Приложение № 1

к приказу руководителя комитета труда и социальной защиты населения администрации города Ставрополя

от «__»_____ 2014 г. № ___

Положение
по организации и проведению работ по обработке и защите персональных данных, обрабатываемых в информационных системах персональных данных комитета труда и социальной защиты населения администрации города Ставрополя

г. Ставрополь

СОДЕРЖАНИЕ

1. ИНФОРМАЦИЯ О ДОКУМЕНТЕ 3
2. ОБЩИЕ ПОЛОЖЕНИЯ 6
3. ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ПДН 7
4. ПРИНЦИПЫ ОБРАБОТКИ ПДН 8
5. ПОРЯДОК ОТНЕСЕНИЯ СВЕДЕНИЙ К ПЕРСОНАЛЬНЫМ ДАННЫМ 9
6. ОРГАНИЗАЦИОННАЯ СТРУКТУРА СЗПДН 9
7. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН 12
8. КАТЕГОРИРОВАНИЕ ПДН И КЛАССИФИКАЦИЯ ИСПДН 17
9. ОЦЕНКА ВОЗМОЖНОСТИ ОПТИМИЗАЦИИ ИСПДН 18
10. МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПДН 19
11. ОБУЧЕНИЕ ПЕРСОНАЛА, УЧАСТВУЮЩЕГО В ОБРАБОТКЕ ПДН 19
12. ДОПУСК ПЕРСОНАЛА К ОБРАБОТКЕ ПДН 20
13. УНИЧТОЖЕНИЕ ПДН 20
14. ОРГАНИЗАЦИЯ РАБОТЫ С НОСИТЕЛЯМИ ПДН 21
15. КОНТРОЛЬ ИЗМЕНЕНИЙ В СОСТАВЕ И СТРУКТУРЕ ИСПДН 21
16. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ФИЗИЧЕСКОГО ДОСТУПА К ЭЛЕМЕНТАМ ИСПДН 223
17. РЕЗЕРВИРОВАНИЕ ПДН 223
18. КОНТРОЛЬ ЗА ОБЕСПЕЧЕНИЕМ НЕОБХОДИМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ПДН 234
19. РЕАГИРОВАНИЕ НА НЕШТАТНЫЕ СИТУАЦИИ 23
20. КОНТРОЛЬ ЛОЯЛЬНОСТИ ПЕРСОНАЛА 24
21. НОРМАТИВНЫЕ ССЫЛКИ 24
22. КОНТРОЛЬ ВЕРСИЙ ДОКУМЕНТА 26

1. ИНФОРМАЦИЯ О ДОКУМЕНТЕ

1.1.Назначение документа

Настоящий документ определяет порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных комитета труда и социальной защиты населения администрации города Ставрополя (далее – Комитет) и содержит общие принципы защиты персональных данных.

1.2.Цели документа

Данный документ направлен на достижение следующих целей:

- выполнение требований нормативных документов Российской Федерации, связанных с персональными данными;
- защита прав и свобод граждан при обработке их персональных данных в информационных системах персональных данных Комитета;
- защита персональных данных, обрабатываемых в Комитете, от несанкционированного доступа и от других несанкционированных действий;
- снижение уровня регуляторных рисков в отношении Комитета.

1.3.Ответственность и область применения

Настоящий документ обязаны знать и использовать в работе все сотрудники Комитета.

1.4.Вводимые определения терминов и сокращений

Таблица 1. Перечень сокращений

Сокращение	Расшифровка сокращения
АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ИС	Информационная система
ИСПДн	Информационная система персональных данных
ЛВС	Локальная вычислительная сеть
ПДн	Персональные данные
СЗПДн	Система защиты персональных данных
СКС	Структурированная кабельная система
СОИБ	Система обеспечения информационной безопасности
СТЗ	Специальное техническое задание
ТЗ	Техническое задание

Таблица 2. Перечень терминов

Наименование термина	Определение термина
Безопасность информации [данных]	Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.
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.

