регистрацию и учет действий с информацией;
- обеспечивать целостность данных;
- производить обнаружений вторжений.

Список используемых технических средств отражается в Плане мероприятий по обеспечению защиты персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены руководителем Учреждения или лицом, ответственным за обеспечение защиты ПДн.

## 4 Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:
- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационной системы персональных данных. Список соответствия функций подсистем СЗПДн классу защищенности представлен в Приложении.

### 4.1 Подсистемы управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:
- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

### 4.2 Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Учреждения, а так же средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов ИСПДн.

### 4.3 Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Учреждения.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

### 4.4 Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика по следующим параметрам;
- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
- идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;
- регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
- контроля целостности своей программной и информационной части;
- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- регистрации и учета запрашиваемых сервисов прикладного уровня;
- блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к

перехвату;

- контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.

### 4.5 Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

### 4.6 Подсистема обнаружения вторжений

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

### 4.7 Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Учреждения, при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

## 5 Пользователи ИСПДн

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

В ИСПДн Учреждения можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора ИСПДн;
- Администратора безопасности;
- Оператора АРМ;
- Администратора сети;
- Технического специалиста по обслуживанию периферийного оборудования;
- Программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положение о разграничении прав доступа к обрабатываемым персональным данным.

### 5.1 Администратор ИСПДн

Администратор ИСПДн, сотрудник Учреждения, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

### 5.2 Администратор безопасности

Администратор безопасности, сотрудник Учреждения, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

### 5.3 Оператор АРМ

Оператор АРМ, сотрудник Учреждения, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

### 5.4 Администратор сети

Администратор сети, сотрудник Учреждения, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

### 5.5 Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию, сотрудник Учреждения, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

### 5.6 Программист-разработчик ИСПДн

Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники Учреждения, так и сотрудники сторонних организаций.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

## 6 Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Учреждения, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник

подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники Учреждения, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники Учреждения должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники Учреждения должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Учреждения, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Учреждения обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники Учреждения должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

## 7 Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций.

## 8 Ответственность сотрудников ИСПДн Учреждения

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ "О персональных данных" лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Учреждения - пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях Учреждения, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Учреждения.

Необходимо внести в Положения о подразделениях Учреждения, осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

## 9 Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

1. Федеральный закон от 27.07.2006 г. N 152-ФЗ "О персональных данных" (далее - ФЗ "О персональных данных"), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
2. "Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденное Постановлением Правительства РФ от 17.11.2007 г. N 781.
3. "Порядок проведения классификации информационных систем персональных данных", утвержденный совместным Приказом ФСТЭК России N 55, ФСБ России N 86 и Мининформсвязи РФ N 20 от 13.02.2008 г.
4. "Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", утвержденное Постановлением Правительства РФ от 15.09.2008 г. N 687.
5. "Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных", утвержденные Постановлением Правительства РФ от

06.07.2008 г. N 512.

6. Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

7. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

8. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

**Приложение 1**

| N | **План-перечень технических мероприятий по обеспечении безопасности ИСПД** | КЗ |
|---|---|---|
| I | В подсистеме управления доступом: | |
| 1 | Реализовать идентификацию и проверку подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов; | + |
| 2 | Реализовать идентификацию терминалов, технических средств обработки ПДн, узлов ИСПДн, компьютеров, каналов связи, внешних устройств ИСПДн по их логическим именам (адресам, номерам); | - |
| 3 | Реализовать идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам; | - |
| 4 | Реализовать контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа; | - |
| 5 | при наличии подключения ИСПДн к сетям общего пользования должно применяться межсетевое экранирование. | Не ниже 5-го уровня защищенности |
| 6 | Для обеспечения безопасного межсетевого взаимодействия в ИСПДн для разных классов необходимо использовать МЭ | Не ниже 5-го уровня защищенности |
| II | Средство защиты от программно математических воздействий (ПМВ): | |
| 1 | Реализовать идентификацию и аутентификацию субъектов доступа при входе в средство защиты от программно математических воздействий (ПМВ) и перед выполнением ими любых операций по управлению функциями средства защиты от ПМВ по паролю (или с | + |

| | | |
|---|---|---|
| | использованием иного механизма аутентификации) условно-постоянного действия длиной не менее шести буквенно-цифровых символов; | |
| 2 | Осуществлять контроль любых действий субъектов доступа по управлению функциями средства защиты от ПМВ только после проведения его успешной аутентификации; | + |
| 3 | Предусмотреть механизмы блокирования доступа к средствам защиты от ПМВ при выполнении устанавливаемого числа неудачных попыток ввода пароля; | + |
| 4 | Необходимо проводить идентификацию файлов, каталогов, программных модулей, внешних устройств, используемых средств защиты от ПМВ; | + |
| III | В подсистеме регистрации и учета: | |
| 1 | Осуществлять регистрацию входа (выхода) субъекта доступа в систему (из системы), либо регистрацию загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы; | + |
| 2 | Проводить учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку); | + |
| 3 | Проводить регистрацию входа/выхода субъектов доступа в средство защиты от ПМВ, регистрацию загрузки и инициализации этого средства и ее программного останова. В параметрах регистрации указывается время и дата входа/выхода субъекта доступа в средство защиты от ПМВ или загрузки/останова этого средства, а также идентификатор субъекта доступа, инициировавшего данные действия; | + |
| 4 | Проводить регистрацию событий проверки и обнаружения ПМВ. В параметрах регистрации указываются время и дата проверки или обнаружения ПМВ, идентификатор субъекта доступа, инициировавшего данные действия, характер выполняемых действий по проверке, тип обнаруженной вредоносной программы (ВП), результат действий средства защиты по блокированию ПМВ; | + |
| 5 | Проводить регистрацию событий по внедрению в средство защиты от ПМВ пакетов обновлений. В параметрах регистрации указываются время и дата обновления, идентификатор субъекта доступа, инициировавшего данное действие версия и контрольная сумма пакета обновления; | + |
| 6 | Проводить регистрацию событий запуска/завершения работы модулей средства защиты от ПМВ. В параметрах регистрации указываются время и дата запуска/завершения работы, идентификатор модуля, идентификатор субъекта доступа, инициировавшего данное действие, результат запуска/завершения работы; | + |
| 7 | должна проводиться регистрация событий управления субъектом доступа функциями средства защиты от ПМВ. В параметрах регистрации указываются время и дата события управления каждой | + |

| | | |
|---|---|---|
| | функцией, идентификатор и спецификация функции, идентификатор субъекта доступа, инициировавшего данное действие, результат действия; | |
| 8 | Проводить регистрацию событий попыток доступа программных средств к модулям средства защиты от ПМВ или специальным ловушкам. В параметрах регистрации указываются время и дата попытки доступа, идентификатор модуля, идентификатор и спецификация модуля средства защиты от ПМВ (специальной ловушки), результат попытки доступа; | + |
| 9 | Проводить регистрацию событий отката для средства защиты от ПМВ. В параметрах регистрации указываются время и дата события отката, спецификация действий отката, идентификатор субъекта доступа, инициировавшего данное действие, результат действия; | + |
| 10 | Обеспечить защиту данных регистрации от их уничтожения или модификации нарушителем; | + |
| 11 | Реализовать механизмы сохранения данных регистрации в случае сокращения отведенных под них ресурсов; | + |
| 12 | Реализовать механизмы просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров; | + |
| 13 | Проводить автоматический непрерывный мониторинг событий, которые могут являться причиной реализации ПМВ (создание, редактирование, запись, компиляция объектов, которые могут содержать ВП). | + |
| 14 | Реализовать механизм автоматического анализа данных регистрации по шаблонам типовых проявлений ПМВ с автоматическим их блокированием и уведомлением администратора безопасности; | + |
| 15 | Проводить несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации; | + |
| 16 | Осуществлять регистрацию входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы. | - |
| 17 | Осуществлять регистрацию выдачи печатных (графических) документов на "твердую" копию. В параметрах регистрации указываются (дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи - логическое имя (номер) внешнего устройства, краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ; | - |
| 18 | Осуществлять регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный - несанкционированный), | - |
| 19 | Осуществлять регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата | - |

| | | |
|---|---|---|
| | (успешная, неуспешная - несанкционированная), идентификатор субъекта доступа, спецификация защищаемого файла; | |
| 20 | Осуществлять регистрацию попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная - несанкционированная), идентификатор субъекта доступа, спецификация защищаемого объекта - логическое имя (номер); | - |
| 21 | Проводить учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку); | - |
| 22 | Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютеров и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов, информации); | - |
| IV | В подсистеме обеспечения целостности: | |
| 1 | Обеспечить целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ; | + |
| 2 | Осуществлять физическую охрану ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации; | + |
| 3 | Проводить периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД; | + |
| 4 | должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности; | + |
| 5 | Проводить проверку целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм; | + |
| 6 | Обеспечить возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности; | + |
| 7 | Реализовать механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм; | + |
| 8 | Проводить резервное копирование ПДн на отчуждаемые носители информации; | - |

| | | |
|---|---|---|
| V | В подсистеме антивирусной защиты: | |
| 1 | Проводить автоматическую проверку на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа; | + |
| 2 | Реализовать механизмы автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения; | + |
| 3 | Регулярно выполнять (при первом запуске средств защиты ПДн от ПМВ и с устанавливаемой периодичностью) проверка на предмет наличия в них ВП; | + |
| 4 | Должна инициироваться автоматическая проверка ИСПДн на предмет наличия ВП при выявлении факта ПМВ; | + |
| 5 | Реализовать механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП. | + |
| 6 | Дополнительно в ИСПДн должен проводиться непрерывный автоматический мониторинг информационного обмена с внешней сетью с целью выявления ВП. | + |
| VI | Контроль отсутствия НДВ в ПО СЗИ | |
| 1 | Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации - СЗИ, в том числе и встроенных в общесистемное и прикладное программное обеспечение - ПО), должен быть обеспечен соответствующий уровень контроля отсутствия в нем НДВ (не декларированных возможностей). | + |
| VII | Обнаружение вторжений в ИСПДн | |
| | Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ). | + |
| 1 | Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа | + |
| 2 | Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа и методы выявления аномалий | - |
| VIII | Защита ИСПДн от ПЭМИН | |
| 1 | Для обработки информации необходимо использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ 29216-91, ГОСТ Р 50948-2001, ГОСТ Р 50949-2001, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96). | + |
| IX | Оценка соответствия ИСПДн требованиям безопасности ПДн | |
| 1 | Провести обязательную сертификацию (аттестацию) по требованиям безопасности информации; | - |

| | | |
|---|---|---|
| 2 | Декларировать соответствие или обязательную сертификацию (аттестацию) по требованиям безопасности информации (по решению оператора); | + |

**Примечание:** Для ИСПДн 4 класса перечень мероприятий по защите ПДн определяется в зависимости от ущерба который может быть нанесен в следствии несанкционированного или непреднамеренного доступа к ПДн.

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 6**

**Перечень**
**персональных данных, подлежащих защите в информационных системах персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |

Москва 2009

## Введение

Настоящий Перечень персональных данных, подлежащих защите в информационных системах персональных данных (ИСПДн) учреждения (далее - Перечень) здравоохранения, социальной сферы, труда и занятости (далее - Учреждения), разработан Министерством здравоохранения и социального развития РФ.

Перечень разработан в соответствии со списком объектов защиты, изложенных в Концепции информационной безопасности ИСПДн Учреждения.

Перечень содержит полный список категорий данных, безопасность которых должна обеспечиваться системой защиты персональных данных (СЗПДн).

## 1 Общие положения

Объектами защиты являются - информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень объектов защиты определен по результатам Отчета о результатах проведения внутренней проверки.

Объекты защиты каждой ИСПДн включают:

1) Обрабатываемая информация:
- персональные данные субъектов ПДн (раздел 2.1.1);
- персональные данные сотрудников (раздел 2.1.2);

2) Технологическая информация (раздел 2.2).

3) Программно-технические средства обработки (раздел 2.3).

4) Средства защиты ПДн (раздел 2.4).

5) Каналы информационного обмена и телекоммуникации (раздел 2.5).

6) Объекты и помещения, в которых размещены компоненты ИСПДн (раздел 2.6).

## 2 ИСПДн _____

### 2.1 Обрабатываемая информация

#### 2.1.1 Перечень персональных данных субъектов ПДн

Персональные данные субъектов ПДн (пациентов) включают:
- ФИО;
- Дата рождения;
- Контактный телефон;
- Адрес прописки;
- Адрес фактического проживания;
- Паспортные данные;
- Данные о состоянии здоровья (история болезни).

#### 2.1.2 Перечень персональных данных сотрудников Учреждения

Персональные данные сотрудников Учреждения включают:
- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Адрес по прописке;
- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- Информация о трудовой деятельности до приема на работу;
- Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
- Адрес проживания (реальный);
- Телефонный номер (домашний, рабочий, мобильный);
- Семейное положение и состав семьи (муж/жена, дети);
- Информация о знании иностранных языков;
- Форма допуска;
- Оклад;

- Данные о трудовом договоре (N трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, N и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- ИНН;
- Данные об аттестации работников;
- Данные о повышении квалификации;
- Данные о наградах, медалях, поощрениях, почетных званиях;
- Информация о приеме на работу, перемещении по должности, увольнении;
- Информация об отпусках;
- Информация о командировках;
- Информация о болезнях;
- Информация о негосударственном пенсионном обеспечении.

### 2.2 Технологическая информация

Технологическая информация, подлежащая защите, включает:
- управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

### 2.3 Программно-технические средства обработки

Программно-технические средства включают в себя:
- общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);
- резервные копии общесистемного программного обеспечения;
- инструментальные средства и утилиты систем управления ресурсами ИСПДн;
- аппаратные средства обработки ПДн (АРМ и сервера);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

### 2.4 Средства защиты ПДн

Средства защиты ПДн состоят из аппаратно-программных средств, включают в себя:

- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

### 2.5 Каналы информационного обмена и телекоммуникации

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

### 2.6 Объекты и помещения, в которых размещены компоненты ИСПДн

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 7**

**Приказ**
**о проведении внутренней проверки информационных систем персональных данных учреждения здравоохранения, социальной сферы, труда и занятости (проект приказа)**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____<br>подпись, дата | _____ |
| _____ | _____<br>подпись, дата | _____ |
| _____ | _____<br>подпись, дата | _____ |

Москва 2009

**ПРИКАЗ**

"___" _____ 20__ г. г. _____ N_____

О проведении работ по защите персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости

В целях исполнения Федерального закона N 152-ФЗ от 27 июля 2006 года "О персональных данных" в учреждениях здравоохранения, социальной сферы, труда и занятости:

ПРИКАЗЫВАЮ:

1) Провести внутреннюю проверку информационных систем персональных данных в срок до _____г.

2) Результаты внутренней проверки отразить в Отчете по результатам проведения внутренней проверки.

В Отчете должны быть отражены:

а) Состав и структура объектов защиты.

б) Конфигурация и структура информационных систем персональных данных.

в) Информация о разграничении прав доступа к обрабатываемым персональным данным.

г) Режим обработки персональных данных.

д) Выявленные угрозы безопасности персональных данных.

е) Перечень мероприятий обеспечивающих защиту персональных данных.

ж) Перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним.

3) Провести классификацию информационных систем персональных данных.

4) В целях проведения классификации информационных систем Учреждения, создать комиссию в составе:

Председатель комиссии

_____ (ФИО) - _____ (должность)

Члены комиссии:

_____ (ФИО) - _____ (должность)

_____ (ФИО) - _____ (должность)

_____ (ФИО) - _____ (должность)

5) Комиссии по классификации информационных систем персональных данных в срок до __._____.20__ г. провести классификацию информационных систем персональных данных, функционирующих в _____, в соответствии с порядком, утвержденным приказом ФСТЭК России, ФСБ России,

Мининформсвязи России от 13 февраля 2008 г. N 55/86/20.

6) Итоги классификации отразить в Акте классификации информационной системы персональных данных.

7) Контроль за исполнением настоящего приказа возложить на _____.

ФИО _____ (_____)
(подпись) (ФИО)

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 8**

**Отчет**
**о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационных системах персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

Москва 2009

**Определения**

В настоящем документе используются следующие термины и их определения.

**Автоматизированная система** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** - подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** - состояние защищенности персональных

данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Биометрические персональные данные** - сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

**Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** - возможность получения информации и ее использования.

**Закладочное устройство** - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных (ИСПДн)** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Источник угрозы безопасности информации** - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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

**Межсетевой экран** - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**Недекларированные возможности** - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение

(обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор (персональных данных)** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Технические средства информационной системы персональных данных** - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

**Перехват (информации)** - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Политика "чистого стола"** - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

**Пользователь информационной системы персональных данных** - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

**Программное (программно-математическое) воздействие** - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Раскрытие персональных данных** - умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** - действия, направленные на

передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Ресурс информационной системы** - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Специальные категории персональных данных** - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технический канал утечки информации** - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**Угрозы безопасности персональных данных** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Учреждение** - учреждения здравоохранения, социальной сферы, труда и занятости.

