Министерство здравоохранения и социального развития
Российской Федерации

СОГЛАСОВАНО

Начальник 2 управления
ФСТЭК России

_____ А.В. Куц
«22» декабря 2009 г.

УТВЕРЖДАЮ

Директор Департамента
информатизации Министерства
здравоохранения и социального
развития Российской Федерации

_____ О.В. Симаков
«23» декабря 2009 г.

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

Москва 2009

Список исполнителей

Руководитель проекта _____ Пономарев Т.М.

подпись, дата

Исполнители:

Консультант-аналитик _____ Дудко Д.О.

подпись, дата

Технический писатель _____ Чернышова М.В.

подпись, дата

СОДЕРЖАНИЕ

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 неограни-

ченного 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. № 152-ФЗ «О персональных данных» и принятых во исполнение его положений, нормативно-правовых актов и методических документов.

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. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 17 ноября 2007 г. № 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).

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 пересмот-

рен 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. 69). 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. 85).

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 – $Х_{пд}$. Определяются следующие категории обрабатываемых в информационной системе персональных данных ($Х_{пд}$):

- 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 уста-

новить 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 Зако-

ном, 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 Приказ 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.

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 тре-

бование 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 ($Х_{ПД}$) (см. раздел 4 на стр. 24).

9) Должен быть определен объем записей персональных данных ($Х_{ПДН}$). 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.

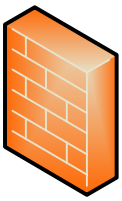
При составлении конфигурации могут использоваться следующие условные обозначения:

– Группа пользователей ИСПДн.

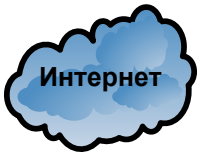
– АРМ пользователей ИСПДн.

– 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.