Наименование термина	Определение термина
Вредоносная программа	Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействии 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 к информации	Возможность получения информации и ее использования.
Защита информации	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
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.
Информационная система персональных данных	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.
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.
Контролируемая зона	Пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.
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.
Модель угроз (безопасности информации)	Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.
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 защищаемой 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.
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.
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

Наименование термина	Определение термина
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.
Оператор	Государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.
Ответственный за применение нормативного документа	Должностное лицо, ответственное за внедрение и применение нормативного документа. Термин применим к нормативным документам, кроме регламента процесса, для регламента процесса используется термин «Владелец процесса». «Ответственный за применение НД» и «Ответственный за разработку НД» могут совпадать.
Ответственный за разработку нормативного документа	Должностное лицо или отдел, ответственное за создание и поддержание нормативного документа в актуальном состоянии. Ответственный за разработку НД отвечает за плановый пересмотр документа и за внесение внеочередных изменений в соответствии с данным положением.
Отдел	Официально выделенная в организационной структуре Комитета группа работников, выполняющая определенные функции и задачи, предусмотренные Положением об отделе
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.
Перехват (информации)	Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.
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.
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.
Ресурс информационной системы	Именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.
Субъект доступа (субъект)	Лицо или процесс, действия которого регламентируются правилами разграничения доступа.
Технический канал утечки информации	совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.
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.

Наименование термина	Определение термина
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.
Уполномоченное оператором лицо	Лицо, которому на основании договора оператор поручает обработку персональных данных.
Целостность информации	Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).
Цель защиты информации	Заранее намеченный результат защиты информации.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение устанавливает требования по защите персональных данных, принципы обработки персональных данных в информационных системах персональных данных, направленные на защиту интересов Комитета в области его деятельности, обеспечение непрерывности деятельности Комитета.

Требования Положения распространяются на все отделы Комитета, в которых осуществляется автоматизированная и неавтоматизированная обработка персональных данных, а также на отделы, осуществляющие сопровождение, обслуживание и обеспечение функционирования информационных систем персональных данных.

Настоящее Положение разработана в соответствии со следующими нормативными актами:

- Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства Российской Федерации от 15 сентября 2008 г № 687;
- Порядок проведения классификации информационных систем персональных данных, утвержденный Приказом ФСТЭК России, ФСБ России и Мининформсвязи России № 55/86/20 от 13 февраля 2008 года;
- нормативные и методические документы ФСБ России, ФСТЭК России, Роскомнадзора.

Персональные данные являются сведениями, отнесенными к информации ограниченного доступа.

Настоящее Положение является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности персональных данных;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности персональных данных и выработки комплекса согласованных мер нормативно-правового, технического и организационно-технического характера, направленных на выявление, отражение и уменьшение угроз безопасности ПДн;

- координации деятельности отделов Комитета при проведении работ по созданию, развитию и эксплуатации ИСПДн с соблюдением требований по обеспечению безопасности персональных данных;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности персональных данных в ИСПДн.

Принципы и требования по обеспечению безопасности персональных данных распространяются:

- на все возможные формы существования информации (физические поля (электрические, акустические, электромагнитные, оптические и т.п.), носители на бумажной, магнитной, оптической и иной основе);
- на все возможные форматы представления персональных данных (документы, голос, изображения, файлы, почтовые сообщения, базы данных, записи базы данных, другие информационные массивы).

Предотвращение несанкционированного и нелегитимного доступа к информационным системам, технологиям и информационным ресурсам результатом которого может стать уничтожение, модификация, искажение, копирование, распространение, блокирование ПДн требует применения комплекса правовых, организационных, организационно-технических мер защиты с использованием сертифицированных средств защиты информации.

Настоящее Положение определяет:

- роли, полномочия, ответственность за обеспечение безопасности ПДн, отделов Комитета;
- порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн;
- мероприятия по обеспечению безопасности ПДн;
- требования по управлению процессом обеспечения безопасности ПДн;
- требования к составу и содержанию документов Комитет, регламентирующих защиту и работу с ПДн.

При работе с персональными данными, во всех случаях, не урегулированных нормативными документами Комитета, необходимо руководствоваться действующим законодательством Российской Федерации.

3. ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ПДН

Целью создания системы защиты ПДн является исключение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий.

В общем случае можно выделить следующие основные цели защиты ПДн, это обеспечение:

- конфиденциальности ПДн;
- целостности ПДн;
- доступности ПДн;
- неотказуемости;
- учетности[1];
- аутентичности[2];

[1] **Учетность** – свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта (ИСО 7498–2:99);
– обеспечение того, что действия субъекта по отношению к объекту могут быть прослежены уникально по отношению к субъекту.