**Уязвимость** - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## Обозначения и сокращения

**АВС** - антивирусные средства

**АРМ** - автоматизированное рабочее место
**ВТСС** - вспомогательные технические средства и системы
**ИСПДн** - информационная система персональных данных
**КЗ** - контролируемая зона
**ЛВС** - локальная вычислительная сеть
**МЭ** - межсетевой экран
**НСД** - несанкционированный доступ
**ОС** - операционная система
**ПДн** - персональные данные
**ПМВ** - программно-математическое воздействие
**ПО** - программное обеспечение
**ПЭМИН** - побочные электромагнитные излучения и наводки
**САЗ** - система анализа защищенности
**СЗИ** - средства защиты информации
**СЗПДн** - система (подсистема) защиты персональных данных
**СОВ** - система обнаружения вторжений
**ТКУИ** - технические каналы утечки информации
**УБПДн** - угрозы безопасности персональных данных

## Введение

Внутренняя проверка (далее - Проверка) произведена на основании Приказа NN _____
Проверка проводилась (дата) _____ на территории Учреждения _____ по адресу _____
Проверка проводилась в соответствии с принципами и положениями Концепции информационной безопасности и Политики информационной безопасности.
В ходе проверки были выявлены следующие ИСПДн:
1) _____
2) _____
3) _____

В ходе проверки для каждой ИСПДн определялось:
1) Состав и структура объектов защиты.
2) Конфигурация и структура ИСПДн.
3) Режим обработки ПДн.
4) Перечень лиц, участвующих в обработке ПДн.
5) Права доступа лиц, допущенных к обработке ПДн.
6) Угрозы безопасности персональных данных. Оценивалась вероятность их реализации, реализуемость, опасность и актуальность.
7) Существующие меры защиты ПДн.
8) Список необходимых мер защиты ПДн.

Данные Проверки служат информационной основой для других нормативно-организационных документов.
Данные о составе и структуре объектов защиты отражаются в Перечне персональных данных, подлежащих защите.
Данные о составе и структуре обрабатываемых персональных данных, конфигурации ИСПДн и режиме обработке являются основой для составления Акта

классификации информационной системы персональных данных.

Данные о лицах, допущенных к обработке ПДн, и уровне их доступа отражаются в Положении о разграничении прав доступа к обрабатываемым персональным данным.

Данные об угрозах безопасности ПДн служат основной для составления Модели угроз безопасности персональных данных.

Данные о существующих и необходимых мерах защиты ПДн служат основной для составления Плана мероприятий по обеспечению защиты ПДн.

Данные о технических средствах защиты отражаются в Перечне по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним.

# 1 ИСПДн <Название ИСПДн 1>

## 1.1 Структура ИСПДн

**Таблица 1** - Параметры ИСПДн

| | |
|---|---|
| Заданные характеристики безопасности персональных данных | Типовая информационная система/специальная информационная система |
| Структура информационной системы | Автоматизированное рабочее место/Локальная информационная система/Распределенная информационная система |
| Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена | Имеется/не имеется |
| Режим обработки персональных данных | Однопользовательская/многопользовательская система |
| Режим разграничения прав доступа пользователей | Система с разграничение# доступа/без разграничения доступа |
| Местонахождение технических средств информационной системы | Все технические средства находятся в пределах Российской Федерации/технические средства частично или целиком находятся за пределами Российской Федерации |
| Дополнительная информация | К персональным данным предъявляется требование целостности и (или) доступности |

## 1.2 Состав и структура персональных данных

В ИСПДн обрабатываются следующие персональные данные:

1) персональные данные субъектов ПДн (пациентов):

- ФИО;
- Дата рождения;
- Контактный телефон;
- Адрес прописки;
- Адрес фактического проживания;

- Паспортные данные;
- Данные о состоянии здоровья (история болезни).

2) персональные данные сотрудников:

- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Адрес по прописке;
- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- Информация о трудовой деятельности до приема на работу;
- Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
- Адрес проживания (реальный);
- Телефонный номер (домашний, рабочий, мобильный);
- Семейное положение и состав семьи (муж/жена, дети);
- Информация о знании иностранных языков;
- Форма допуска;
- Оклад;
- Данные о трудовом договоре (N трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, N и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- ИНН;
- Данные об аттестации работников;
- Данные о повышении квалификации;
- Данные о наградах, медалях, поощрениях, почетных званиях;
- Информация о приеме на работу, перемещении по должности, увольнении;
- Информация об отпусках;
- Информация о командировках;
- Информация о болезнях;
- Информация о негосударственном пенсионном обеспечении

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к ____ категории персональных данных, т.е. к данным, позволяющим _____.

Объем обрабатываемых персональных данных, не превышает _____ записей о субъектах персональных данных.

В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20, на основании категории и объема обрабатываемых персональных данных - ИСПДн "_____" классифицируется, как _____ ИСПДн класса K_.

Так же в ИСПДн существуют следующие объекты защиты:

1) Технологическая информация:

- управляющая информация (конфигурационные файлы, таблицы

маршрутизации, настройки системы защиты и пр.);

- технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию об информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

2) Программно-технические средства обработки:

- общесистемное и специальное программное обеспечение, участвующее в обработке ПДн (операционные системы, СУБД, клиент-серверные приложения и другие);
- резервные копии общесистемного программного обеспечения;
- инструментальные средства и утилиты систем управления ресурсами ИСПДн;
- аппаратные средства обработки ПДн (АРМ и сервера);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

3) Средства защиты ПДн:

- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

4) Каналы информационного обмена и телекоммуникации.

5) Объекты и помещения, в которых размещены компоненты ИСПДн.

### 1.3 Конфигурация ИСПДн

На рисунке 1 представлена конфигурация элементов ИСПДн.

На рисунке 2 представлено территориальное расположение ИСПДн относительно контролируемой зоны.

### 1.4 Структура обработки ПДн

В ИСПДн _____ обработка персональных данных происходит следующим образом:

1) _____

2) _____
3) _____

### 1.5 Режим обработки ПДн

В ИСПДн _____ обработка персональных данных осуществляется в однопользовательском/многопользовательском режиме с разграничением/без разграничения прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 2 и иллюстрирован на примере таблицы 3.

**Таблица 2** - Матрица доступа

| Группа | Уровень доступа к ПДн | Разрешенные действия | Сотрудники отдела |
|---|---|---|---|
| Администраторы ИСПДн | Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн.<br><br>Обладает полной информацией о технических средствах и конфигурации ИСПДн.<br><br>Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.<br><br>Обладает правами конфигурирования и административной настройки технических средств ИСПДн. | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение | Отдел информационных технологий |
| Администратор безопасности | Обладает правами Администратора ИСПДн.<br><br>Обладает полной информацией об ИСПДн.<br><br>Имеет доступ к средствам защиты | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение | Петров П.П. |

| | | | |
|---|---|---|---|
| | информации и протоколирования и к части ключевых элементов ИСПДн.<br><br>Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). | | |
| Операторы ИСПДн с правами записи | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение | Отдел регистратуры |
| Операторы ИСПДн с правами чтения | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн. | - использование | Сотрудники call-центра |
| | | | |
| | | | |
| | | | |

В ИСПДн осуществляют работу следующие сотрудники:

**Таблица 3** - Перечень сотрудников

| N | Роль | ФИО сотрудника | Подразделение |
|---|---|---|---|
| | Администратор ИСПДн | Иванов И.И. | |
| | Администратор ИСПДн | Петров П.П. | |
| | Оператор | Сидорова А.А. | |
| | | | |
| | | | |
| | | | |
| | | | |

### 1.6 Угрозы безопасности ПДн

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

1) Угрозы от утечки по техническим каналам.

а) Угрозы утечки акустической информации.

б) Угрозы утечки видовой информации.

в) Угрозы утечки информации по каналам ПЭМИН.

2) Угрозы несанкционированного доступа к информации.

а) Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.

1) Кража ПЭВМ;

2) Кража носителей информации;

3) Кража ключей и атрибутов доступа;

4) Кражи, модификации, уничтожения информации;

5) Вывод из строя узлов ПЭВМ, каналов связи;

6) Несанкционированное отключение средств защиты.

б) Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

1) Действия вредоносных программ (вирусов);

2) Недекларированные возможности системного ПО и ПО для обработки персональных данных;

3) Установка ПО не связанного с исполнением служебных обязанностей.

в) Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

1) Утрата ключей и атрибутов доступа;

2) Непреднамеренная модификация (уничтожение) информации сотрудниками;

3) Непреднамеренное отключение средств защиты;

4) Выход из строя аппаратно-программных средств;

5) Сбой системы электроснабжения;

6) Стихийное бедствие.

г) Угрозы преднамеренных действий внутренних нарушителей.

1) Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке;

2) Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке.

д) Угрозы несанкционированного доступа по каналам связи.

1) Угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:

- Перехват за переделами с контролируемой зоны;

- Перехват в пределах контролируемой зоны внешними нарушителями;

- Перехват в пределах контролируемой зоны внутренними нарушителями.

2) Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

3) Угрозы выявления паролей по сети.

4) Угрозы навязывание ложного маршрута сети.

5) Угрозы подмены доверенного объекта в сети.

6) Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.

7) Угрозы типа "Отказ в обслуживании".

8) Угрозы удаленного запуска приложений.

9) Угрозы внедрения по сети вредоносных программ.

Анализ вероятности реализации, реализуемости, опасности и актуальности угроз

представлен в Модели угроз.

### 1.7 Существующие меры защиты

Существующие в ИСПДн технические меры защиты представлены в таблице ниже.

**Таблица 4** - Меры защиты

| Элемент ИСПДн | Программное средство обработки ПДн | Установленные средства защиты |
|---|---|---|
| АРМ пользователя | ОС Windows XP<br><br>Браузер | Средства ОС:<br>- управление и разграничение доступа пользователей;<br>- регистрацию и учет действий с информацией.<br><br>Антивирус НАЗВАНИЕ<br>- регистрацию и учет действий с информацией;<br>- обеспечивать целостность данных;<br>- производить обнаружений# вторжений. |
| АРМ администратора | ОС Windows XP<br><br>Клиент приложения | Средства ОС:<br>- управление и разграничение доступа пользователей;<br>- регистрацию и учет действий с информацией.<br><br>Антивирус НАЗВАНИЕ<br>- регистрацию и учет действий с информацией;<br>- обеспечивать целостность данных;<br>- производить обнаружений# вторжений. |
| Сервер приложений | OS Windows Server 2007 | Средства ОС:<br>- управление и разграничение доступа пользователей;<br>- регистрацию и учет действий с информацией;<br>- обеспечивать целостность данных.<br><br>Антивирус НАЗВАНИЕ<br>- регистрацию и учет действий с информацией;<br>- обеспечивать целостность данных;<br>- производить обнаружений# вторжений. |
| СУБД | БД ORACLE | Средства БД<br>Средства ОС: |

| | | |
|---|---|---|
| | | - управление и разграничение доступа пользователей;<br>- регистрацию и учет действий с информацией;<br>- обеспечивать целостность данных.<br>- производить обнаружений# вторжений. |
| Граница ЛВС | | Межсетевой экран:<br>- управление и разграничение доступа пользователей;<br>- регистрацию и учет действий с информацией;<br>- обеспечивать целостность данных.<br>- производить обнаружений# вторжений. |
| Каналы передачи | | СКЗИ НАЗВАНИЕ<br>Средства СКЗИ:<br>- управление и разграничение доступа пользователей;<br>- регистрацию и учет действий с информацией;<br>- обеспечивать целостность данных. |
| | | |
| | | |
| | | |
| | | |

В ИСПДн введены следующие организационные меры защиты:

- В Учреждении осуществляется контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания
- Ведется учет носителей информации.
- Носители информации хранятся в сейфе.
- В Учреждении существует отдел/ответственный сотрудник за обеспечение безопасности ПДн.
- В учреждение проводятся периодические внутренние проверки режима безопасности ПДн.
- Введена парольная политика, устанавливающая сложность ключей и атрибутов доступа (паролей), а так же их периодическую смену.
- Пользователи осведомлены и проинструктированы о порядке работы и защиты персональных данных.
- Осуществляется резервное копирование защищаемой информации.
- В помещениях, где расположены элементы ИСПДн, установлена пожарная сигнализация.

### 1.8 Необходимые меры защиты

На основании анализа актуальности выявленных угроз безопасности, для достижения требуемого уровня защиты рекомендуется осуществить следующие мероприятия:

1) _____

2) _____
3) _____

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 9**

**Акт**
**классификации информационной системы персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |

Москва 2009

УТВЕРЖДАЮ
Руководитель учреждения
здравоохранения, социальной сферы,
труда и занятости
Фамилия И.О.

**АКТ**
**классификации информационной системы персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**

По результатам проведенного анализа исходных данных информационной системы персональных данных _____ выявлены следующие характеристики:

| | |
|---|---|
| Категория обрабатываемых персональных данных | X_ПД: 1/2/3/4 |

| | |
|---|---|
| Объем обрабатываемых персональных данных | X_ПДН: 1/2/3 |
| Заданные характеристики безопасности персональных данных | Типовая информационная система/специальная информационная система |
| Структура информационной системы | Автоматизированное рабочее место/Локальная информационная система/Распределенная информационная система |
| Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена | Имеется/не имеется |
| Режим обработки персональных данных | Однопользовательская/многопользовательская система |
| Режим разграничения прав доступа пользователей | Система с разграничением доступа/без разграничения доступа |
| Местонахождение технических средств информационной системы | Все технические средства находятся в пределах Российской Федерации/технические средства частично или целиком находятся за пределами Российской Федерации |
| Дополнительная информация | К персональным данным предъявляется требование целостности и (или) доступности |
| Тип информационной системы персональных данных: | Специальная |

На основании полученных данных и в соответствии с моделью угроз персональных данных (для специальных информационных систем) информационной системе персональных данных _____ _____ присвоен класс К1/К2/К3/К4.

Председатель комиссии

_____ (ФИО) - _____ (должность)

Члены комиссии:

_____ (ФИО) - _____ (должность)

_____ (ФИО) - _____ (должность)

_____ (ФИО) - _____ (должность)

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ

_____

_____

"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 10**

**Положение**
**о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |

Москва 2009

**Общие положения**

В данном документе представлен список лиц ответственных за обработку персональных данных в информационных системах персональных данных, а так же их уровень прав доступа к обрабатываемым персональным данным.

Разграничение прав осуществляется на основании Отчета по результатам проведения внутренней проверки, а так же исходя из характера и режима обработки персональных данных в ИСПДн.

Список лиц ответственных за обработку персональных данных в информационных системах персональных данных, а так же их уровень прав доступа для каждой ИСПДн представлен в Приложении NN____.

**Приложение 1**
**ИСПДн _____**

УТВЕРЖДАЮ
Заместитель руководителя учреждения
здравоохранения, социальной сферы,
труда и занятости
_____ (_____)
"_____" _____ 2009 г

**Перечень**
**групп, участвующих в обработке персональных данных в ИСПДн**

| Группа | Уровень доступа к ПДн | Разрешенные действия |
|---|---|---|
| | | |
| | | |
| | | |

| | | |
|---|---|---|
| | | |
| | | |
| | | |

**Перечень лиц, получивших доступ к персональным данным**

| N | Роль | ФИО сотрудника | Подразделение |
|---|---|---|---|
| | Администратор ИСПДн | Иванов И.И. | |
| | Администратор ИСПДн | Петров П.П. | |
| | Оператор | Сидорова А.А. | |
| | | | |
| | | | |
| | | | |
| | | | |

**Приложение 2**
**ИСПДн _____**

УТВЕРЖДАЮ
Заместитель руководителя учреждения
здравоохранения, социальной сферы,
труда и занятости
_____ (_____)
"_____" _____ 2009 г

**Перечень**
**групп, участвующих в обработке персональных данных в ИСПДн**

| Группа | Уровень доступа к ПДн | Разрешенные действия |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

**Перечень лиц, получивших доступ к персональным данным**

| N | Роль | ФИО сотрудника | Подразделение |
|---|---|---|---|
| | Администратор ИСПДн | Иванов И.И. | |
| | Администратор ИСПДн | Петров П.П. | |
| | Оператор | Сидорова А.А. | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ

_____

_____

"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 11**

**Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

_____ _____ _____

подпись, дата

_____ _____ _____

подпись, дата

_____ _____ _____

подпись, дата

Москва 2009

**Определения**

В настоящем документе используются следующие термины и их определения.

**Автоматизированная система** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** - подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Биометрические персональные данные** - сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности

строения тела и другую подобную информацию.

**Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** - возможность получения информации и ее использования.

**Закладочное устройство** - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных (ИСПДн)** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и

свободы субъекта персональных данных или других лиц.

**Источник угрозы безопасности информации** - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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

**Межсетевой экран** - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**Недекларированные возможности** - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор (персональных данных)** - государственный орган, муниципальный

орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Технические средства информационной системы персональных данных** - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

**Перехват (информации)** - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Политика "чистого стола"** - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

**Пользователь информационной системы персональных данных** - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

**Программное (программно-математическое) воздействие** - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Раскрытие персональных данных** - умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Ресурс информационной системы** - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной

системы.

**Специальные категории персональных данных** - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технический канал утечки информации** - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**Угрозы безопасности персональных данных** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Учреждение** - учреждения здравоохранения, социальной сферы, труда и занятости.

**Уязвимость** - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## Обозначения и сокращения

**АВС** - антивирусные средства
**АРМ** - автоматизированное рабочее место
**ВТСС** - вспомогательные технические средства и системы
**ИСПДн** - информационная система персональных данных
**КЗ** - контролируемая зона
**ЛВС** - локальная вычислительная сеть
**МЭ** - межсетевой экран
**НСД** - несанкционированный доступ

**ОС** - операционная система
**ПДн** - персональные данные
**ПМВ** - программно-математическое воздействие
**ПО** - программное обеспечение
**ПЭМИН** - побочные электромагнитные излучения и наводки
**САЗ** - система анализа защищенности
**СЗИ** - средства защиты информации
**СЗПДн** - система (подсистема) защиты персональных данных
**СОВ** - система обнаружения вторжений
**ТКУ И** - технические каналы утечки информации
**УБПДн** - угрозы безопасности персональных данных

## Введение

Модель угроз безопасности персональных данных (далее - Модель) при их обработке в ИСПДн

1) _____
2) _____
3) _____

строится на основании Отчета о результатах проведения внутренней проверки.