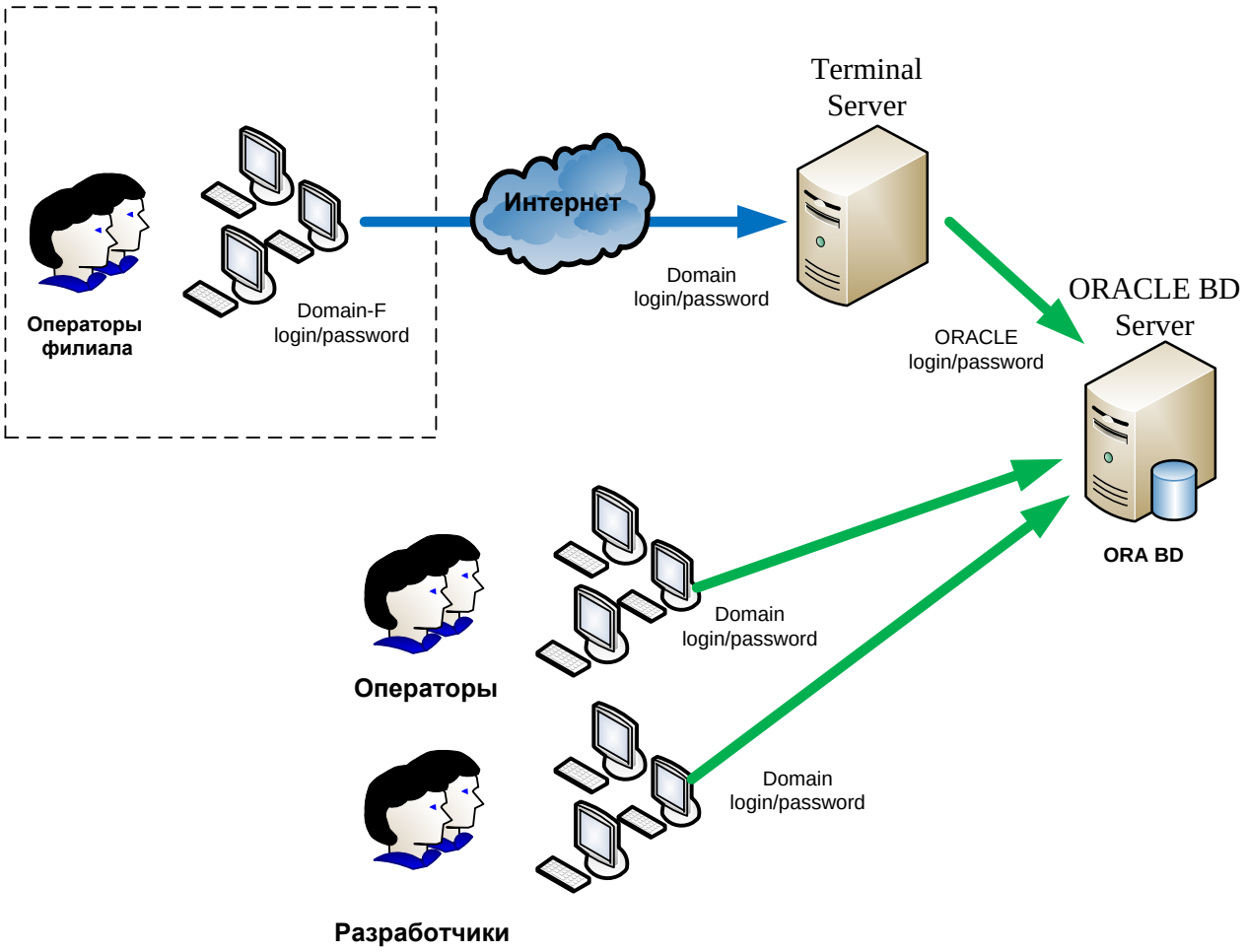


Рисунок 1

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.

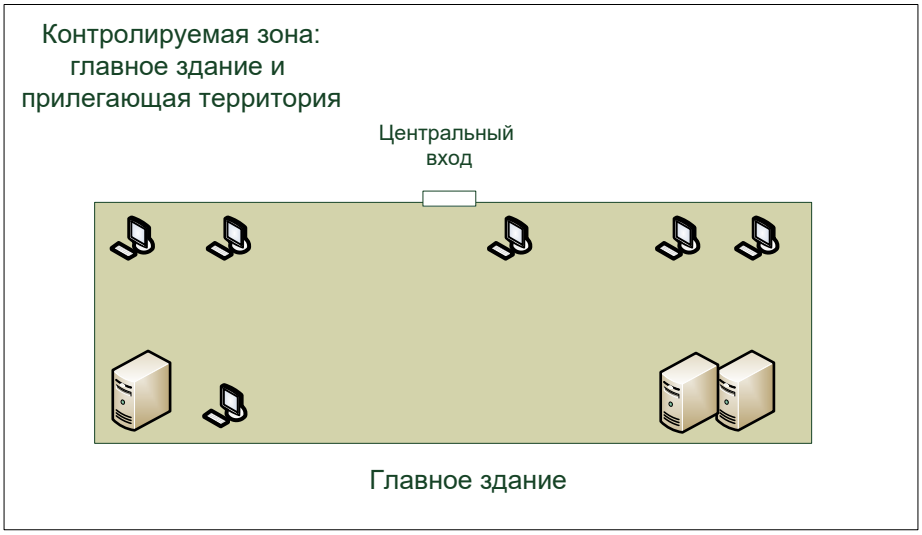


Рисунок 2

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 действия	Сотрудники отдела
Администраторы ИСПДн	Обладают полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладают полной информацией о технических средствах и конфигурации ИСПДн. Имеют доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладают правами конфигурирования и административной настройки технических средств ИСПДн.	– сбор – систематизация – накопление – хранение – уточнение – использование – уничтожение	Отдел информационных технологий
Администратор безопасности	Обладает правами Администратора ИСПДн. Обладает полной информацией об ИСПДн.	– сбор – систематизация – накопление – хранение – уточнение – использование	Петров П.П.

	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).	– уничтожение	
Операторы ИСПДн с правами записи	Обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	– сбор – систематизация – накопление – хранение – уточнение – использование – уничтожение	Отдел регистратуры
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 Браузер	Средства ОС: - управление и разграничение доступа пользователей; - регистрация и учет действий с информацией. Антивирус НАЗВАНИЕ - регистрация и учет действий с информацией; - обеспечение целостности данных; - обнаружение вторжений.
АРМ администратора	ОС Windows XP Клиент приложения	Средства ОС: - управление и разграничение доступа пользователей; - регистрация и учет действий с информацией. Антивирус НАЗВАНИЕ - регистрация и учет действий с информацией; - обеспечение целостности данных; - обнаружение вторжений.
Сервер приложений	OS Windows Server 2007	Средства ОС: - управление и разграничение доступа пользователей; - регистрация и учет действий с информацией; - обеспечение целостности данных. Антивирус НАЗВАНИЕ - регистрация и учет действий с информацией;