– адекватности[3].

Конкретный состав целей защиты ПДн зависит от конкретной ИСПДн и определяется по результатам разработки (актуализации) модели угроз и нарушителя безопасности ПДн.

К основным задачам в области обеспечения безопасности ПДн относится:

- определение новых ИСПДн;
- инвентаризация и управление изменениями в составе и структуре ИСПДн;
- сбор согласий на обработку ПДн с субъектов ПДн;
- разработка и актуализация «Перечня персональных данных, обрабатываемых в Комитете (Приложение 1);
- контроль целей обработки ПДн, состава обрабатываемых ПДн целям обработки;
- уничтожение ПДн;
- оптимизация информационных и бизнес процессов обработки ПДн;
- управление взаимодействиями с внешними контрагентами по вопросам обработки ПДн;
- взаимодействие с субъектами ПДн по вопросам обработки их ПДн;
- классификация ИСПДн;
- разработка (актуализация) документации на систему защиты ПДн;
- выбор и внедрение необходимых и достаточных мер и средств защиты ПДн;
- сертификация применяемых средств защиты информации;
- эксплуатация системы защиты ПДн в соответствии с документацией на нее;
- контроль уровня защищенности ПДн;
- обучение персонала по вопросам защиты ПДн;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к обработке ПДн;
- взаимодействие с регуляторными органами по вопросам защиты ПДн;
- актуализация и подача уведомлений в Уполномоченный орган по защите прав субъектов ПДн;
- реагирование на нештатные ситуации, расследование нештатных ситуаций возникающих при обработке ПДн;
- получение лицензий ФСТЭК России и ФСБ России в области защиты ПДн;
- контроль лояльности администраторов ИСПДн.

4. ПРИНЦИПЫ ОБРАБОТКИ ПДН

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» обработка ПДн должна осуществляться в соответствии со следующими принципами:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

---

[2] **Аутентичность**

– свойство обеспечения идентичности субъекта или ресурса заявленной идентичности. Аутентичность применяется к таким субъектам как пользователи, процессы, системы и информация (ISO/IEC 13335–1:2004);
– идентичность объекта тому, что заявлено.

[3] **Адекватность**

– свойство соответствия преднамеренному поведению и результатам (ISO/IEC 13335–1:2004).

- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных

В Комитете должен проводиться регулярный анализ соответствия процессов обработки ПДн указанным принципам. Данный анализ проводится в случае:

- создания новых ИСПДн;
- внесения изменений в технологические процессы существующие в ИСПДн;
- изменения нормативной базы затрагивающей принципы и(или) процессы обработки ПДн в ИСПДн Комитета;
- проведения контрольных и проверочных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

Обработка персональных данных в Комитете осуществляется только с согласия субъектов персональных данных. Форма журнала представлена с Инструкцией о порядке обработки персональных данных в комитете труда и социальной защиты населения администрации города Ставрополя.

5. ПОРЯДОК ОТНЕСЕНИЯ СВЕДЕНИЙ К ПЕРСОНАЛЬНЫМ ДАННЫМ

В соответствии с Федеральным законом № 152-ФЗ «О персональных данных» от 27 июля 2006 г. «Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных».

Отнесение сведений Комитета к соответствующим категориям информации представляет собой процесс обоснованного установления (документального оформления и утверждения руководством Комитета) критериев их выделения из всей совокупности сведений, находящихся в обращении.

В качестве таких критериев в отношении персональных данных в Комитете разрабатывается и утверждается «Перечень персональных данных, обрабатываемых в Комитете».

Перечень персональных данных, обрабатываемых в Комитете, утверждается руководителем Комитета».

6. ОРГАНИЗАЦИОННАЯ СТРУКТУРА СЗПДН

Система защиты ПДн является частью общей Системы обеспечения информационной безопасности Комитета.

Основу организационной структуры СЗПДн составляют:

- руководство;
- отдел правового и кадрового обеспечения;
- ответственные за обеспечение безопасности ПДн;
- администраторы ИСПДн[4];
- владельцы ИСПДн и процессов обработки ПДн;
- отделы, участвующие в процессах обработки ПДн;

[4] Сотрудники, осуществляющие конфигурацию, настройку и управление программными, техническими, программно-аппаратными средствами ИСПДн, в том числе средствами защиты ПДн

- сотрудники Комитета.