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификацию потенциальных нарушителей, оценку исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

- Описание угроз.
- Оценку вероятности возникновения угроз.
- Оценку реализуемости угроз.
- Оценку опасности угроз.
- Определение актуальности угроз.

В заключении даны рекомендации по мерам защиты для уменьшения опасности актуальных угроз.

## 1 ИСПДн <Название ИСПДн>

### 1.1 Структура ИСПДн

**Таблица 1** - Параметры ИСПДн

| | |
|---|---|
| Заданные характеристики безопасности персональных данных | Типовая информационная система/специальная информационная система |
| Структура информационной системы | Автоматизированное рабочее место/ Локальная информационная система/Распределенная информационная система |
| Подключение информационной системы к сетям общего пользования и (или) сетям международного | Имеется/не имеется |

| | |
|---|---|
| информационного обмена | |
| Режим обработки персональных данных | Однопользовательская/многопользовательская система |
| Режим разграничения прав доступа пользователей | Система с разграничением доступа/без разграничения доступа |
| Местонахождение технических средств информационной системы | Все технические средства находятся в пределах Российской Федерации/технические средства частично или целиком находятся за пределами Российской Федерации |
| Дополнительная информация | К персональным данным предъявляется требование целостности и (или) доступности |

### 1.2 Состав и структура персональных данных

В ИСПДн обрабатываются следующие персональные данные:
1) _____
2) _____
3) _____

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к ____ категории персональных данных, т.е. к данным, позволяющим _____.

Объем обрабатываемых персональных данных, не превышает _____ записей о субъектах персональных данных.

### 1.3 Конфигурация ИСПДн

На рисунке 1 представлена конфигурация элементов ИСПДн.

На рисунке 2 представлено территориальное расположение ИСПДн относительно контролируемой зоны.

### 1.4 Структура обработки ПДн

В ИСПДн _____ обработка персональных данных происходит следующим образом:
1) _____
2) _____
3) _____

### 1.5 Режим обработки ПДн

В ИСПДн _____ обработка персональных данных осуществляется в однопользовательском/многопользовательском режиме с разграничением/без разграничения прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание,

блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 2.

**Таблица 2** - Матрица доступа

| Группа | Уровень доступа к ПДн | Разрешенные действия | Сотрудники отдела |
|---|---|---|---|
| Администраторы ИСПДн | Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн.<br><br>Обладает полной информацией о технических средствах и конфигурации ИСПДн.<br><br>Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.<br><br>Обладает правами конфигурирования и административной настройки технических средств ИСПДн. | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение | Отдел информационных технологий |
| Администратор безопасности | Обладает правами Администратора ИСПДн.<br><br>Обладает полной информацией об ИСПДн.<br><br>Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.<br><br>Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). | - сбор<br>- систематизация<br>- накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение | Петров П.П. |
| Операторы ИСПДн с правами | Обладает всеми необходимыми | - сбор<br>- систематизация | Отдел регистратуры |

| | | | |
|---|---|---|---|
| записи | атрибутами и правами, обеспечивающими доступ ко всем ПДн. | - накопление<br>- хранение<br>- уточнение<br>- использование<br>- уничтожение | |
| Операторы ИСПДн с правами чтения | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн. | - использование | Сотрудники call-центра |
| | | | |
| | | | |
| | | | |

### 1.6 Классификация нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

- внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

- внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

#### 1.6.1 Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

#### 1.6.2 Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИСПДн ИСПДн# обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы ИСПДн (категория I);
- администраторы конкретных подсистем или баз данных ИСПДн (категория II);
- пользователи ИСПДн (категория III);
- пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);
- лица, обладающие возможностью доступа к системе передачи данных (категория V);
- сотрудники ЛПУ, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (категория VI);
- обслуживающий персонал ЛПУ (охрана, работники инженерно-технических служб и т.д.) (категория VII);
- уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

### 1.6.3 Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

- общая информация - информации о назначения и общих характеристиках ИСПДн;

- эксплуатационная информация - информация, полученная из эксплуатационной документации;

- чувствительная информация - информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;

- сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

- данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;

- данные о реализованных в ПСЗИ принципах и алгоритмах;

- исходные тексты программного обеспечения ИСПДн;

- сведения о возможных каналах реализации угроз;

- информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в АИС, к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об ИСПДн и функционально ориентированных АИС, включая информацию об уязвимостях технических и программных средств ИСПДн. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об АИС являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в ЛПУ конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая

информация.

### 1.6.4 Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

- аппаратные компоненты СЗПДн и СФ СЗПДн;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах ЛПУ конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

## 1.7 Исходный уровень защищенности ИСПДн

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн ($Y_1$).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн _____.

**Таблица 3** - Исходный уровень защищенности

| Позиция | Технические и эксплуатационные характеристики | Уровень защищенности |
|---|---|---|
| 1 | По территориальному размещению | |
| 2 | По наличию соединения с сетями общего пользования | |
| 3 | По встроенным (легальным) операциям с записями баз персональных данных | |
| 4 | По разграничению доступа к персональным данным | |
| 5 | По наличию соединений с другими базами ПДн иных | |

| | | |
|---|---|---|
| | ИСПДн | |
| 6 | По уровню (обезличивания) ПДн | |
| 7 | По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки | |

### 1.8 Вероятность реализации УБПДн

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент ( $Y_2$ ) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы ($Y_2$ = 0);
- низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2$ = 2);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны ($Y_2$ = 5);
- высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты ($Y_2$ = 10).

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

#### 1.8.1 Угрозы утечки информации по техническим каналам

##### 1.8.1.1 Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В ИСПДн Учреждения функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вероятность реализации угрозы - маловероятна.

##### 1.8.1.2 Угрозы утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

В учреждении введен контроль доступа в контролируемую зону, АРМ

пользователей расположены так, что практически исключен визуальный доступ к мониторам, а на окнах установлены жалюзи.

Вероятность реализации угрозы - маловероятна.

#### 1.8.1.3 Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.

Угрозы данного класса маловероятны, т.к. размер контролируемой зоны большой, и элементы ИСПДн, находятся в самом центре здания и экранируются несколькими несущими стенами, и паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.

### 1.8.2 Угрозы несанкционированного доступа к информации

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование, неправомерное распространение);
- нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).

#### 1.8.2.1 Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн

##### Кража ПЭВМ

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

В учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы - маловероятной.

##### Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, ведется учет и хранение носителей в сейфе.

Вероятность реализации угрозы - маловероятна.

##### Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, организовано хранение ключей в сейфе и введена политика "чистого стола".

Вероятность реализации угрозы - маловероятна.

**Кражи, модификации, уничтожения информации**

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы - маловероятна.

**Вывод из строя узлов ПЭВМ, каналов связи**

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы - маловероятна.

**Несанкционированное отключение средств защиты**

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания, пользователи ИСПДн проинструктированы о работе с ПДн.

Вероятность реализации угрозы - маловероятна.

### 1.8.2.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)

**Действия вредоносных программ (вирусов)**

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу

(набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

В Учреждении на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы - низкая.

**Недекларированные возможности системного ПО и ПО для обработки персональных данных**

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

В Учреждении есть/нет программного обеспечения разрабатываемого собственными разработчиками/сторонними специалистами.

Вероятность реализации угрозы - _____.

**Установка ПО не связанного с исполнением служебных обязанностей**

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

В Учреждении введено разграничение правами пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО.

Вероятность реализации угрозы - маловероятна.

**1.8.2.3 Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера**

### Утрата ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В Учреждении введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика "чистого стола", осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Вероятность реализации угрозы - низкая.

### Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

В Учреждении осуществляется резервное копирование обрабатываемых ПДн, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы - маловероятна.

### Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы - маловероятна.

### Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В Учреждении осуществляет резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы - маловероятна.

### Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В Учреждении ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания и осуществляет резервное копирование информации.

Вероятность реализации угрозы - маловероятна.

**Стихийное бедствие**

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В Учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы - маловероятна.

### 1.8.2.4 Угрозы преднамеренных действий внутренних нарушителей

**Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке**

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы - маловероятна.

**Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке**

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В Учреждении пользователи осведомлены о порядке работы с персональными данными, а так же подписали Договор о неразглашении.

Вероятность реализации угрозы - маловероятна.

### 1.8.2.5 Угрозы несанкционированного доступа по каналам связи

В соответствии с "Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена" (п. 6.6 Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

- угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

- угрозы выявления паролей по сети;
- угрозы навязывание ложного маршрута сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы типа "Отказ в обслуживании";
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

### Угроза "Анализ сетевого трафика"

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

- изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;

- перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

### Перехват за переделами с контролируемой зоны

Вероятность реализации угрозы - _____.

### Перехват в пределах контролируемой зоны внешними нарушителями

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы - маловероятна.

### Перехват в пределах контролируемой зоны внутренними нарушителями

В Учреждении введен контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания.

Вероятность реализации угрозы - маловероятна.

### Угроза "сканирование сети"

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Вероятность реализации угрозы - _____.

### Угроза выявления паролей

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя "проход" для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Вероятность реализации угрозы - _____.

### Угрозы навязывание ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

Вероятность реализации угрозы - _____.

### Угрозы подмены доверенного объекта

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн - цели угроз.

Вероятность реализации угрозы - _____.

### Внедрение ложного объекта сети

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

Вероятность реализации угрозы - _____.

### Угрозы типа "Отказ в обслуживании"

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);
- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа "Land", "TearDrop", "Bonk", "Nuke", "UDP-bomb") или имеющих длину, превышающую максимально допустимый размер (угроза типа "Ping Death"), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может "вместить" трафик (направленный "шторм запросов"), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Вероятность реализации угрозы - _____.

### Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, "сетевые шпионы", основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;
- удаленный запуск приложения путем переполнения буфера приложений-серверов;
- удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного "вируса Морриса".

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, "троянскими" программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т.п.). В результате их использования удается добиться

удаленного контроля над станцией в сети.

Вероятность реализации угрозы - _____.

### Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. "Полноценные" сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, "подтолкнуть" пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;
- программы-генераторы компьютерных вирусов;
- программы, демонстрирующие уязвимости средств защиты информации и др.

Вероятность реализации угрозы - _____.

## 1.9 Реализуемость угроз

По итогам оценки уровня защищенности ($Y_1$) и вероятности реализации угрозы ($Y_2$), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = \left(Y_1 + Y_2\right)/20$

Оценка реализуемости УБПДн представлена в таблице.

**Таблица 4** - Реализуемость УБПДн

| Тип угроз безопасности ПДн | Коэффициент реализуемости угрозы (Y) | Возможность реализации |
|---|---|---|
| 1. Угрозы от утечки по техническим каналам. | | |
| 1.1. Угрозы утечки акустической информации | | |
| 1.2. Угрозы утечки видовой информации | | |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | | |
| 2. Угрозы несанкционированного доступа к информации. | | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | | |
| 2.1.1. Кража ПЭВМ | | |
| 2.1.2. Кража носителей информации | | |
| 2.1.3. Кража ключей и атрибутов доступа | | |

| | | |
|---|---|---|
| 2.1.4. Кражи, модификации, уничтожения информации | | |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | | |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | | |
| 2.1.7. Несанкционированное отключение средств защиты | | |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | | |
| 2.2.1. Действия вредоносных программ (вирусов) | | |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | | |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | | |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | | |
| 2.3.1. Утрата ключей и атрибутов доступа | | |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | | |
| 2.3.3. Непреднамеренное отключение средств защиты | | |
| 2.3.4. Выход из строя аппаратно-программных средств | | |
| 2.3.5. Сбой системы электроснабжения | | |
| 2.3.6. Стихийное бедствие | | |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | | |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке | | |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | | |
| 2.5.Угрозы несанкционированного доступа по каналам связи. | | |
| 2.5.1.Угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: | | |
| 2.5.1.1. Перехват за переделами с контролируемой зоны | | |

| | | |
|---|---|---|
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | | |
| 2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями. | | |
| 2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. | | |
| 2.5.3. Угрозы выявления паролей по сети | | |
| 2.5.4. Угрозы навязывание ложного маршрута сети | | |
| 2.5.5. Угрозы подмены доверенного объекта в сети | | |
| 2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | | |
| 2.5.7. Угрозы типа "Отказ в обслуживании" | | |
| 2.5.8. Угрозы удаленного запуска приложений | | |
| 2.5.9. Угрозы внедрения по сети вредоносных программ | | |

## 1.10 Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

- низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности УБПДн представлена таблице.

**Таблица 5** - Опасность УБПДн

| Тип угроз безопасности ПДн | Опасность угрозы |
|---|---|
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации | |
| 1.2. Угрозы утечки видовой информации | |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | |
| 2.1.1. Кража ПЭВМ | |

| | |
|---|---|
| 2.1.2. Кража носителей информации | |
| 2.1.3. Кража ключей и атрибутов доступа | |
| 2.1.4. Кражи, модификации, уничтожения информации | |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | |
| 2.1.7. Несанкционированное отключение средств защиты | |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | |
| 2.2.1. Действия вредоносных программ (вирусов) | |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | |
| 2.3.1. Утрата ключей и атрибутов доступа | |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | |
| 2.3.3. Непреднамеренное отключение средств защиты | |
| 2.3.4. Выход из строя аппаратно-программных средств | |
| 2.3.5. Сбой системы электроснабжения | |
| 2.3.6. Стихийное бедствие | |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке | |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | |
| 2.5. Угрозы несанкционированного доступа по каналам связи. | |
| 2.5.1. Угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: | |
| 2.5.1.1. Перехват за переделами с контролируемой зоны | |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | |
| 2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями. | |
| 2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. | |
| 2.5.3. Угрозы выявления паролей по сети | |
| 2.5.4. Угрозы навязывание ложного маршрута сети | |
| 2.5.5. Угрозы подмены доверенного объекта в сети | |

| | |
|---|---|
| 2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | |
| 2.5.7. Угрозы типа "Отказ в обслуживании" | |
| 2.5.8. Угрозы удаленного запуска приложений | |
| 2.5.9. Угрозы внедрения по сети вредоносных программ | |

### 1.11 Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

**Таблица 6** - Правила определения актуальности УБПДн

| Возможность реализации угрозы | Показатель опасности угрозы | | |
|---|---|---|---|
| | Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

Оценка актуальности угроз безопасности представлена в таблице.

**Таблица 7** - Актуальность УБПДн

| Тип угроз безопасности ПДн | Опасность угрозы |
|---|---|
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации | |
| 1.2. Угрозы утечки видовой информации | |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | |
| 2.1.1. Кража ПЭВМ | |
| 2.1.2. Кража носителей информации | |
| 2.1.3. Кража ключей и атрибутов доступа | |
| 2.1.4. Кражи, модификации, уничтожения информации | |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | |
| 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | |
| 2.1.7. Несанкционированное отключение средств защиты | |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | |
| 2.2.1. Действия вредоносных программ (вирусов) | |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | |

| | |
|---|---|
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | |
| 2.3.1. Утрата ключей и атрибутов доступа | |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | |
| 2.3.3. Непреднамеренное отключение средств защиты | |
| 2.3.4. Выход из строя аппаратно-программных средств | |
| 2.3.5. Сбой системы электроснабжения | |
| 2.3.6. Стихийное бедствие | |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке | |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | |
| 2.5.Угрозы несанкционированного доступа по каналам связи. | |
| 2.5.1.Угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: | |
| 2.5.1.1. Перехват за переделами с контролируемой зоны | |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | |
| 2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями. | |
| 2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. | |
| 2.5.3.Угрозы выявления паролей по сети | |
| 2.5.4. Угрозы навязывание ложного маршрута сети | |
| 2.5.5. Угрозы подмены доверенного объекта в сети | |
| 2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | |
| 2.5.7. Угрозы типа "Отказ в обслуживании" | |
| 2.5.8. Угрозы удаленного запуска приложений | |
| 2.5.9. Угрозы внедрения по сети вредоносных программ | |

Были выявлены следующие актуальные угрозы:

1) _____
2) _____
3) _____

Для снижения опасности реализации актуальных УБПДн рекомендуется осуществить следующие мероприятия:

1) _____
2) _____

## 1.12 Модель угроз безопасности

Исходный класс защищенности - _____.