		- обеспечение целостности данных; - производить обнаружений вторжений.
СУБД	БД ORACLE	Средства БД Средства ОС: - управление и разграничение доступа пользователей; - регистрация и учет действий с информацией; - обеспечение целостности данных. - обнаружение вторжений.
Граница ЛВС		Межсетевой экран: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией; - обеспечение целостности данных. - обнаружение вторжений.
Каналы передачи		СКЗИ НАЗВАНИЕ Средства СКЗИ: - управление и разграничение доступа пользователей; - регистрация и учет действий с информацией; - 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 ($Х_{ПД}$).** Определяется исходя из особенностей персональных данных, порядок категорирования которых описан в разделе 4.

- Должен быть определен объем записей персональных данных ($Х_{ПДН}$). 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 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 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 про-

граммных 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 ($Х_{ПД}$) (см. раздел 4).

8) Должно быть определен объем записей персональных данных ($Х_{ПДН}$). 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.

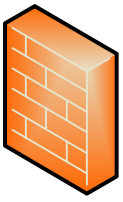
При составлении конфигурации могут использоваться следующие условные обозначения:

– Группа пользователей ИСПДн.

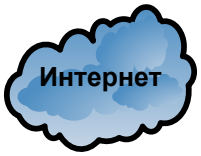
– АРМ пользователей ИСПДн.

– 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.