Руководство Комитета осуществляет следующие основные функции в области обеспечения безопасности ПДн:

- обеспечивает общую организацию работ по защите ПДн;
- издает приказы по вопросам организации СЗПДн;
- утверждает «Перечень персональных данных, обрабатываемых в Комитете»;
- назначает ответственного за обеспечение безопасности ПДн;
- рассматривает и утверждает нормативные документы Комитета по защите ПДн;
- заслушивает при необходимости ответственных за обеспечение безопасности ПДн и других должностных лиц о состоянии работ по защите ПДн.

Отдел правового и кадрового обеспечения осуществляет следующие основные функции:

- дает юридическую оценку возможности создания (модернизации) ИСПДн.
- проводит ознакомление сотрудников с нормативными документами в области защиты ПДн и делает отметки в журнале инструктажа лиц, допущенных к обработке ПДн. Форма журнала представлена в Приложении 3.

Ответственные за обеспечение безопасности ПДн осуществляют следующие основные функции:

- разрабатывают «Перечень ПДн, обрабатываемых в Комитете»;
- проводят классификацию ИСПДн;
- распределяют ответственность по вопросам обработки и защиты ПДн;
- определяют допустимые сроки хранения ПДн по каждой категории ПДн;
- организуют подачу Уведомлений в Уполномоченный орган по защите прав субъектов ПДн;
- заслушивают руководителей отделов о принимаемых мерах по состоянию и совершенствованию СЗПДн;
- организуют работы по разработке, изменению и уточнению политик, регламентов, стандартов в части защиты ПДн;
- осуществляют организацию плановых и внеплановых проверочных мероприятий;
- организуют выполнение требований по защите ПДн в Комитете;
- проводят разработку и актуализацию корпоративных нормативных документов, регламентирующих защиту ПДн;
- разрабатывают и актуализируют Модели угроз безопасности ПДн и технические задания на СЗПДн;
- разрабатывают (актуализируют) проектную документацию на СЗПДн;
- подготавливают проекты решений по изменению «Перечня персональных данных, обрабатываемых в Комитете, классификации ИСПДн, Уведомления об обработке ПДн и других коллегиальных решений по обработке и обеспечению безопасности ПДн в Комитете;
- определяют необходимость обучения сотрудников вопросам обеспечения безопасности ПДн, а также определяют формы и программы обучения сотрудников Комитета в области защиты ПДн;
- организуют работы по сбору сведений об изменениях в составе и структуре ИСПДн;
- осуществляют контроль соответствия изменений в составе и архитектуре ИСПДн требованиям нормативных документов Российской Федерации по защите ПДн, а также внутренних организационно-распорядительных документов Комитета;
- контролируют исполнение требований по уничтожению ПДн;
- разрабатывают рекомендации по оптимизации существующих и новых информационных и процессов обработки ПДн по критериям соответствия

требованиям по защите ПДн и минимизации затрат на создание и эксплуатацию системы защиты ПДн;
- контролируют исполнение требований нормативных документов Комитета в области обеспечения безопасности ПДн, отделами и сотрудниками;
- организуют и осуществляют взаимодействие с регуляторами по вопросам защиты ПДн;
- осуществляют контроль лояльности администраторов ИБ ИСПДн;
- организуют получение лицензий ФСТЭК России и ФСБ России по технической и криптографической защите конфиденциальной информации, необходимые в целях защиты ПДн;
- проводят работы по классификации ИСПДн;
- отслеживают необходимость и организуют работы по сертификации (подтверждению сертификата), применяемых средств и систем защиты ПДн;
- управляют проектами по внедрению систем и средств защиты ПДн;
- контролируют ввод в действие, эксплуатацию СЗПДн;
- проводят расследования инцидентов, связанных с нарушением безопасности ПДн, правил обработки ПДн, принимают меры по недопущению повторения нештатных ситуаций.