**Таблица 8** - Угрозы безопасности

| Наименование угрозы | Вероятность реализации угрозы (Y2) | Возможность реализации угрозы (Y) | Опасность угрозы | Актуальность угрозы | Меры по противодействию угрозе | |
|---|---|---|---|---|---|---|
| | | | | | Технические | Организационные |
| 1. Угрозы от утечки по техническим каналам | | | | | | |
| 1.1. Угрозы утечки акустической информации | | | | | | |
| 1.2. Угрозы утечки видовой информации | | | | | | |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | | | | | | |
| 2. Угрозы несанкционированного доступа к информации | | | | | | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | | | | | | |
| 2.1.1. Кража ПЭВМ | | | | | | |
| 2.1.2. Кража носителей информации | | | | | | |
| 2.1.3. Кража ключей доступа | | | | | | |
| 2.1.4. Кражи, модификации, уничтожения информации. | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | | | | | | |
| 2.1.6. Несанкционированное отключение средств защиты | | | | | | |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий); | | | | | | |
| 2.2.1. Действия вредоносных программ (вирусов) | | | | | | |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | | | | | | |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | | | | | | |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | | | | | | |
| 2.3.1. Утрата ключей и атрибутов доступа | | | | | | |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | | | | | | |
| 2.3.3. Непреднамеренное отключение средств защиты | | | | | | |
| 2.3.4. Выход из строя аппаратно-программных средств | | | | | | |
| 2.3.5. Сбой системы электроснабжения | | | | | | |
| 2.3.6. Стихийное бедствие | | | | | | |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | | | | | | |
| 2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке | | | | | | |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| допущенными к ее обработке | | | | | | |
| 2.5. Угрозы несанкционированного доступа по каналам связи | | | | | | |
| 2.5.1. Угроза "Анализ сетевого трафика" с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: | | | | | | |
| 2.5.1.1. Перехват за переделами с контролируемой зоны; | | | | | | |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями; | | | | | | |
| 2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями. | | | | | | |
| 2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2.5.3. Угрозы выявления паролей по сети. | | | | | | |
| 2.5.4. Угрозы навязывание ложного маршрута сети. | | | | | | |
| 2.5.5. Угрозы подмены доверенного объекта в сети. | | | | | | |
| 2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях. | Маловероятно | Низкая | Низкая | Неактуальная | | |
| 2.5.7. Угрозы типа "Отказ в обслуживании". | Маловероятно | Низкая | Низкая | Неактуальная | | |
| 2.5.8. Угрозы удаленного запуска приложений. | Маловероятно | Низкая | Низкая | Неактуальная | | |
| 2.5.9. Угрозы внедрения по сети вредоносных программ. | Маловероятно | Низкая | Низкая | Неактуальная | | |

**Заключение**

В соответствии с Порядком проведения классификации информационных систем персональных данных утвержденного приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20, на основании категории и объема обрабатываемых персональных данных - ИСПДн "_____" классифицируется, как _____ ИСПДн класса K_.

Аттестация ИСПДн _____ (не) требуется.

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 12**

**План**
**мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |

Москва 2009

**1 Общие положения**

План мероприятий по обеспечению защиты персональных данных (далее - План), содержит необходимый перечень мероприятий для обеспечения защиты персональных данных.

План составлен на основании списка мер, методов и средств защиты, определенных в Концепции информационной безопасности и Политике информационной безопасности.

Выбор конкретных мероприятий осуществляется на основании анализа Отчета по результатам внутренней проверки и Модели угроз безопасности.

В План включены следующие категории мероприятий:

- организационные (административные);
- физические;
- технические (аппаратные и программные);
- контролирующие.

В План включена следующая информация:

- Название мероприятия.
- Периодичность мероприятия (разовое/периодическое).
- Исполнитель мероприятия/ответственный за исполнение.

План внутренних проверок составляется на все информационные системы персональных данных Учреждения.

## 2 План мероприятий по обеспечению безопасности ПДн

| Мероприятие | Периодичность | Исполнитель/ Ответственный |
|---|---|---|
| ИСПДн 1 | | |
| Организационные мероприятия | | |
| Первичная внутренняя проверка | Разовое<br>срок до 01.01.2010 г. | |
| Определение перечня ИСПДн | Разовое<br>срок до | |
| Определение обрабатываемых ПДн и объектов защиты | Разовое<br>срок до | |
| Определение круга лиц участвующих в обработке ПДн | Разовое<br>срок до | |
| Определение ответственности лиц участвующих в обработке | Разовое<br>срок до | |
| Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей | Разовое<br>срок до | |
| Назначение ответственного за безопасность ПДн | Разовое<br>срок до | |
| Введение режима защиты ПДн | Разовое<br>срок до | |
| Утверждение Концепции информационной безопасности | Разовое<br>срок до | |
| Утверждение Политики информационной безопасности | Разовое<br>срок до | |
| Собрание коллегиального органа по классификации ИСПДн | Разовое<br>срок до | |
| Классификация всех выявленных ИСПДн | Разовое<br>срок до | |
| Первичный анализ актуальности УБПДн | Разовое<br>срок до | |
| Установление контролируемой зоны вокруг ИСПДн | Разовое<br>срок до | |

| | | |
|---|---|---|
| Выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц не допущенных к обработке ПДн | Разовое<br>срок до | |
| Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн. | Разовое<br>срок до | |
| Организация порядка резервного копирования защищаемой информации на твердые носители | Разовое<br>срок до | |
| Организация порядка восстановления работоспособности технических средств, ПО, баз данных с подсистем СЗПДн | Разовое<br>срок до | |
| Введение в действие инструкции по порядку формирования, распределения и применения паролей | Разовое<br>срок до | |
| Организация информирования и обучения сотрудников о порядке обработки ПДн | Разовое<br>срок до | |
| Организация информирования и обучения сотрудников о введенном режиме защиты ПДн | Разовое<br>срок до | |
| Разработка должностных инструкций о порядке обработки ПДн и обеспечении введенного режима защиты | Разовое<br>срок до | |
| Разработка инструкций о порядке работы при подключении к сетям общего пользования и (или) международного обмена | Разовое<br>срок до | |
| Разработка инструкций о действии в случае возникновения внештатных ситуаций | Разовое<br>срок до | |
| Разработка положения о внесении изменения в штатное программное обеспечение элементов ИСПДн | Разовое<br>срок до | |
| Разработка положения о порядке внесения изменений в программное обеспечение собственной разработки или штатное ПО специально дорабатываемое собственными разработчиками или сторонними организациями.<br>Положение должно включать в себя техническое задание на изменения, технический проект, приемо-сдаточные испытания, акт о введении в эксплуатацию. | Разовое<br>срок до | |
| Организация журнала учета обращений субъектов ПДн | Разовое<br>срок до | |
| Организация перечня по учету технических средств и средств защиты, а так же документации к ним | Разовое<br>срок до | |
| Физические мероприятия | | |

| | | |
|---|---|---|
| Организация постов охраны для пропуска в контролируемую зону | Разовое<br>срок до | |
| Внедрение технической системы контроля доступа в контролируемую зону и помещения (по электронным пропускам, токену, биометрическим данным и т.п.) | Разовое<br>срок до | |
| Внедрение технической системы контроля доступа к элементам ИСПДн (по электронным пропускам, токену, биометрическим данным и т.п.) | Разовое<br>срок до | |
| Внедрение видеонаблюдения | Разовое<br>срок до | |
| Установка дверей на входе в помещения с аппаратными средствами ИСПДн | Разовое<br>срок до | |
| Установка замков на дверях в помещениях с аппаратными средствами ИСПДн | Разовое<br>срок до | |
| Установка жалюзи на окнах | Разовое<br>срок до | |
| Установка решеток на окнах первого и последнего этажа здания | Разовое<br>срок до | |
| Установка системы пожаротушения в помещениях, где расположены элементы ИСПДн | Разовое<br>срок до | |
| Установка систем кондиционирования в помещениях, где расположены аппаратные средства ИСПДн | Разовое<br>срок до | |
| Установка систем бесперебойного питания на ключевые элементы ИСПДн | Разовое<br>срок до | |
| Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн | Разовое<br>срок до | |
| Технические (аппаратные и программные) мероприятия | | |
| Внедрение единого хранилища зарегистрированных действий пользователей с ПДн | Разовое<br>срок до | |
| Внедрение специальной подсистемы управления доступом, регистрации и учета (НАЗВАНИЕ) | Разовое<br>срок до | |
| Внедрение антивирусной защиты (НАЗВАНИЕ) | Разовое<br>срок до | |
| Внедрение межсетевого экранирования (НАЗВАНИЕ) | Разовое<br>срок до | |
| Внедрение подсистемы анализа защищенности (НАЗВАНИЕ) | Разовое<br>срок до | |
| Внедрение подсистемы обнаружения вторжений (НАЗВАНИЕ) | Разовое<br>срок до | |
| Внедрение криптографической защиты (НАЗВАНИЕ) | Разовое<br>срок до | |
| Контролирующие мероприятия | | |

| | | |
|---|---|---|
| Создание журнала внутренних проверок и поддержание его в актуальном состоянии | Ежемесячно | |
| Контроль над соблюдением режима обработки ПДн | Еженедельно | |
| Контроль над соблюдением режима защиты | Ежедневно | |
| Контроль над выполнением антивирусной защиты | Еженедельно | |
| Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена | Еженедельно | |
| Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн | Ежегодно | |
| Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн | Еженедельно | |
| Контроль за обеспечением резервного копирования | Ежемесячно | |
| Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз | Ежегодно | |
| Поддержание в актуальном состоянии нормативно-организационных документов | Ежемесячно | |
| Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями. | Ежемесячно | |

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ

_____

_____

"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 13**

**Порядок**
**резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |

Москва 2009

## 1 Назначение и область действия

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее - Инструкция), связанные с функционированием ИСПДн Учреждения _____, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей Учреждения, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор ИСПДн _____.

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор безопасности _____

## 2 Порядок реагирования на инцидент

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых

пользователям ИСПДн, а так же потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

- В результате непреднамеренных действий пользователей.
- В результате преднамеренных действий пользователей и третьих лиц.
- В результате нарушения правил эксплуатации технических средств ИСПДн.
- В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в "Журнале по учету мероприятий по контролю".

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Учреждения (Администратор безопасности, Администратор и Оператор ИСПДн), сотрудниками предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

## 3 Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

### 3.1 Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения Учреждения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

- резервные линии электропитания в пределах комплекса зданий;

- аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

- кластеризация;

- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

### 3.2 Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных - не реже раза в неделю;

- для технологической информации - не реже раза в месяц;

- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн - не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ

_____

_____

"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 14**

**План**
**внутренних проверок режима защиты персональных данных в ИСПД учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

Москва 2009

## 1 Общие положения

План внутренних проверок режима защиты персональных данных, содержит перечень внутренних проверок.

План составляется для мероприятий, в соответствии с Планом мероприятий по обеспечению защиты персональных данных, и определяет периодичность проведения проверок.

В План внутренних проверок содержит следующую информацию:

- Название проверяемого мероприятия.
- Периодичность проведения проверки.
- Исполнитель мероприятия.

План внутренних проверок распространяется на все информационные системы персональных данных Учреждения.

## 2 План внутренних проверок режима защиты персональных данных

| Мероприятие | Периодичность | Исполнитель |
|---|---|---|
| Контроль над соблюдением режима обработки ПДн | Еженедельно | |
| Контроль над соблюдением режима защиты | Ежедневно | |
| Контроль над выполнением антивирусной защиты | Еженедельно | |
| Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена | Еженедельно | |
| Проведение внутренних проверок на предмет выявления изменений в | Ежегодно | |

| | | |
|---|---|---|
| режиме обработки и защиты ПДн | | |
| Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн | Еженедельно | |
| Контроль за обеспечением резервного копирования | Ежемесячно | |
| Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз | Ежегодно | |
| Поддержание в актуальном состоянии нормативно-организационных документов | Ежемесячно | |
| Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО специально дорабатываемое собственными разработчиками или сторонними организациями. | Ежемесячно | |

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 15**

**Журнал**
**по учету мероприятий по контролю обеспечения защиты персональных данных в ИСПД учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

Москва 2009

## 1 Общие положения

Журнал учета мероприятий по контролю над соблюдением режима защиты персональных данных, содержит перечень периодически проводимых мероприятий.

В Журнале отмечаются мероприятия, в соответствии с Планом мероприятий по обеспечению защиты персональных данных, носящих периодический характер.

В журнал заносится следующая информация:

- Название проведенного мероприятия.
- Дата проведенного мероприятия.
- Исполнитель мероприятия.
- Результат (отчет, действия) мероприятия, если есть.

## 2 Журнал учета мероприятий по контролю над соблюдением режима защиты персональных данных

| Мероприятие | Дата | Исполнитель | Результат |
|---|---|---|---|
| Проверка осведомленности пользователей о режиме защиты ПДн | 01.01.2010 | Иванов А.А. | |
| Переход на новую версию СУБД ORACLE | 01.01.2010 | Сидоров С.С. | Установлена СУБД ORACLE версии 10 |
| Плановый аудит информационной безопасности | 01.01.2010 | ЗАО "Практика Безопасности" | Аналитический отчет |
| Установлена система контроля доступа в помещение серверной по электронному пропуску | 01.01.2010 | ЗАО "Ромашка" | |
| Введена охрана контролируемой зоны | 01.01.2010 | ЧОП "Снежинка" | |
| Составлены акты классификации ИСПДн | 01.01.2010 | Иванов А.А. Сидоров С.С. | |
| Проверка антивирусной защиты | 01.01.2010 | Сидоров С.С. | Еженедельная проверка - нарушений не обнаружено |
| Осуществлено плановое резервное копирование обрабатываемых персональных данных | 01.01.2010 | Сидоров С.С. | Носители N 3-5 |
| | | | |
| | | | |

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 16**

**Журнал**
**учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в ИСПД учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

_____ _____ _____
подпись, дата
_____ _____ _____
подпись, дата
_____ _____ _____
подпись, дата

Москва 2009

**Журнал учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в ИСПДн "_____"**

| N | ФИО | Дата | Цель |
|---|---|---|---|
| | Иванов И.И. | 01.10.2010 | Информирование |
| | Сидоров С.С. | 01.10.2010 | Прекращение обработки |
| | Петров П.П. | 01.10.2010 | Уточнение ПДн |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 17**

**Инструкция**
**администратора ИСПД учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

_____ _____ _____
подпись, дата
_____ _____ _____
подпись, дата
_____ _____ _____
подпись, дата

Москва 2009

## 1 Общие положения

1.1. Администратор ИСПДн (далее - Администратор) назначается приказом руководителя Учреждения, на основании Положение о разграничении прав доступа к обрабатываемым персональным данным.

1.2. Администратор подчиняется _____.

1.3. Администратор в своей работе руководствуется настоящей инструкцией, Концепцией и Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Учреждения _____.

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

1.5. Методическое руководство работой Администратора осуществляется

ответственным за обеспечение защиты персональных данных.

## 2 Должностные обязанности

Администратор обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
- аппаратных средств;
- аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.

2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

2.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 18**

**Инструкция**
**пользователя информационной системы персональных данных учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |

Москва 2009

## 1 Общие положения

1.1. Пользователь ИСПДн (далее - Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Концепцией и Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Учреждения _____.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

## 2 Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 3).

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена - Интернет и других (раздел 4).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться в _____ по электронной почте: _____ или по внутреннему телефону _____.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн по внутреннему телефону _____.

2.9. Пользователям запрещается:

- Разглашать защищаемую информацию третьим лицам.
- Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.
- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
- Несанкционированно открывать общий доступ к папкам на своей рабочей станции.
- Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.
- Отключать (блокировать) средства защиты информации.
- Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.
- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
- Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках

возложенных, в пределах возложенных на него функций.

## 3 Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

- Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.
- Пароль должен состоять не менее чем из 8 символов.
- В пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

- Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа "123", "111", "qwerty" и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.
- Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- Запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

- Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.
- Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранение пароля:

- Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.
- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.
- своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

## 4 Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

- Осуществлять работу при отключенных средствах защиты (антивирус и других).
- Передавать по Сети защищаемую информацию без использования средств шифрования.
- Запрещается скачивать из Сети программное обеспечение и другие файлы.
- Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие).
- Запрещается нецелевое использование подключения к Сети.

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 19**

**Частная инструкция по обеспечению безопасности информации на объекте вычислительной техники**

**Инструкция
администратора безопасности при использовании ресурсов объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |

Москва 2009

## 1 Общие положения

1.1. Администратор безопасности ИСПДн (далее - Администратор) назначается приказом руководителя Учреждения, на основании Положение о разграничении прав доступа к обрабатываемым персональным данным.

1.2. Администратор подчиняется _____

1.3. Администратор в своей работе руководствуется настоящей инструкцией, Концепцией и Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Учреждения _____.

1.4. Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.5. Администратор безопасности является ответственным должностным лицом Учреждения, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.6. Администратор безопасности должен иметь специальное рабочее место, размещенное в здании Учреждения так, что бы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а так же средствами контроля за техническими средствами защиты.

1.8. Администратор безопасности осуществляет методическое руководство Операторов и Администраторов ИСПДн, в вопросах обеспечения безопасности персональных данных.

1.9. Требования администратора информационной безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.10. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

## 2 Должностные обязанности

Администратор безопасности обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Осуществлять установку, настройку и сопровождение технических средств защиты.

2.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.4. Участвовать в приемке новых программных средств.

2.5. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.6. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

2.7. Вести контроль над процессом осуществления резервного копирования

объектов защиты.

2.8. Осуществлять контроль над выполнением Плана мероприятий по защите персональных данных.

2.9. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.10. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.11. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.12. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты.

2.13. Контролировать исполнение пользователями парольной политики.

2.14. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

2.15. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

2.16. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.17. Не допускать к работе на элементах ИСПДн посторонних лиц.

2.18. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.

2.19. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

2.20. Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.21. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.22. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ

_____

_____

"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 20**

**Частная инструкция по обеспечению безопасности информации на объекте вычислительной техники**

**Инструкция**
**пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |

Москва 2009

## 1 Назначение и область действия

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн Учреждения _____, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

Задачей данной Инструкции является:

- определение мер защиты от прерывания;
- определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех пользователей Учреждения, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

## 2 Порядок реагирования на аварийную ситуацию

### 2.1 Действия при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении 1.

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в "Журнале по учету

мероприятий по контролю".

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Учреждения сотрудниками (Администратор безопасности, Администратор и Оператор ИСПДн) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

### 2.2 Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

- Уровень 1 - Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

- Уровень 2 - Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

- Отказ элементов ИСПДн и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;

- сбоя системы кондиционирования.

- Отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за:

- химического выброса в атмосферу;

- сбоев общественного транспорта;

- эпидемии;

- массового отравления персонала;

- сильного снегопада;

- торнадо;

- сильных морозов.