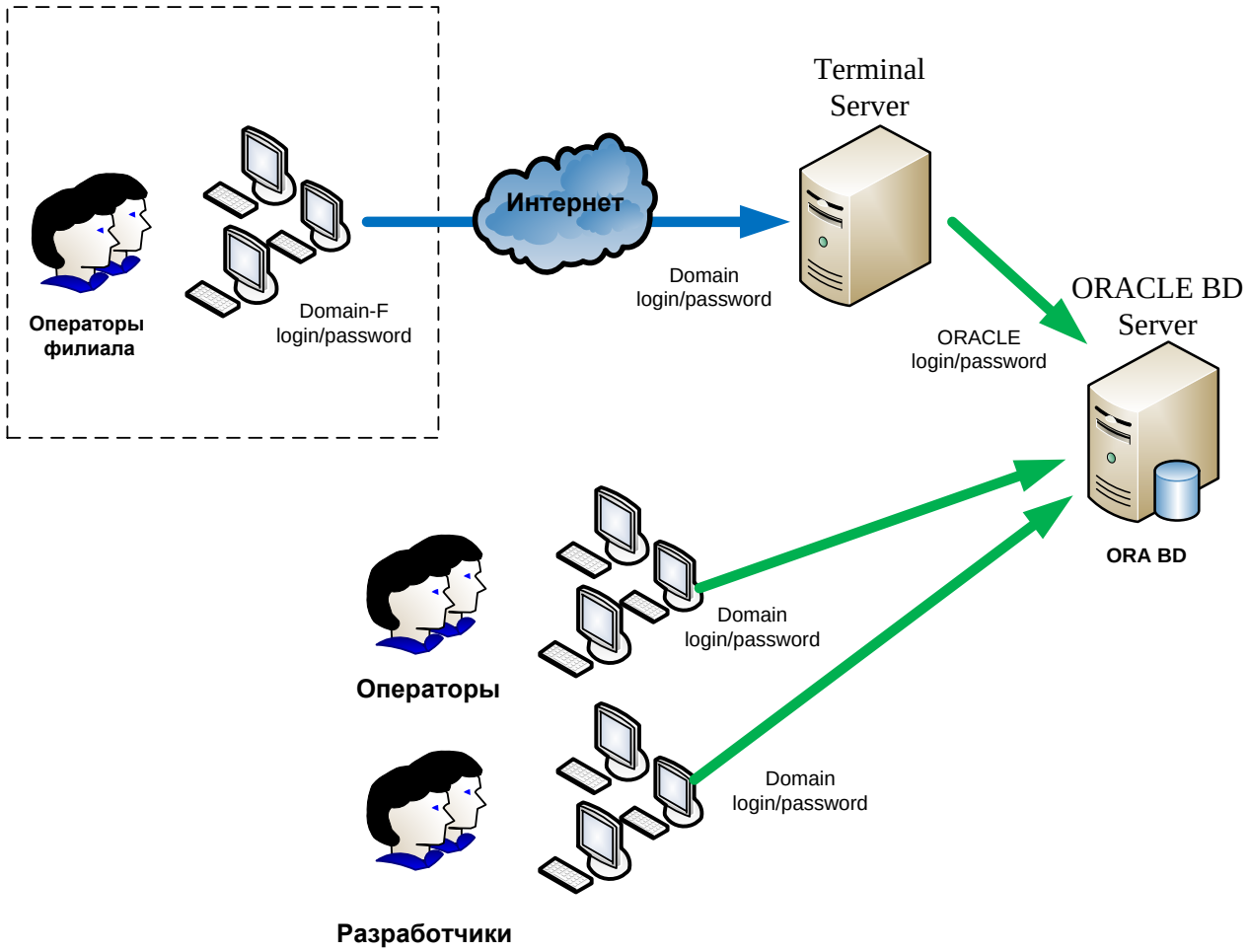


Рисунок 3

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.

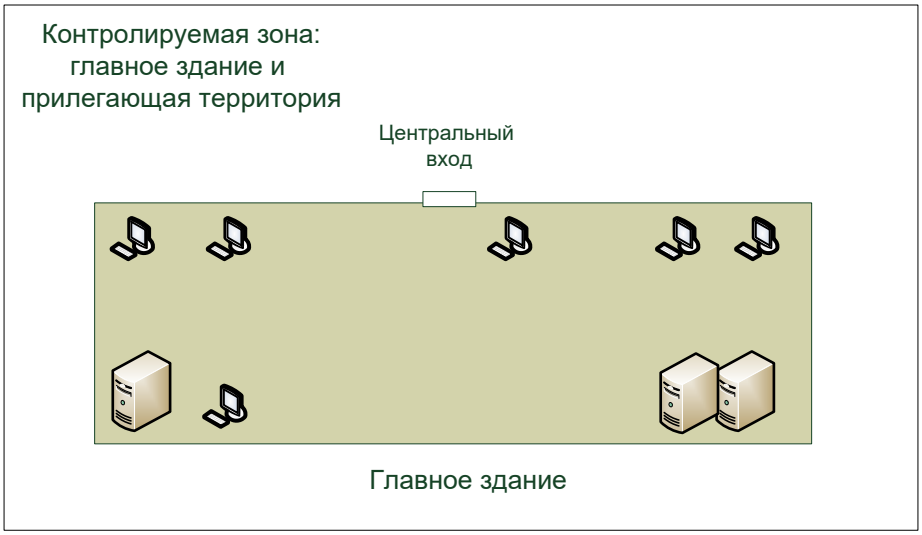


Рисунок 4

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	Разрешенные	Сотрудники отдела

	ПДн	действия	
Администраторы ИСПДн	Обладают полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладают полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладают правами конфигурирования и административной настройки технических средств ИСПДн.	– сбор – систематизация – накопление – хранение – уточнение – использование – уничтожение	Отдел информационных технологий
Администратор безопасности	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	– сбор – систематизация – накопление – хранение – уточнение – использование – уничтожение	Петров П.П.

	контрольных (инспекционных).		
Операторы ИСПДн с правами записи	Обладают всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	– сбор – систематизация – накопление – хранение – уточнение – использование – уничтожение	Отдел регистратуры
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. № 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 срок до 01.01.2010 г.	
Определение перечня ИСПДн	Разовое срок до	
Определение обрабатываемых ПДн и объектов защиты	Разовое срок до	
Определение круга лиц участвующих в обработке ПДн	Разовое срок до	
Определение ответственности лиц участвующих в обработке	Разовое срок до	
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое срок до	
Назначение ответственного за безопас-	Разовое	