- Уровень 3 - Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к работоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;

- взрыв;

- просадка грунта с частичным обрушением здания;

- массовые беспорядки в непосредственной близости от Объекта.

## 3 Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

### 3.1 Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения Учреждения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Порядке резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

### 3.2 Организационные меры

Ответственные за реагирование сотрудники ознакомляют всех сотрудников Учреждения, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу.

По окончанию ознакомления сотрудник расписывается в журнале, предоставляемом Ответственным за реагирование сотрудником. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

Должно быть проведено обучение должностных лиц Учреждения, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения, газоснабжения.

Администраторы ИСПДн и Администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

Ответственность за организацию обучения должностных лиц несет _____. Сроки и порядок их обучения согласуется с Администратором безопасности.

**Приложение 1**
**Источники угроз**

**Таблица 1** - Источники угроз

| | |
|---|---|
| **Технологические угрозы** | |
| 1 | Пожар в здании |
| 2 | Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения) |
| 3 | Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением) |
| 4 | Химический выброс в атмосферу |
| **Внешние угрозы** | |
| 5 | Массовые беспорядки |
| 6 | Сбои общественного транспорта |
| 7 | Эпидемия |
| 8 | Массовое отравление персонала |
| **Стихийные бедствия** | |
| 9 | Удар молнии |
| 10 | Сильный снегопад |
| 11 | Сильные морозы |
| 12 | Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания |
| 13 | Затопление водой в период паводка |
| 14 | Наводнение, вызванное проливным дождем |
| 15 | Торнадо |
| 16 | Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод) |
| **Телеком и ИТ угрозы** | |
| 17 | Сбой системы кондиционирования |
| 18 | Сбой ИТ - систем |
| **Угроза, связанная с человеческим фактором** | |
| 19 | Ошибка персонала, имеющего доступ к серверной |
| 20 | Нарушение конфиденциальности, целостности и доступности конфиденциальной информации |
| **Угрозы, связанные с внешними поставщиками** | |
| 21 | Отключение электроэнергии |
| 22 | Сбой в работе интернет-провайдера |
| 23 | Физически разрыв внешних каналов связи |

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ

_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 21**

**Перечень**
**по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним**

СОГЛАСОВАНО

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

Москва 2009

## 1 Общие положения

Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним, составляется на основании Отчета о результатах проведения внутренней проверки обеспечения защиты персональных данных .

Требования к техническим средствам защиты описаны в Политике информационной безопасности, раздел 4.

В Перечне должна содержаться следующая информация:

- Название средства защиты.
- Эксплуатационная информация.
- Техническая документация.

Перечень по учету технических средств защиты информации, эксплуатационной и технической документации к ним, составляется для каждой ИСПДн.

Перечень должен поддерживаться в актуальном состоянии.

**Приложение 1 ИСПДн____**
**Перечень**
**по учету применяемых средств защиты информации, эксплуатационной и технической документации**

| Техническое средство | Эксплуатационная информация | Техническая документация |
|---|---|---|

| | | |
|---|---|---|
| Антивирус<br>НАЗВАНИЕ<br><br>версия | Антивирус настроен на:<br>- резидентный антивирусный мониторинг;<br>- ежедневное антивирусное сканирование;<br>- скрипт-блокирование;<br>- автоматизированное обновление антивирусных баз с периодичностью _____.<br><br>Ключи и атрибуты доступа хранятся у _____ в _____ (сейф, криптографически защищенный носитель и т.п.) | Журнал настроек Межсетевого экрана хранится у<br>_____ |
| Межсетевой экран<br>НАЗВАНИЕ<br><br>версия | Межсетевой экран настроен на:<br>- фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;<br>- регистрацию и учет запрашиваемых сервисов прикладного уровня:<br>- _____<br>- _____<br>- _____<br>- блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату.<br><br>Ключи и атрибуты доступа хранятся у _____ в _____ (сейф, криптографически защищенный носитель и т.п.) | Инструкция по установке и настройке от производителя.<br><br>Журнал настроек Межсетевого экрана хранится у<br>_____ |
| | | |
| | | |
| | | |

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 22**

**Типовое Техническое задание**
**на разработку системы обеспечения безопасности информации объекта вычислительной техники учреждения здравоохранение, социальной сферы, труда и занятости**

СОГЛАСОВАНО

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

Москва 2009

## 1 Общие сведения

1.1. Заказчик: Министерство здравоохранения и социального развития Российской Федерации, учреждение здравоохранение, социальной сферы, труда и занятости (далее Заказчик).

1.1.1. Исполнитель: _____ (далее - Исполнитель) (Лицензия ФСТЭК России рег. N от "__" _____ 20___ г. на деятельность по технической защите конфиденциальной информации), аттестат аккредитации N СЗИ RU.____.____.____ от "__".__.____ г. (продлен до "__" _____ 20___ г.).

1.1.2. Основание для выполнения работ: Договор N___ от "__" _____2009 г.

1.2. Плановые сроки начала и окончания работы определяются Договором.

## 2 Цели и задачи выполнения работ

Основной целью проведения работ является приведение порядка обработки, хранения и передачи персональных данных сотрудников, клиентов и контрагентов учреждения здравоохранения, социальной сферы, труда и занятости в соответствие требованиям перечисленных в Разделе 3 данного Технического Задания нормативно-правовых документов, в том числе и в части требований к технической защите автоматизированных систем, обрабатывающих персональные данные.

В рамках проекта будут решены следующие задачи:

- определены места и способы обработки персональных данных;
- составлен актуальный для Заказчика перечень требований, предъявляемых к защите персональных данных;
- реализованы организационные и технические меры по защите персональных данных, доработана нормативная документация Заказчика.
- проведены аттестационные испытания информационных систем персональных данных;
- оказаны консультационные услуги по подготовке предприятия (организации) к выполнению лицензионных требований и условий, определенных постановлением Правительства Российской Федерации от 15 августа 2006 г. N 504 "О лицензировании деятельности по технической защите конфиденциальной информации".

## 3 Требования к составу и содержанию работ

Работы должны проводится в соответствии с положениями нижеследующих нормативно-правовых документов:

- Федеральный закон от 27.07.2006 г. N 152-ФЗ "О персональных данных" (далее - ФЗ "О персональных данных"), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн;
- "Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденное Постановлением Правительства РФ от 17.11.2007 г. N 781;
- "Порядок проведения классификации информационных систем персональных данных", утвержденный совместным Приказом ФСТЭК России N 55, ФСБ России N 86 и Мининформсвязи РФ N 20 от 13.02.2008 г.;
- "Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", утвержденное Постановлением Правительства РФ от 15.09.2008 г. N 687;
- "Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных", утвержденные Постановлением Правительства РФ от 06.07.2008 г. N 512;
- Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:
- Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП);
- Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП);
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП);
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП) Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

Работы должны проводиться в один этап:

- Этап 1. Приведение в соответствие порядка обработки персональных данных.

### 3.1 Этап 1. Первая очередь приведения в соответствие порядка обработки персональных данных

Следующие работы должны быть проведены в отношении всех существующих у Заказчика ИСПДн:

- Определение категорий субъектов персональных данных.
- Определение перечня (состава) персональных данных, обрабатываемых в информационной системе.
- Определение целей обработки персональных данных.
- Определение срока, в течение которого производится обработка персональных

данных (в том числе их хранение).

- Определение перечня действий с персональными данными, которые производятся в ходе их обработки.
- Определение используемых оператором способов обработки персональных данных.
- Уточнение степени участия персонала в обработке персональных данных, характера их взаимодействия между собой.
- Определение условий расположения информационной сети передачи данных относительно границ контролируемой зоны.
- Определение конфигурации и топологии информационной сети персональных данных в целом и ее отельных компонент, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения.
- Определение исходных данных для классификации информационных систем персональных данных.
- Сбор сведений об имевших место инцидентах информационной безопасности, связанных с персональными данными.
- Изучение существующих организационных мер обеспечения безопасности персональных данных.
- Разработка актуализированной модели угроз.
- Разработка перечня требований по защите персональных данных.
- Определение необходимости аттестации системы.
- Выявление имеющихся средств технической защиты информации, которые могут быть использования для обеспечения безопасности персональных данных.
- Изучение применяемых в информационной системе технических мер обеспечения безопасности персональных данных.
- Анализ соответствия применяющихся мер и средств технической защиты предъявляемым требованиям нормативно-правовой базы Российской Федерации в области защиты персональных данных.
- Разработка рекомендаций по технической защите системы.
- Определение необходимости сертификации имеющихся технических средств и программного обеспечения защиты системы.
- Определение необходимости аттестации системы.
- Определение необходимости получения соответствующих лицензий на осуществление деятельности по защите системы.
- Разработка Эскизного проекта по защите системы.
- Доработка нормативной и рабочей документации системы в части приведения в соответствие требованиям нормативно-правовых документов.

В отношении систем, для которых выявлена необходимость аттестации, должны быть проведены аттестационные испытания.

Состав и порядок проведения работ по аттестации должен определяться Частным Техническим заданием, разрабатываемым Исполнителем в соответствии с данным Техническим заданием.

В рамках работ первого этапа должны быть оказаны консультационные услуги по подготовке предприятия (организации) к выполнению лицензионных требований и условий, определенных постановлением Правительства Российской Федерации от 15 августа 2006 г. N 504 "О лицензировании деятельности по технической защите конфиденциальной информации".

Состав и порядок оказания услуг должен определяться Частным Техническим заданием, разрабатываемым Исполнителем в соответствии с данным Техническим

Заданием.

В рамках первого этапа работ должна быть проведена доработка нормативно-распорядительных документов Заказчика в части приведения в соответствие порядка обработки персональных данных требованиям законодательства.

В случае отсутствия у Заказчика необходимых нормативных документов должны быть разработаны проекты таких документов.

Перечень дорабатываемых и разрабатываемых документов должен быть определен после обследования текущего состояния организационных мер по обеспечению безопасности персональных данных.

## 4 Порядок контроля и приемки работ

4.1. Критериями для приемки работ является настоящее техническое задание (далее - ТЗ) и соответствующие Частные Технические задания, разрабатываемые в процессе выполнения работ.

4.2. Приемка работ осуществляется единовременно, приемке подлежат предоставляемые Заказчику документы согласно разделу 6 настоящего ТЗ.

4.3. Завершение работ оформляется актом приема-сдачи работ (услуг).

4.4. Не позднее последнего дня согласно календарному плану работ, Заказчику предоставляется итоговая версия отчетных документов в электронном виде.

4.5. Заказчик направляет замечания в письменном виде не позднее 5 рабочих дней после предоставления итоговой версии отчетных документов.

## 5 Требования к составу и содержанию мероприятий по подготовке объекта к выполнению работ

5.1. При подготовке к проведению Исполнителем работ на территории Заказчика, со стороны Заказчика необходимо обеспечить следующее:

- назначить ответственное лицо от Заказчика, наделенное соответствующими полномочиями, для обеспечения выполнения работ Исполнителем на территории Заказчика, а также для организации взаимодействия с должностными лицами Заказчика и для обеспечения дистанционного сбора информации (анкетирование, переписка и т.п.);
- выделить рабочие места для членов рабочей группы со стороны Исполнителя, обеспеченные всем необходимым для работы;
- определить сопровождающее лицо для организации и проведения интервьюирования;
- обеспечить доступность лиц, с которыми необходимо провести интервьюирование (перечень лиц, подлежащих интервьюированию, определяется Заказчиком на основе перечня необходимой для проведения работ информации, запрашиваемой Исполнителем), а также лиц, экспертное мнение которых необходимо выяснять при проведении работ.

## 6 Требования к документированию

6.1. По результатам работ должны быть разработаны следующие документы:

1) Положение о защите персональных данных.

2) Положение о подразделении по защите информации.

3) Приказ о назначении ответственных лиц за обработку ПДн.

4) Концепция информационной безопасности ИСПДн учреждения.

5) Политика информационной безопасности ИСПДн учреждения.

6) Перечень персональных данных, подлежащих защите.

7) Приказ о проведении внутренней проверки.

8) Отчет о результатах проведения внутренней проверки.

9) Акт классификации информационной системы персональных данных угроз для конкретной ИСПДн.

10) Положение о разграничении прав доступа к обрабатываемым персональным данным.

11) Модель угроз безопасности персональных данных угроз для конкретной ИСПДн.

12) План мероприятий по обеспечению защиты ПДн.

13) Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

14) Должностные инструкции сотрудников, обрабатывающих ПДн:

- Должностная инструкция администратора ИСПДн.
- Инструкция пользователя ИСПДн.
- Должностная инструкция администратора безопасности ИСПДн.
- Инструкция пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций.

15) План внутренних проверок.

16) Журнал по учету мероприятий по контролю состояния защиты ПДн.

17) Журнал учёта обращений субъектов ПДн о выполнении их законных прав.

18) Положение об Электронном журнале обращений пользователей информационной системы к ПДн.

6.2. Отчетные документы предоставляются Заказчику в электронном виде в формате документов Microsoft Office и на бумажных носителях.

## 7 Порядок проведения работ

7.1. Для выполнения работ Заказчик и Исполнитель по согласованию сторон формируют экспертную группу из специалистов Заказчика и Исполнителя, имеющих необходимую компетенцию.

7.2. Специалисты Заказчика предоставляют всю необходимую информацию Исполнителю для проведения работ и, при необходимости, участвуют совместно с Исполнителем в проводимых работах.

7.3. До начала проведения работ Заказчик предоставляет список и контактную информацию своих сотрудников, которые будут отвечать за взаимодействие с сотрудниками Исполнителя, за оперативное предоставление необходимой информации и согласование отчетных материалов Исполнителя.

7.4 Исходные данные собираются Исполнителем в ходе проведения работ путем:

- интервьюирования персонала Заказчика, в том числе руководителей и сотрудников структурных подразделений;
- анкетирования и направления письменных запросов на предоставление информации;
- анализа документов и записей результатов деятельности Заказчика в части обеспечения безопасности информационных систем персональных данных (нормативных документов, проектной и эксплуатационной документации, актов,

журналов и пр.).

## 8 Дополнительные условия и ограничения

8.1. В случае поставки и внедрения технических средств защиты третьей стороной до начала работ по аттестации ИСПДн, Заказчик согласует с Исполнителем следующее:

- состав и спецификацию технических средств;
- состав сопроводительной документации к техническим средствам и сертификатов;
- схемы установки и подключения;
- настройки аппаратно-программных средств;
- рабочую документацию этапа внедрения.

8.2. Срок поставки и внедрения технических средств защиты не входит в расчет сроков этапов работ.

8.3. В случае задержки по срокам предоставления исходных данных при проведении работ, или неполного предоставления информации со стороны Заказчика, по согласованию сторон возможен перенос сроков выполнения работ по договору в сторону увеличения.

8.4. Область проведения работ ограничена подразделениями _____, расположенными в офисах на территории г. Москва, информационные системы персональных данных, технические средства которых размещены на этой же территории.

**Приложение 1**

### Календарный план работ

| N п/п | Наименование этапа | Продолжительность работ, рабочих дней | Стоимость работ, рубли | Отчетность (по завершении этапа) |
|---|---|---|---|---|
| 1 | Приведение в соответствие порядка обработки персональных данных | | | Согласно раздела 6 Технического задания |

От Исполнителя

_____

(должность)

_____

_____ __.__.

_____

"_____" _____ 2009 г.

От Заказчика

_____

(должность)

_____

_____ __.__.

_____

"_____" _____ 2009 г.

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 23**

**Типовой Эскизный проект**
**на создание системы обеспечения безопасности информации объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |

Москва 2009

**Аннотация**

Настоящий документ входит в состав комплекта документации, разработанной в соответствии с требованиями технического задания по договору N___ от "__" _____ 2009 г.

Документ описывает основные технические решения по защите комплекса информационных систем персональных данных (далее ИСПДн) объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости (далее - Объекта), в которых обработка персональных данных (далее - ПДн) осуществляется с использованием средств автоматизации, в объеме, достаточном для приведения комплекса ИСПДн в соответствие с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных".

Для работы с документом требуются следующие документы:

- "Техническое задание на работы по обеспечению безопасности обработки персональных данных объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости";
- "Отчет об обследовании информационных систем персональных данных объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости";

- "Модель угроз безопасности информационной системы Персональных данных объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости";
- "Требования по защите персональных данных ИСПДн объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости".

## Определения

В настоящем документе используются следующие термины и их определения.

## Допуск

**Допуск** - это право (возможность) субъекта доступа на получение информации и её использование. Права допуска (допуск) предоставляются организацией по определенным правилам с соблюдением определенных процедур. Предоставленные права допуска представляют собой текстовые документы, выполненные по установленным в организации формам и правилам.

## Доступ

**Доступ** - это правила реализации субъектом доступа предоставленных ему прав доступа. Эти правила по-другому называются правилами разграничения доступа.

## Заказчик

Министерство здравоохранения и социального развития Российской Федерации.

## Исполнитель

ЗАО "Практика Безопасности".

## ИСПДн

Информационная система персональных данных.
**ИСПДн** - это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

## Комплекс ИСПДн

Комплекс информационных систем персональных данных.
**Комплекс ИСПДн** - это совокупность ИСПДн предприятия (организации).

## Матрица доступа

**Матрица доступа** - это таблица (совокупность таблиц), отображающая правила разграничения доступа.

## НСД

Несанкционированный доступ (несанкционированные действия).

**НСД** - это доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных

## Обработка ПДн

Обработка персональных данных.

**Обработка ПДн** - это действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение.

Обработка ПДн может осуществляться как с использованием средств автоматизации, так и без использования таковых.

Обработка ПДн с использованием средств автоматизации

Обработка персональных данных с использованием средств автоматизации.

**Обработка ПДн с использованием средств автоматизации** - это обработка ПДн в пределах ИСПДн с использованием информационных технологий и технических средств ИСПДн.

Особенности обработки ПДн с использованием средств автоматизации регулируются Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (утверждено Постановлением Правительства РФ от 17 ноября 2007 г. N 781).

Обработка ПДн без использования средств автоматизации

Обработка персональных данных без использования средств автоматизации.

**Обработка ПДн без использования средств автоматизации** - это обработка ПДн, содержащихся в ИСПДн либо извлеченных из неё, если такие действия с ПДн, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека. При этом обработка ПДн не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержатся в ИСПДн, либо были извлечены из неё.

Особенности обработки ПДн без использования средств автоматизации регулируются Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждено Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687).

## Объект внедрения

Под объектом внедрения понимается совокупность:

- технических средств, позволяющих осуществлять обработку персональных данных (ТС ИСПДн);
- помещений, в которых эти технические средства расположены;
- технологическое оборудование этих помещений (системы электропитания, кондиционирования, пожаротушения и пр.);
- сетевая инфраструктура, обеспечивающая функционирование технических средств.

## Объект доступа

**Объект доступа** - это единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа. Для КСЗ ИСПДн такими объектами являются защищаемые ПДн, технические и программные средства ИСПДн и КСЗ ИСПДн.

## Персональные данные (ПДн)

**ПДн** - это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

## Правила разграничения доступа (ПРД)

**ПРД** - это совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

В ИСПДн, использующих средства автоматизации, ПРД реализуются техническими средства информационной системы персональных данных (ТС ИСПДн). ТС ИСПДн обеспечивают автоматическую и/или автоматизированную реализацию правил доступа субъектов доступа к объектам доступа, а также автоматический контроль за соблюдением этих правил с автоматической регистрацией в электронной форме событий, происходящих при этом событий.

ПРД устанавливаются при проектировании КСЗ ИСПДн и представляют собой таблицу(ы), именуемую как "Матрица доступа".

## Система защиты персональных данных (СЗПДн)

**СЗПДн** - это комплекс организационных и технических мероприятий, направленных на обеспечение безопасности ПДн на предприятии. Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн.

## Комплекс средств защиты ИСПДн (КСЗ ИСПДн)

**КСЗ ИСПДн** - совокупность технических средств защиты информации (в том

числе шифровальных (криптографических) средств, средств предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), предназначенных для защиты ПДн, обрабатываемых на предприятии (в организации) автоматизированным способом.

## Субъект доступа

**Субъект доступа** - это лицо или процесс, действия которого регламентируются правилами разграничения доступа.

## Технические средства информационной системы персональных данных (ТС ИСПДн)

**ТС ИСПДн** - это средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

## Обозначения и сокращения

| | |
|---|---|
| **АРМ** | Автоматизированное рабочее место |
| **АСО** | Активное сетевое оборудование |
| **ВП** | Вредоносная программа |
| **ДМЗ** | Демилитаризованная зона |
| **ДСП** | Для служебного пользования |
| **ИБ** | Информационная безопасность |
| **ИС** | Информационная система |
| **ИСПДн** | Информационная система персональных данных |
| **КИС** | Корпоративная информационная система |
| **ЛВС** | Локальная вычислительная сеть |
| **МЭ** | Межсетевой экран |
| **НДВ** | Недекларированные возможности |
| **НСД** | Несанкционированный доступ |
| **ОАО** | Открытое акционерное общество |
| **ОС** | Операционная система |
| **ПАК** | Программно-аппаратный комплекс |
| **ПМВ** | Программно-математическое воздействие |
| **ПО** | Программное обеспечение |
| **ППО** | Прикладное программное обеспечение |
| **РЦОД** | Резервный центр обработки данных |
| **САЗ** | Система анализа защищенности |
| **СЗИ** | Система защиты информации |
| **КСЗ ИСПДн** | Комплекс средств защиты информационных систем персональных |

| | |
|---|---|
| | данных |
| **СК** | Страховая компания |
| **СОВ** | Система обнаружения вторжений |
| **СУБД** | Система управления базами данных |
| **ФСБ** | Федеральная служба безопасности |
| **ФСТЭК России** | Федеральная служба по техническому и экспортному контролю |
| **ЦОД** | Центр обработки данных |

## 1 Общие положения

1) Заказчик: Министерство здравоохранения и социального развития Российской Федерации (далее - Заказчик).

2) Исполнитель: ЗАО "Практика Безопасности" (далее - Исполнитель) (Лицензия Гостехкомиссии России рег. N _____ от "__" _____ ____ г. на деятельность по технической защите конфиденциальной информации), аттестат аккредитации N СЗИ _____ от __.__.20__ г. (продлен до 21.12.20__г.).

3) Основание для выполнения работ: Договор N___ от "__" _____2009 г.

4) Плановые сроки начала и окончания работы определяются Договором.

### 1.1 Полное наименование системы защиты и ее условное обозначение

Наименование системы защиты: комплекс средств защиты информационных систем персональных данных Объекта. Условное обозначение - КСЗ ИСПДн Объекта.

### 1.2 Цели, назначение и области использования системы защиты

КСЗ ИСПДн предназначен для приведения ИСПДн Объекта в соответствие с Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных".

### 1.3 Наименование предприятий, участвующих в создании системы защиты

В создании системы защиты принимает участие Исполнитель.

### 1.4 Перечень документов, на основании которых создается система

#### 1.4.1 Нормативные документы

1) Федеральный закон от 27.07.2006 г. N 152-ФЗ "О персональных данных" (далее - ФЗ "О персональных данных"), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.

2) "Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденное Постановлением Правительства РФ от 17.11.2007 г. N 781.

3) "Порядок проведения классификации информационных систем персональных

данных", утвержденный совместным Приказом ФСТЭК России N 55, ФСБ России N 86 и Мининформсвязи РФ N 20 от 13.02.2008 г.

4) "Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", утвержденное Постановлением Правительства РФ от 15.09.2008 г. N 687.

5) "Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных", утвержденные Постановлением Правительства РФ от 06.07.2008 г. N 512.

6) Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

7) Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

8) Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

9) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

10) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)

### 1.4.2 Документы предпроектных стадий создания КСЗ ИСПДн

1) "Техническое задание на работы по обеспечению безопасности обработки персональных данных объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости";

2) "Отчет об обследовании информационных систем персональных данных объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости";

3) "Модель угроз безопасности информационной системы Персональных данных объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости";

4) "Требования по защите персональных данных ИСПДн объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости".

## 2 Описание процесса поддержания безопасности ПДн

### 2.1 Технологии обеспечения информационной безопасности Объекта

#### 2.1.1 Общие требования к обеспечению безопасности ПДн в ИСПДн

Обеспечение безопасности ПДн при их обработке в ИСПДн должно осуществляться подразделением технической защиты информации совместно с

администраторами на всех стадиях жизненного цикла ИСПДн в рамках системы защиты ПДн (далее - СЗПДн) и состоять из согласованных организационных и технических мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, минимизацию возможного ущерба, а также восстановление данных и нормального функционирования ИСПДн в случае реализации угроз.

В целях защиты ПДн от несанкционированного доступа и иных неправомерных действий мероприятия по организации и техническому обеспечению безопасности ПДн для каждой ИСПДн должны включать:

- классификацию ИСПДн на основании установленных критериев в соответствии с "Порядком проведения классификации информационных систем персональных данных", утвержденным совместным Приказом ФСТЭК России N 55, ФСБ России N 86 и Мининформсвязи РФ N 20 от 13.02.2008 г.;
- выявление и закрытие технических каналов утечки ПДн на основе анализа и актуализации модели угроз безопасности ПДн;
- установку, настройку и применение соответствующих программных, аппаратных и программно-аппаратных средств защиты информации в рамках СЗПДн;
- разработку должностных инструкций по обеспечению безопасности ПДн при их обработке в ИСПДн для персонала, задействованного в эксплуатации данной ИСПДн.

Предотвращение утечки ПДн по техническим каналам за счет побочных электромагнитных излучений и наводок, а также за счет электроакустических преобразований реализуется путем выбора мест установки аппаратных средств ИСПДн и применения защищенных технических средств, сертифицированных по требованиям информационной безопасности, внедрением объектовых мер защиты, в том числе, установлением контролируемой зоны вокруг объектов ИСПДн, а также, при необходимости, применением средств активного противодействия. Конкретные требования к мерам защиты определяются по результатам специальных исследований технических средств в зависимости от класса ИСПДн, условий ее размещения и актуальных угроз безопасности ПДн.

Обеспечение безопасности ПДн при их обработке в ИСПДн осуществляется путем реализации для ИСПДн следующих мероприятий в рамках СЗПДн:

- управление доступом;
- регистрация и учет;
- обеспечение целостности;
- контроль отсутствия недекларированных возможностей;
- антивирусная защита;
- обеспечение безопасного межсетевого взаимодействия ИСПДн;
- анализ защищенности;
- обнаружение вторжений;
- криптографическая защита.

Средства защиты информации, применяемые в составе СЗПДн, в законодательно установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

Конкретный состав, характеристики и настройки технических средств защиты информации определяются на основании нормативно-методических документов ФСТЭК России исходя из класса ИСПДн и актуальных угроз безопасности ПДн.

Все технические средства защиты информации должны быть снабжены инструкциями по эксплуатации (рекомендациями по использованию).

ИСПДн 1 и 2 классов должны проходить обязательную сертификацию (аттестацию) по требованиям безопасности информации. Для ИСПДн 3 класса возможно декларирование соответствия, либо обязательная сертификация

(аттестация) по требованиям безопасности информации.

Необходимость и целесообразность применения средств криптографической защиты для обеспечения безопасности ПДн при их обработке в ИСПДн определяется на основе анализа и актуализации модели угроз безопасности ПДн. В случае принятия решения об использовании криптографических средств необходимо руководствоваться требованиями Правительства РФ и ФСБ России, изложенных в соответствующих документах.

### 2.1.2 Требования по безопасности ПДн для создаваемых (модернизируемых) ИСПДн

Обязательным требованием для вновь создаваемых и модернизируемых ИСПДн является создание в их составе СЗПДн. Работы по проектированию, созданию и внедрению СЗПДн в составе создаваемых (модернизируемых) ИСПДн осуществляются совместно подразделением технической защиты информации и подразделением ИТ.

В целях достижения оптимальной совместимости и интеграции СЗПДн в ИСПДн проектирование и создание СЗПДн должно осуществляться на основе технического (частного технического) задания совместно с проектированием ИСПДн и учитывать основные технические решения и функциональное назначение создаваемой ИСПДн.

Техническое задание на разработку СЗПДн основывается на данных о создаваемой (модернизируемой) ИСПДн, полученных в рамках предпроектного обследования, которое должно включать следующие мероприятия:

- определение перечня ПДн, подлежащих защите от несанкционированного доступа;
- определение условий расположения ИСПДн относительно границ контролируемой зоны;
- определение конфигурации и топологии ИСПДн в целом и ее отдельных компонент, физических, функциональных и технологических характеристик ИСПДн;
- определение технических средств и систем, общесистемных и прикладных программных средств в составе ИСПДн, их характеристик и условий расположения;
- определение режимов обработки ПДн в ИСПДн в целом и в отдельных компонентах: однопользовательский или многопользовательский; с разграничением прав доступа или без разграничения прав доступа пользователей;
- определение способов обработки ПДн в ИСПДн в целом и в отдельных компонентах: полностью или частично автоматизированная обработка ПДн; с передачей ПДн по внутренней сети, с передачей ПДн по сетям связи общего пользования, либо без передачи ПДн;
- определение класса ИСПДн;
- разработка частной модели угроз безопасности ПДн для специальных ИСПДн.

По результатам предпроектного обследования на основе нормативно-методического документа ФСТЭК России "Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн", с учетом установленного класса ИСПДн (либо в соответствии с частной моделью угроз) задаются конкретные требования по обеспечению безопасности ПДн, включаемые в техническое (частное техническое) задание на разработку СЗПДн.

Техническое (частное техническое) задание на разработку СЗПДн должно содержать:

- обоснование разработки СЗПДн;
- исходные данные создаваемой (модернизируемой) ИСПДн в техническом,

программном, информационном и организационном аспектах;

- класс ИСПДн;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;
- конкретизацию мероприятий и требований к СЗПДн;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации при необходимости;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

### 2.2 Действия персонала по обеспечению информационной безопасности

Обеспечение конфиденциальности ПДн, обрабатывающихся в Учреждении, является обязательным требованием для всех сотрудников Учреждения, которым ПДн стали известны, как в связи со служебной деятельностью, так и по случайности или ошибке.

Все лица, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн должны быть под роспись ознакомлены с требованиями настоящего Положения.

В Учреждении должен быть организован процесс обучения по направлению обеспечения безопасности ПДн. Обучение по данному направлению рекомендовано лицам, имеющим постоянный доступ к ПДн, и лицам, эксплуатирующим ИСПДн. В обязательном порядке обучение должны проходить лица, ответственные за эксплуатацию средств защиты информации ИСПДн.

Планы и графики обучения сотрудников Учреждении по направлению обеспечения безопасности ПДн составляются и реализуются подразделением по управлению персоналом.

В случае нарушения установленного порядка обработки ПДн работники Учреждения несут ответственность в соответствии с разделом 13 настоящего Положения.

#### 2.2.1 Предоставление работникам доступа к ПДн

Сотрудникам Учреждения предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей и в соответствии с порядком, установленным настоящим Положением и "Порядком предоставления доступа пользователей".

Сотрудники Учреждения, которые в силу выполняемых служебных обязанностей постоянно работают с ПДн, получают допуск к необходимым категориям ПДн с установленными правами доступа на срок выполнения ими соответствующих должностных обязанностей на основании Списка лиц, допущенных к работе с ПДн, который утверждается Заместителем руководителя Учреждения (Руководителем Службы безопасности) по представлению руководителей структурных подразделений Учреждения.

Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником Учреждения по согласованию с подразделением технической защиты информации в соответствии с "Порядком

предоставления доступа пользователей" путем подачи заявки на доступ с указанием цели и срока доступа и категорий ПДн, к которым запрашивается доступ.

Доступ к ПДн может быть прекращен или ограничен в случае нарушения требований настоящего Положения или "Порядком предоставления доступа пользователей", либо в случае перевода или увольнения сотрудника.

Список лиц, допущенных к работе с ПДн, должен содержать следующие поля: имя сотрудника, его должность и наименование подразделения, ФИО руководителя сотрудника (см. Приложение А к настоящему Положению).

### 2.2.2 Требования к администраторам ИСПДн и администраторам информационной безопасности ИСПДн

Квалификационные требования для администраторов ИСПДн и администраторов ИБ ИСПДн определяются подразделением по работе с персоналом совместно с подразделением по технической защите информации.

В обязанности администраторов ИСПДн входит управление учетными записями пользователей ИСПДн, поддержание штатной работы ИСПДн, обеспечение резервного копирования данных, а также установка и конфигурирование аппаратного и программного обеспечения ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн.

В обязанности администраторов ИБ ИСПДн входит обеспечение соответствия порядка обработки и обеспечения безопасности ПДн в ИСПДн требованиям по конфиденциальности, целостности и доступности ПДн, предъявляемых к конкретной ИСПДн, и общим требованиям по безопасности ПДн, установленных федеральным законодательством.

В обязанности администраторов ИБ ИСПДн также входит установка, конфигурирование и администрирование аппаратных и программных средств защиты информации ИСПДн, учет и хранение машинных носителей ПДн, периодический аудит журналов безопасности и анализ защищенности ИСПДн, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения критичных для безопасности ПДн полномочий у одного лица не рекомендуется совмещать роли администратора ИСПДн и администратора ИБ ИСПДн в лице одного сотрудника.

Квалификационные требования и детальный перечень прав и обязанностей администраторов ИСПДн и администраторов ИБ ИСПДн закрепляются в соответствующих должностных инструкциях, с которыми сотрудники, назначаемые на данные роли должны быть ознакомлены под роспись.

## 3 Основные технические решения

КСЗ ИСПДн Объекта проектируется как многоуровневая, иерархическая, масштабируемая территориально распределённая система с централизованным управлением программно-аппаратными средствами, входящими в ее состав.

КСЗ ИСПДн предназначен для реализации требований по защите ИСПДн Объекта, предъявленных в документе "Требования по защите персональных данных ИСПДн объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости". Программно-технические средства данного КСЗ ИСПДн

размещаются на территории офиса в выделенном помещении. Данные рекомендуемые программно-технические средства будут перечислены в соответствующих разделах настоящего документа.

### 3.1 Структура КСЗ ИСПДн Объекта

Перечень и назначение подсистем, входящих в состав КСЗ ИСПДн Объекта в соответствии с требованиями документа "Требования по защите персональных данных ИСПДн объекта вычислительной техники учреждения здравоохранения, социальной сферы, труда и занятости".