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

Разработка инструкций о действии в случае возникновения внештатных ситуаций	Разовое срок до	
Разработка положения о внесении изменения в штатное программное обеспечение элементов ИСПДн	Разовое срок до	
Разработка положения о порядке внесения изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями. Положение должно включать в себя техническое задание на изменения, технический проект, приемо-сдаточные испытания, акт о введении в эксплуатацию.	Разовое срок до	
Организация журнала учета обращений субъектов ПДн	Разовое срок до	
Организация перечня по учету технических средств и средств защиты, а так же документации к ним	Разовое срок до	
Физические мероприятия		
Организация постов охраны для пропуска в контролируемую зону	Разовое срок до	
Внедрение технической системы контроля доступа в контролируемую зону и помещения (по электронным пропускам, токену, биометрическим данным и т.п.)	Разовое срок до	
Внедрение технической системы контроля доступа к элементам ИСПДн (по электронным пропускам, токену, биометрическим данным и т.п.)	Разовое срок до	
Внедрение видеонаблюдения	Разовое срок до	
Установка дверей на входе в помещения с аппаратными средствами ИСПДн	Разовое срок до	
Установка замков на дверях в помещениях с аппаратными средствами ИСПДн	Разовое срок до	
Установка жалюзи на окнах	Разовое срок до	
Установка решеток на окнах первого и последнего этажа здания	Разовое срок до	
Установка системы пожаротушения в	Разовое	

помещениях, где расположены элементы ИСПДн	срок до	
Установка систем кондиционирования в помещениях, где расположены аппаратные средства ИСПДн	Разовое срок до	
Установка систем бесперебойного питания на ключевые элементы ИСПДн	Разовое срок до	
Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн	Разовое срок до	
Технические (аппаратные и программные) мероприятия		
Внедрение единого хранилища зарегистрированных действий пользователей с ПДн	Разовое срок до	
Внедрение специальной подсистемы управления доступом, регистрации и учета (НАЗВАНИЕ)	Разовое срок до	
Внедрение антивирусной защиты (НАЗВАНИЕ)	Разовое срок до	
Внедрение межсетевого экранирования (НАЗВАНИЕ)	Разовое срок до	
Внедрение подсистемы анализа защищенности (НАЗВАНИЕ)	Разовое срок до	
Внедрение подсистемы обнаружения вторжений (НАЗВАНИЕ)	Разовое срок до	
Внедрение криптографической защиты (НАЗВАНИЕ)	Разовое 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 при-	Еженедельно	

меняемого ПО на всех элементах ИС-ПДн		
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 инфор-	01.01.2010	ЗАО «Практи-	Аналитический отчет

мационной безопасности		ка Безопасности»	
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 № 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:

№	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 НАЗВАНИЕ версия	Антивирус настроен на: – резидентный антивирусный мониторинг; – ежедневное антивирусное сканирование; – скрипт-блокирование; – автоматизированное обновление антивирусных баз с периодичностью _____. – … – … – … Ключи и атрибуты доступа хранятся у _____ в _____ (сейф, криптографически защищенный носитель и т.п.)	Журнал настроек Межсетевого экрана хранится у _____
Межсетевой экран НАЗВАНИЕ версия	Межсетевой экран настроен на: – фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов; – регистрацию и учет запрашиваемых сервисов прикладного уровня: – – – – – блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами,	Инструкция по установке и настройке от производителя. Журнал настроек Межсетевого экрана хранится у _____

	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

№	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 дан-	+	+	+

	ных 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 № 152-ФЗ «О персональных данных»

2 Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

3 Федеральный закон от 19 декабря 2005 года № 160-ФЗ «О ратификации Конвенции Совета Европы О защите физических лиц при автоматической обработке персональных данных»

4 Федеральный закон от 10 января 202 года № 1-ФЗ «Об электронной цифровой подписи»

5 Указ Президента Российской Федерации от 12 мая 2009 года № 537 “О стратегии национальной безопасности Российской Федерации до 2020 года”.

6 Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 года № Пр-1895

7 Указ Президента Российской Федерации от 17 марта 2008 г. № 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 № 188 «Об утверждении Перечня сведений конфиденциального характера»

9 Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»

10 Постановление Правительства Российской Федерации от 31 августа 2006 г. № 532 «О лицензировании деятельности по разработке и / или производству средств защиты конфиденциальной информации»

11 Постановление Правительства Российской Федерации от 26 июня 1995 года № 608 «О сертификации средств защиты информации»

12 Постановление Правительства Российской Федерации от 28 февраля 1996 года № 226 «О государственном учете и регистрации баз и банков данных»

13 Постановление Правительства Российской Федерации от 3 ноября 1994 года № 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 № 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 1994г.

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. Классифика-

ция по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом Гостехкомиссии России от 4 июня 1999 г. № 114

20 Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден приказом Гостехкомиссии России от 19 июня 2002 г. № 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. № 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 № 149/5-144.

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 № 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.