**Таблица 1** - Состав подсистем КСЗ ИСПДн Объекта

| N п\п | Наименование подсистемы | Назначение подсистемы |
|---|---|---|
| 1 | Подсистема управления доступом | Идентификация и проверка подлинности субъектов доступа к объектам доступа |
| 2 | Подсистема регистрации и учета | Сбор и обработка событий ИБ |
| 3 | Подсистема обеспечения целостности | Обеспечение неизменности программной среды |
| 4 | Подсистема антивирусной защиты и защиты от ПМВ | Автоматическая проверка программ и данных на наличие ВП или последствий ПМВ |
| 5 | Подсистема обнаружения вторжений | Выявление сетевых атак на ТС ИСПДн |
| 6 | Подсистема межсетевого экранирования | Сегментация и разграничение доступа в сетевой сегмент ИСПДн Объекта |
| 7 | Подсистема анализа защищенности | Выявление уязвимостей ТС ИСПДн |

### 3.2 Состав функций, реализуемых подсистемами КСЗ ИСПДн

#### 3.2.1 Подсистема управления доступом, регистрации и учета

Подсистему управления доступом, регистрации и учета Объекта рекомендуется реализовывать на базе программных средств блокирования несанкционированных действий, сигнализации и регистрации. Это специальные, не входящие в ядро какой-либо операционной системы программные и программно-аппаратные средства защиты самих операционных систем, электронных баз ПДн и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами защиты и направлены на исключение или затруднение выполнения опасных для ИСПДн действий пользователя или нарушителя. К ним относятся специальные утилиты и программные комплексы защиты, в которых реализуются функции диагностики, регистрации, уничтожения, сигнализации и имитации.

Средства диагностики осуществляют тестирование файловой системы и баз ПДн Объекта, постоянный сбор информации о функционировании элементов подсистемы обеспечения безопасности информации.

Средства уничтожения предназначены для уничтожения остаточных данных и

могут предусматривать аварийное уничтожение данных в случае угрозы НСД, которая не может быть блокирована системой защиты Объекта.

Средства сигнализации предназначены для предупреждения операторов при их обращении к защищаемым ПДн и для предупреждения администратора при обнаружении факта НСД к ПДн, искажении программных средств защиты, выходе или выводе из строя аппаратных средств защиты и о других фактах нарушения штатного режима функционирования ИСПДн Объекта.

Средства имитации моделируют работу с нарушителями при обнаружении попытки НСД к защищаемым ПДн или программным средствам. Имитация позволяет увеличить время на определение места и характера НСД, что особенно важно в территориально распределенных сетях, и дезинформировать нарушителя о месте нахождения защищаемых ПДн.

### 3.2.2 Подсистема обеспечения целостности

Подсистема обеспечения целостности реализуется преимущественно операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

### 3.2.3 Подсистема антивирусной защиты и защиты от ПМВ

Подсистема контроля отсутствия недекларированных возможностей реализуется в большинстве случае на базе систем управления базами данных, средств защиты информации, антивирусных средств защиты информации.

Для обеспечения безопасности ПДн и программно-аппаратной среды ИСПДн Объекта, обеспечивающей обработку этой информации, рекомендуется применять специальные средства антивирусной защиты, обеспечивающие:

- обнаружение и (или) блокирование деструктивных вирусных воздействий на общесистемное и прикладное программное обеспечение, реализующее обработку ПДн, а также на ПДн Объекта;
- обнаружение и удаление неизвестных вирусов;
- обеспечение самоконтроля (предотвращение инфицирования) данного антивирусного средства при его запуске.
- Средства антивирусной защиты Объекта должны удовлетворять следующим требованиям:
- совместимость указанных средств со штатным программным обеспечением ИСПДн Объекта;
- минимальная степень снижения производительности функционирования ИСПДн по основному назначению;
- наличие средств централизованного управления функционированием с рабочего места администратора безопасности информации в ИСПДн;
- возможность оперативного оповещения администратора безопасности информации в ИСПДн Объекта обо всех событиях и фактах проявления программно-математических воздействий (ПМВ);
- наличие подробной документации по эксплуатации;
- возможность осуществления периодического тестирования или

самотестирования средства;

- возможность наращивания состава средств защиты от ПМВ новыми дополнительными средствами без существенных ограничений работоспособности ИСПДн и "конфликта" с другими типами средств защиты.

### 3.2.4 Подсистема обнаружения вторжений

Подсистема обнаружения вторжений реализует следующий функционал:

- осуществление мониторинга сетевого трафика между сетевым сегментом ИСПДн Объекта и остальными сетями Заказчика с целью обнаружения признаков атак (включая сети публичного доступа);
- мониторинг сетевых атак и обнаружение вторжений на ТС, входящие в состав ИСПДн Объекта;
- оперативное оповещение ответственных лиц о попытках несанкционированного доступа к защищаемым ресурсам, подозрительной активности в сети, обнаруженных атаках и вирусах;
- централизованное управление всеми ПАК СОВ.

### 3.2.5 Подсистема межсетевого экранирования

Подсистема межсетевого экранирования реализует следующий функционал:

- сегментация и подключение сетевого сегмента ИСПДн Объекта к остальным сетям Заказчика (включая сети публичного доступа);
- защита от несанкционированного доступа (далее - НСД) в точке подключения сетевых сегментов ИСПДн Объекта к остальным сетям Заказчика (включая сети публичного доступа).

Входящие в ее состав МЭ должны отвечать следующим требованиям:

- разграничение доступа пользователей ИСПДн Объекта к объектам доступа путём фильтрации пакетов;
- межсетевое экранирование на границе с остальными сетями Заказчика (включая сети публичного доступа);
- регистрация и учет фильтруемых пакетов.
- централизованное управление МЭ;
- резервирование настроек и политик МЭ;
- архивирование событий, поступающих ПАК;
- оповещение об аппаратных и программных сбоях МЭ.

### 3.2.6 Подсистема анализа защищенности

Подсистема анализа защищенности реализует следующий функционал:

Средства анализа защищенности применяются с целью контроля настроек защиты операционных систем на рабочих станциях, серверах и коммуникационном оборудовании, и позволяют оценить возможность проведения нарушителями успешных атак.

Функционал средства анализа защищенности (САЗ) должен удовлетворять следующим требованиям:

- защита ресурсов, обрабатывающих ПДн с помощью автоматического мониторинга информационной безопасности;

- автоматизация рутинной работы персонала по выявлению вторжений на защищаемые информационные ресурсы КСЗ ИСПДн;
- автоматизация процессов инвентаризации ресурсов и управления уязвимостями, контроля изменений в КСЗ ИСПДн;
- максимальная автоматизация процессов с целью снижения трудозатрат и повышения оперативности контроля состояния защищенности КСЗ ИСПДн;
- комплексный анализ сложных систем, включая сетевое оборудование, сетевые приложения и Web-службы, входящие в состав ИСПДн;
- возможность мониторинга ИСПДн Объекта на соответствие требованиям и политикам безопасности;
- оперативное автоматическое обновление баз знаний САЗ.

### 3.3 Обеспечение заданных характеристик системы защиты

#### 3.3.1 Общие требования по защите ПДн в ИСПДн Объекта

Таблица соответствия технического решения по защите ПДн, обрабатываемых в ИСПДн Объекта, общим требованиям по защите, предъявляемых в документе "Требования по защите персональных данных ИСПДн Объекта" представлена в таблице 2.

**Таблица 2** - Таблица соответствия технического решения по защите ПДн, обрабатываемых в ИСПДн Объекта, предъявляемым к нему общим требованиям

| N п\п | Категория требования | Формулировка требования | Реализация требования |
|---|---|---|---|
| 1 | Сертификация | Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации - СЗИ, в том числе и встроенных в общесистемное и прикладное программное обеспечение - ПО), должен быть обеспечен 4 уровень контроля отсутствия в нем НДВ.<br>При необходимости применения в информационных системах обработки персональных данных средств защиты информации от несанкционированного доступа и средств межсетевого экранирования, у которых отсутствует сертификация на соответствие требованиям руководящего документа "Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей" (1999 г.), оператором по согласованию с ФСТЭК России может | |

| | | | |
|---|---|---|---|
| | | приниматься решение о применении указанных средств защиты информации в информационных системах обработки персональных данных. | |
| 2 | | Должны использоваться сертифицированные средства защиты информации. | |
| 3 | Лицензирование | Оператор данной ИСПДн должен получить лицензию на осуществление деятельности по технической защите конфиденциальной информации. | |
| 4 | Аттестация | Для данной ИСПДн требуется обязательная сертификация (аттестация) по требованиям безопасности информации. | |
| 5 | Контроль работы средств защиты информации | Должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы средств защиты информации в составе СЗПДн | |
| 6 | Документация по вопросам обеспечения безопасности ПДн | Должны быть разработаны следующие документы:<br>- Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн;<br>- Должностные инструкции персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;<br>- Рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации;<br>- В состав Руководства администратора безопасности информации должен быть включен порядок установки, настройки, конфигурирования и администрирования средств антивирусной защиты информации.<br>- Также в организационно-правовой документации Компании должны быть отражены следующие процессы:<br>- Распределение функций управления доступом к ПДн и их обработкой между должностными лицами;<br>- Порядок изменения правил доступа к защищаемой информации;<br>- Порядок изменения правил доступа к | |

| | | | |
|---|---|---|---|
| | | резервируемым информационным и аппаратным ресурсам;<br>- Порядок действия должностных лиц в случае возникновения нештатных ситуаций;<br>- Порядок проведения контрольных мероприятий и действий по его результатам. | |

### 3.3.2 Требования к подсистеме управления доступом

Таблица соответствия функциональных возможностей компонентов подсистемы управления доступом КСЗ ИСПДн Объекта требованиям, предъявляемым к ним в соответствии с документом "Требования по защите персональных данных ИСПДн Объекта" представлена в таблице 3.

**Таблица 3** - Таблица соответствия функциональных возможностей компонентов подсистемы управления доступом КСЗ ИСПДн Объекта предъявляемым требованиям

| N п\п | Формулировка требования | Реализация требования |
|---|---|---|
| 1 | Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длинной не менее шести буквенно-цифровых символов. | |
| 2 | Должна осуществляться идентификация терминалов, компьютеров, узлов сети ИСПДн, каналов связи, внешних устройств компьютеров по логическим именам. | |
| 3 | Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам. | |
| 4 | Должны быть реализованы механизмы блокирования терминала субъекта доступа самим субъектом доступа или в случае истечения заданного интервала времени неактивности субъекта доступа. | |
| 5 | Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа. | |
| 6 | Для каждого субъекта доступа должен быть определен перечень исполняемых модулей, которые он может активизировать. | |
| 7 | Импорт и экспорт объектов (сообщений, данных, программ и т.п.) должен выполняться субъектом доступа со специальной ролью "оператора ввода/вывода. | |

### 3.3.3 Требования к подсистеме регистрации и учета

Таблица соответствия функциональных возможностей компонентов подсистемы регистрации и учета КСЗ ИСПДн Объекта требованиям, предъявляемым к ним в соответствии с документом "Требования по защите персональных данных ИСПДн Объекта"представлена в таблице 4.

**Таблица 4** - Таблица соответствия функциональных возможностей компонентов подсистемы регистрации и учета КСЗ ИСПДн Объекта предъявляемым требованиям

| N п\п | Формулировка требования | Реализация требования |
|---|---|---|
| 1 | Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная - несанкционированная), идентификатор (код, или фамилия) субъекта, предъявленный при попытке доступа; | |
| 2 | Должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к экспортируемым/импортируемым файлам, содержащим ПДн. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная - несанкционированная), идентификатор субъекта доступа, спецификация защищаемого файла. | |
| 3 | Должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная - несанкционированная), идентификатор субъекта доступа, спецификация защищаемого объекта - логическое имя (номер); | |
| 4 | Должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами ИСПДн с указанием на последнем листе документа общего количества | |

| | | |
|---|---|---|
| | листов (страниц). В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код, шифр), спецификация устройства выдачи - логическое имя (номер) внешнего устройства. | |
| 5 | Должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются дата и время изменения полномочий, идентификатор субъекта доступа (администратора), осуществившего изменения. | |
| 6 | Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнала (учетную карточку); | |
| 7 | Должен проводиться учет защищаемых носителей в журнале (картотеке) с регистрацией их выдачи (приема) | |
| 8 | Должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации | |
| 9 | Данные регистрации должны быть защищены от их уничтожения или модификации нарушителем. | |
| 10 | Должны быть реализованы механизмы просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров | |
| 11 | Должна осуществляться сигнализация попыток нарушения защиты. | |

### 3.3.4 Требования к подсистеме обеспечения целостности

Таблица соответствия функциональных возможностей компонентов подсистемы обеспечения целостности КСЗ ИСПДн Объекта требованиям, предъявляемым к ним в соответствии с документом "Требования по защите персональных данных ИСПДн Объекта" представлена в Таблице 5.

**Таблица 5** - Таблица соответствия функциональных возможностей компонентов подсистемы обеспечения целостности КСЗ ИСПДн Объекта предъявляемым требованиям

| N п\п | Формулировка требования | Реализация требования |
|---|---|---|
| 1 | Должна быть обеспечена целостность программных средств защиты информации в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по контрольным суммам компонент средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации | |

| | | |
|---|---|---|
| 2 | Должна осуществляться физическая охрана ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации, особенно в нерабочее время. | |
| 3 | Должны быть в наличии средства восстановления средств защиты информации в составе СЗПДн, предусматривающие ведение двух копий программных средств защиты, их периодическое обновление и контроль работоспособности. | |
| 4 | Должно проводиться периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест - программ, имитирующих попытки НСД | |
| 5 | Должно проводиться резервное копирование ПДн на отчуждаемые носители информации. | |

### 3.3.5 Требования к подсистеме антивирусной защиты и защиты от ПМВ

Таблица соответствия функциональных возможностей компонентов подсистемы антивирусной защиты и защиты от ПМВ КСЗ ИСПДн Объекта требованиям, предъявляемым к ним в соответствии с документом "Требования по защите персональных данных ИСПДн Объекта" представлена в таблице 6.

**Таблица 6** - Таблица соответствия функциональных возможностей компонентов подсистемы антивирусной защиты и защиты от ПМВ КСЗ ИСПДн Объекта предъявляемым требованиям

| N п\п | Формулировка требования | Реализация требования |
|---|---|---|
| 1 | Должна проводиться автоматическая проверка на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа | |
| 2 | Должны быть реализованы механизмы автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения | |
| 3 | Должна регулярно выполняться проверка на предмет наличия ВП в средствах защиты от ПМВ (при первом запуске средства защиты от ПМВ и с устанавливаемой периодичностью) | |
| 4 | Факт выявления ПМВ должен инициировать автоматическую проверку на предмет наличия ВП | |
| 5 | Должен быть реализован механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных | |

| | | |
|---|---|---|
| | модулей и прикладных программ или программных средств, содержащих ВП | |
| 6 | На всех технических средствах ИСПДн должен проводиться непрерывный согласованный по единому сценарию автоматический мониторинг информационного обмена в ИСПДн с целью выявления проявлений ПМВ | |

### 3.3.6 Требования к подсистеме межсетевого экранирования

Соответствие функциональных возможностей компонентов подсистемы межсетевого экранирования КСЗ ИСПДн Объекта требованиям, предъявляемым к ним в соответствии с документом "Требования по защите персональных данных ИСПДн Объекта" представлены в таблице 7.

**Таблица 7** - Таблица соответствия функционала компонентов подсистемы межсетевого экранирования КСЗ ИСПДн Объекта предъявляемым к ним требованиям

| N п\п | Категория требования | Формулировка требования | Реализация требования |
|---|---|---|---|
| **Общие требования к МЭ** | | | |
| 1 | В ИСПДн должны использоваться МЭ не ниже третьего уровня защищенности | | Сертификат соответствия ФСТЭК России N_____ от _____ по 3 классу защищённости МЭ и соответствие ТУ. Схема сертификации - партия. |
| **МЭ должен обеспечивать:** | | | |
| 2 | Управление доступом (фильтрация данных и трансляция адресов) | МЭ должен обеспечивать следующие функции по фильтрации на сетевом уровне:<br>- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств; | Сертификат соответствия МЭ N ____ требованиям руководящего документа "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" подтверждает соответствие данной категории требований функциональным возможностям МЭ. |
| | | - фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов; | |
| | | - фильтрацию с учетом любых значимых полей сетевых пакетов. | |
| | | - фильтрацию на | |

| | | | |
|---|---|---|---|
| | | транспортном уровне запросов на установление виртуальных соединений. При этом, по крайней мере, учитываются транспортные адреса отправителя и получателя; | |
| | | - фильтрацию на прикладном уровне запросов к прикладным сервисам. При этом, по крайней мере, учитываются прикладные адреса отправителя и получателя; | |
| | | - фильтрацию с учетом даты/времени. | |
| 3 | Идентификация и аутентификация | МЭ должен обеспечивать возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети. | Сертификат соответствия МЭ N ____ требованиям руководящего документа "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" подтверждает соответствие данной категории требований функциональным возможностям МЭ. |
| 4 | Регистрация | МЭ должен обеспечивать возможность регистрации и учета фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации. | |
| | | МЭ должен обеспечивать: регистрацию и учет запросов на установление виртуальных соединений; | |
| | | локальную сигнализацию попыток нарушения правил фильтрации. | |
| 5 | Администрирование: идентификация и аутентификация | МЭ должен обеспечивать: Идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ; | Сертификат соответствия МЭ N ____ требованиям руководящего документа "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" подтверждает |
| | | МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия; | |
| | | МЭ должен препятствовать | |

| | | | |
|---|---|---|---|
| | | доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась;<br>При удаленных запросах администратора МЭ на доступ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации. | соответствие данной категории требований функциональным возможностям МЭ. |
| 6 | Администрирование: регистрация | МЭ должен обеспечивать: регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузка и инициализация системы и ее программный останов. (Регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ);<br>- регистрацию запуска программ и процессов (заданий, задач);<br>- регистрацию действия администратора МЭ по изменению правил фильтрации. | Сертификат соответствия МЭ N ____ требованиям руководящего документа "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" подтверждает соответствие данной категории требований функциональным возможностям МЭ. |
| 7 | Администрирование: простота использования | Многокомпонентный МЭ должен обеспечивать возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации. | Сертификат соответствия МЭ N ____ требованиям руководящего документа "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" подтверждает соответствие данного требования функциональным |

| | | | |
|---|---|---|---|
| | | | возможностям МЭ. |
| 8 | Целостность | МЭ должен обеспечивать контроль целостности своей программной и информационной части, по контрольным суммам. | Сертификат соответствия МЭ N ____ требованиям руководящего документа "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" подтверждает соответствие данного требования функциональным возможностям МЭ. |
| 9 | Восстановление | МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ. | Сертификат соответствия МЭ N ____ требованиям руководящего документа "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" подтверждает соответствие данного требования функциональным возможностям МЭ. |
| 10 | Тестирование | В МЭ должна обеспечиваться возможность регламентного тестирования: реализации правил фильтрации; | Сертификат соответствия МЭ N ____ требованиям руководящего документа "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" |
| | | процесса регистрации; | |
| | | процесса идентификации и аутентификации запросов; | |
| | | процесса идентификации и аутентификации администратора МЭ; | |
| | | процесса регистрации действий администратора | |

| | | | |
|---|---|---|---|
| | | МЭ; | подтверждает соответствие данной категории требований функциональным возможностям МЭ. |
| | | процесса контроля за целостностью программной и информационной части МЭ; | |
| | | процедуры восстановления. | |

### 3.3.7 Требования к подсистеме обнаружения вторжений

Таблица соответствия функциональных возможностей компонентов подсистемы обнаружения вторжений КСЗ ИСПДн Объекта требованиям, предъявляемым к ним в соответствии с документом "Требования по защите персональных данных ИСПДн Объекта" представлена в таблице 7.

ГАРАНТ:

По-видимому, в тексте предыдущего абзаца допущена опечатка. Имеется в виду таблица 8

**Таблица 8** - Таблица соответствия функционала компонентов подсистемы обнаружения вторжений КСЗ ИСПДн Объекта предъявляемым к ним требованиям

| N п\п | Формулировка требования | Реализация требования |
|---|---|---|
| 1 | Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений, использующие сигнатурные методы анализа, а также методы выявления аномалий. | В состав подсистемы обнаружения вторжений КСЗ ИСПДн Объекта входит ПАК СОВ _____, заявленный функционал которого подтвержден сертификатом соответствия ФСТЭК России N ____ от __.__.____ заявленным техническим условиям. |

### 3.3.8 Требования к подсистеме анализа защищенности

Таблица соответствия функциональных возможностей компонентов подсистемы анализа защищенности КСЗ ИСПДн Объекта требованиям, предъявляемым к ним в соответствии с документом "Требования по защите персональных данных ИСПДн Объекта" представлена в таблице 8.

ГАРАНТ:

По-видимому, в тексте предыдущего абзаца допущена опечатка. Имеется в виду таблица 9

**Таблица 9** - Таблица соответствия функционала компонентов подсистемы анализа защищенности КСЗ ИСПДн Объекта предъявляемым к ним требованиям

| N п\п | Формулировка требования | Реализация требования |
|---|---|---|
| 1 | Анализ защищенности должен проводиться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) анализа защищенности (далее - САЗ). | |
| 2 | Для ИСПДн САЗ должна быть обеспечена возможность выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему. | |

## 4 Описание организационной структуры КСЗ ИСПДн Объекта

### 4.1 Роли персонала по обеспечению функционирования КСЗ ИСПДн Объекта

Для обеспечения администрирования, сопровождения и эксплуатации компонентов КСЗ ИСПДн Объекта из состава сотрудников Заказчика должны быть назначены администраторы КСЗ ИСПДн Объекта, выполняющие следующие функции:

- управление настройками и конфигурацией оборудования КСЗ ИСПДН ОБЪЕКТА;
- внесение согласованных с администратором информационной безопасности изменений в настройки компонентов КСЗ ИСПДН ОБЪЕКТА;
- мониторинг событий КСЗ ИСПДН ОБЪЕКТА, принятие мер по нейтрализации инцидентов информационной безопасности;
- контроль работоспособности оборудования и соблюдения условий эксплуатации (температура, влажность, напряжение электросети);
- отключение оборудования в случаях нарушения условий эксплуатации, пожара, стихийных бедствий;
- принятие мер по восстановлению работоспособности КСЗ ИСПДН ОБЪЕКТА в случае сбоев;
- периодическое резервное копирование конфигурационных файлов компонентов КСЗ ИСПДН ОБЪЕКТА;
- проведение регламентных работ по поддержанию работоспособности КСЗ ИСПДН ОБЪЕКТА;
- подготовка отчетов о функционировании КСЗ ИСПДН ОБЪЕКТА.

Администраторы КСЗ ИСПДН ОБЪЕКТА не должны иметь полномочий по управлению журналами аудита (изменению состава регистрируемых событий, очистке журналов).

Администраторы КСЗ ИСПДН ОБЪЕКТА должны обладать следующей квалификацией:

- навыки настройки и администрирования используемых средств диагностики, регистрации, уничтожения, сигнализации и имитации, подтвержденные сертификатом об обучении в специализированном учебном центре;

- навыки настройки и администрирования используемых операционных систем и систем управления базами данных, подтвержденные сертификатом об обучении в специализированном учебном центре;

- навыки настройки и администрирования используемых антивирусных средств, подтвержденные сертификатом об обучении в специализированном учебном центре;

- навыки настройки и администрирования используемых МЭ, подтвержденные сертификатом об обучении в специализированном учебном центре;

- навыки настройки и администрирования используемых СОВ, подтвержденные сертификатом об обучении в специализированном учебном центре;

- навыки настройки и администрирования используемых САЗ, подтвержденные сертификатом об обучении в специализированном учебном центре.

Рекомендуется следующий состав администраторов КСЗ ИСПДН ОБЪЕКТА:

- 2 администратора для поддержки и обслуживания КСЗ ИСПДН ОБЪЕКТА (график работы: 5 дней в неделю в рабочее время);

- 2 дежурных администратора для мониторинга, поддержки КСЗ ИСПДН ОБЪЕКТА и срочного устранения возникающих неисправностей (график работы: сутки через двое).

Для обеспечения контроля соблюдения политики безопасности и контроля за действиями администраторов КСЗ ИСПДН ОБЪЕКТА из состава сотрудников Заказчика быть назначены администраторы информационной безопасности (далее - АИБ), выполняющие следующие функции:

- контроль действий администраторов КСЗ ИСПДН ОБЪЕКТА в части:

а) соблюдения технологии эксплуатации ТС КСЗ ИСПДН ОБЪЕКТА;

б) обоснованности внесения изменений в конфигурационные настройки и параметры компонентов КСЗ ИСПДН ОБЪЕКТА;

- анализ и согласование изменений конфигурационных настроек и параметров компонентов КСЗ ИСПДН ОБЪЕКТА с точки зрения соответствия требованиям защиты информации и ресурсов защищаемых ИСПДн РОСНО;

- анализ журналов регистраций КСЗ ИСПДН ОБЪЕКТА с целью установления и предотвращения попыток НСД к информации и информационным ресурсам защищаемых ИСПДн;

- организация расследований инцидентов информационной безопасности, участие в проведении расследований;

- архивирование журналов аудита;

- фиксация результатов своей работы и подготовка регулярных отчетов.

АИБ не должен иметь полномочий по внесению изменений в конфигурационные настройки и параметры ТС КСЗ ИСПДН ОБЪЕКТА.

Администраторы информационной безопасности должны обладать следующей квалификацией:

- навыки настройки и администрирования используемых средств диагностики, регистрации, уничтожения, сигнализации и имитации, подтвержденные сертификатом об обучении в специализированном учебном центре;

- навыки настройки и администрирования используемых операционных систем и систем управления базами данных, подтвержденные сертификатом об обучении в специализированном учебном центре;

- навыки настройки и администрирования используемых антивирусных средств, подтвержденные сертификатом об обучении в специализированном учебном центре;

- навыки настройки и администрирования используемых МЭ, подтвержденные сертификатом об обучении в специализированном учебном центре;

- навыки настройки и администрирования используемых СОВ, подтвержденные

сертификатом об обучении в специализированном учебном центре;

- навыки настройки и администрирования используемых САЗ, подтвержденные сертификатом об обучении в специализированном учебном центре.

Рекомендуется следующий состав администраторов информационной безопасности КСЗ ИСПДН ОБЪЕКТА:

- 2 администратора информационной безопасности (график работы: 5 дней в неделю в рабочее время).

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 24**

**Положение**
**об Электронном журнале обращений пользователей информационных систем персональных данных учреждений здравоохранения, социальной сферы, труда и занятости (проект приказа)**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |
| _____ | _____ подпись, дата | _____ |

Москва 2009

**ПРИКАЗ**

"___" _____ 20__ г. г. _____ N_____

О проведении работ по защите персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости

В целях исполнения Федерального закона N 152-ФЗ от 27 июля 2006 года "О персональных данных" в учреждениях здравоохранения, социальной сферы, труда и занятости:

ПРИКАЗЫВАЮ:

1) Организовать ведение Журнала обращений пользователей информационных систем обработки персональных данных к персональным данным.

2) Журнал вести в электронном виде.

3) Контроль за исполнением настоящего приказа возложить на_____.

ФИО _____ (_____)
(подпись) (ФИО)

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ
_____
_____
"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 25**

**Уведомление**
**об обработке персональных данных**

СОГЛАСОВАНО

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

Москва 2009

Руководителю Управления Федеральной
службы по надзору в сфере связи
и массовых коммуникаций по
_____
_____

Уведомление об обработке (о намерении осуществлять обработку) персональных данных

_____
_____

(наименование (фамилия, имя, отчество), адрес оператора)

руководствуясь _____
___

(правовое основание обработки персональных данных)

с целью
_____

(цель обработки персональных данных)

осуществляет
обработку: _____

_____

(категории персональных данных)

принадлежащих: _____
____

_____

(категории субъектов, персональные данные которых обрабатываются)

Обработка вышеуказанных персональных данных будет осуществляться путем:

_____

_____

(Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных)

_____

_____

(Описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке)

Дата начала обработки персональных данных: _____

Срок или условие прекращения обработки персональных данных: _____

_____

(должность) (подпись) расшифровка подписи

"___" _____ 200_ г.

**Министерство здравоохранения и социального развития Российской Федерации**

УТВЕРЖДАЮ

_____

_____

"__" _____ 2009 г.

**Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости**

**Приложение 26**

**Рекомендации**
**по заполнению Уведомления об обработке**

СОГЛАСОВАНО

| | | |
|---|---|---|
| _____ | _____<br>подпись, дата | _____ |
| _____ | _____<br>подпись, дата | _____ |
| _____ | _____<br>подпись, дата | _____ |

Москва 2009

1. Настоящие Рекомендации разработаны в целях установления единых принципов и порядка заполнения уведомления об обработке (о намерении осуществлять обработку) персональных данных (далее - Уведомление).

2. Уведомление оформляется на бланке оператора, осуществляющего обработку персональных данных, и направляется в территориальный орган Федеральной службы по надзору в сфере связи и массовых коммуникаций (далее - территориальный орган Россвязькомнадзора).

3. Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации.

4. В поле "наименование (фамилия, имя, отчество), адрес оператора" указывается:

4.1. Для юридических лиц (операторов):

- полное наименование с указанием организационно-правовой формы и сокращенное наименование юридического лица (оператора), осуществляющего обработку персональных данных;
- наименование филиала(ов) (представительства(в) юридического лица (оператора), осуществляющего обработку персональных данных*(1);
- место нахождения*(2);

**Примечание 1.** Если для каких-либо операторов (с учетом филиалов (представительств) значения пунктов 5-12 отличаются, то для них формируется отдельное уведомление.

**Примечание 2.** Для организаций, учреждений, имеющих филиалы (представительства), указываются юридический и фактический адрес (как юридического лица, так и его филиалов и представительств), где осуществляется непосредственная обработка персональных данных (все действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных). При этом, необходимо уточнить - обработка персональных данных осуществляется только юридическим лицом (формирование центральной информационной системы) и (или) филиалами (представительствами).

- индивидуальный номер налогоплательщика (ИНН),

4.2. Для физических лиц:

- фамилия, имя, отчество физического лица (оператора); место жительства*(3);
- данные документа, удостоверяющего личность, дата его выдачи, наименование органа, выдавшего документ, удостоверяющий личность.

4.3. Для индивидуальных предпринимателей:
- фамилия, имя, отчество индивидуального предпринимателя (оператора);
- место жительства*(4);
- индивидуальный номер налогоплательщика (ИНН).

4.4. Для государственных, муниципальных органов (операторов):
- полное и сокращенное наименование государственного, муниципального органа;
- наименование территориального(ых) органа(ов), осуществляющего(их) обработку
- персональных данных;
- место нахождения*(5);
- индивидуальный номер налогоплательщика (ИНН).

При указании наименования (фамилии, имени, отчества), адреса оператора, а также направления деятельности рекомендуется использовать также ссылки на код(ы) классификаторов (ОКВЭД, ОКПО, ОКОГУ, ОКОП, ОКФС).

5. В поле "цель обработки персональных данных" указываются цели обработки персональных данных (а также их соответствие полномочиям оператора) (Примечание N 1).

**Примечание N 1:** Под "целью обработки персональных данных" понимаются, как цели, указанные в учредительных документах оператора, так и цели фактически осуществляемой оператором деятельности по обработке персональных данных.

6. В поле "категории персональных данных" указываются все категории персональных данных, подлежащих обработке:

6.1. Персональные данные (любая информация, относящаяся к определенному или определяемому на основе такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата рождения, место рождение, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая необходимая информация).

6.2. Специальные категории персональных данных (расовая принадлежность, национальная принадлежность, политические взгляды, религиозные убеждения, философские убеждения, состояние здоровья, состояние интимной жизни).

6.3. Биометрические персональные данные (сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность).

7. В поле "категории субъектов, персональные данные которых обрабатываются" указываются категории субъектов (физических лиц) и виды отношений с субъектами (физическими лицами), персональные данные которых обрабатываются. Например: работники (субъекты), состоящие в трудовых отношениях с юридическим лицом (оператором), физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.) (субъекты), состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором) и др.

8. В поле "правовое основание обработки персональных данных" указываются:
- Федеральный закон, постановление Правительства Российской Федерации, иной нормативно-правовой акт, закрепляющий основание и порядок обработки персональных данных (Примечание N 1).

- Номер, дату выдачи и наименование лицензии на осуществляемый вид деятельности, с указанием лицензионных условий, закрепляющих запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных (Примечание N 2).

**Примечание N 1:** Указываются не только соответствующие статьи Федерального закона "О персональных данных", но и статьи иного нормативно-правового акта, регулирующие осуществляемый вид деятельности и касающиеся обработки персональных данных. (Например: ст.ст. 85-90 Трудового кодекса РФ, ст. 85.1 Воздушного кодекса РФ, ст. 12 Федерального закона "Об актах гражданского состояния" и др.).

**Примечание N 2:** Номер лицензии и пункт лицензионных условий, закрепляющий запрет на передачу персональных данных (или информации, касающейся физических лиц), отражается только при наличии лицензии и (или) соответствующего пункта лицензионных условий.

9. В поле "перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных", указываются действия, совершаемые оператором с персональными данными, а также описание используемых оператором способов обработки персональных данных:

- неавтоматизированная обработка персональных данных;
- исключительно автоматизированная обработка персональных данных с передачей полученной информации по сети или без таковой;
- смешанная обработка персональных данных. (Примечание N 1).

**Примечание N 1:** При автоматизированной обработке персональных данных либо смешанной обработке, необходимо указать, передается ли полученная в ходе обработки персональных данных информация по внутренней сети юридического лица (информация доступна лишь для строго определенных сотрудников юридического лица) либо информация передается с использованием сети общего пользования Интернет либо без передачи полученной информации.

10. В поле "описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке", указываются организационные и технические меры, в том числе использование шифровальных (криптографических) средств, используемых для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий при их обработке.

11. В поле "дата начала обработки персональных данных" указывается конкретная дата начала совершения действий с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных (фактическая дата начала обработки персональных данных).

12. В поле "срок или условие прекращения обработки персональных данных" указывается конкретная дата или основание (условие), наступление которого повлечет прекращение обработки персональных данных.

---

*(1) Для юридических лиц с филиальной структурой указывается список субъектов Российской Федерации (с указанием кода субъекта - согласно справочнику "Коды регионов", утвержденному приказом ФНС России от 13.10.2006 года N САЭ-3-04/706@ "Об утверждении формы сведений о доходах физических лиц" зарегистрированным Министерством юстиции Российской Федерации 17.11.2000 г., регистрационный номер 8507), на территории которых находятся филиалы (представительства) юридического лица и (или) где оператором производится обработка персональных данных. Уведомление направляется юридическим лицом в соответствующее территориальное управление Россвязькомнадзора по месту своего нахождения с указанием всех имеющихся филиалов (представительств) (Примечание N 1)

*(2) Указывается место нахождения юридического лица в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, а также место нахождения филиала(ов) (представительств) юридического лица, контактная информация (Примечание N 2).

*(3) Указывается место жительства физического лица в соответствии с данными документа, удостоверяющего личность, а в случае расхождения, также фактическое место жительство, контактная информация

*(4) Указывается место жительства индивидуального предпринимателя (оператора) в соответствии с данными документа, удостоверяющего личность, и свидетельством о постановке индивидуального предпринимателя на учет в налоговом органе, контактная информация.

*(5) Указывается место нахождения государственного, муниципального органа в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, контактная информация.