Администраторы ИБ ИСПДн осуществляют следующие основные функции:
- осуществляют сопровождение средств и систем защиты ПДн;
- проводят оперативный контроль функционирования средств и систем защиты ПДн;
- проводят резервирование ПДн;
- контролируют факты обращений пользователей ИСПДн к персональным данным, зарегистрированные в электронном журнале обращений пользователей к соответствующим ресурсам ИСПДн;
- осуществляют выявление и регистрацию попыток НСД к компонентам ИСПДн, информационным ресурсам;
- контролируют соответствие технических, программных и программно-аппаратных средств ИСПДн требованиям, предъявляемым к ним средствами и системой защиты ПДн;
- проводят оценку эффективности принятых мер и применяемых средств защиты ПДн;
- проводят занятия с сотрудниками по изучению организационно-распорядительных документов по всему комплексу вопросов защиты ПДн;
- осуществляют учет применяемых средств защиты ПДн, эксплуатационной и технической документации к ним;
- контролируют выполнение сотрудниками отдела требований по защите ПДн;
- участвуют в расследованиях причин возникновения нештатных ситуаций;
- готовят предложения по совершенствованию системы защиты ПДн;
- выполняют комплекс мероприятий по защите информации при проведении ремонтных и регламентных работ;
- обеспечивают защиту ПДн при выводе из эксплуатации компонентов ИСПДн.

Конкретное распределение функций Администраторов ИБ ИСПДн должно быть приведено в эксплуатационной документации информационных систем.

Владельцы ИСПДн и процессов обработки ПДн осуществляют следующие основные функции:
- осуществляют контроль и учет проведения изменений в ИСПДн, согласуют проводимые изменения с ответственными за обеспечение безопасности ПДн;

- инициируют процесс создания СЗПДн;
- организуют и проводят уничтожение ПДн;
- составляют и актуализируют списки должностных лиц, имеющих доступ к ПДн;
- обеспечивают раздельное хранение ПДн, обрабатываемых в различных целях, неавтоматизированным способом;
- обеспечивают выполнение требований по защите ПДн, обрабатываемых неавтоматизированным способом;
- проводят согласование форм договоров, анкет, журналов и других документов, предназначенных для включения в них ПДн, с ответственными за обеспечение безопасности ПДн;
- осуществляют взаимодействие с субъектами ПДн, данные которых обрабатываются в их зоне ответственности, по вопросам обработки их ПДн;
- обеспечивают наличие в договорах с контрагентами, которые будут осуществлять обработку ПДн Комитета, требований по обеспечению конфиденциальности ПДн (при необходимости);
- участвуют в оптимизации информационных процессов обработки ПДн;
- участвуют в классификации ИСПДн, разработке Модели угроз безопасности ПДн в ИСПДн.

Отделы, участвующие в процессах обработки ПДн выполняют следующие основные функции:

- осуществляют взаимодействие с субъектами ПДн по вопросам обработки их ПДн;
- осуществляют уведомление субъектов ПДн в случаях определенных нормативными актами;
- эксплуатируют систему защиты ПДн в соответствии с документацией на нее;
- принимают меры по реализации перечня необходимых защитных мероприятий на объектах отделов;
- ведут учет носителей персональных данных.

Сотрудники Комитета выполняют следующие основные функции:

- соблюдают требования нормативных документов по защите ПДн;
- осуществляют обработку ПДн в соответствии с заданием и предоставленными полномочиями.

Владельцем процесса обеспечения безопасности ПДн в каждой ИСПДн является отдел, являющийся владельцем данной ИСПДн.

Для координации процесса обеспечения безопасности ПДн, решения задач требующих скоординированных действий разных отделов Комитета могут создаваться рабочие группы, в состав которых должны входить представители руководства всех заинтересованных отделов Комитета.

Распределение ролей, полномочий, ответственности по обеспечению безопасности ПДн осуществляется в соответствии с нормативными документами Комитета, приведенными в соответствующем разделе.

7. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ выполняемых в рамках жизненного цикла ИСПДн.

Работы по обеспечению безопасности ПДн привязаны к жизненному циклу ИСПДн, а именно к следующим этапам:

- инициация проекта ИСПДн;

- планирование проекта ИСПДн;
- реализация проекта ИСПДн, в составе;
- эксплуатация ИСПДн;
- модернизация ИСПДн;
- вывод из эксплуатации.

Работы по защите ПДн с привязкой к этапам жизненного цикла ИСПДн приведены в таблице 7.1.

Таблица 7.1. Распределение работ по защите ПДн на стадии существования ИСПДн

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
1.	**Инициация проекта ИСПДн**		
1.1.	определение ИСПДн	При создании ИС или существенном изменении существующей ИС определяется необходимость обработки ПДн. Если такая необходимость имеется, то система объявляется - ИСПДн	С автоматизированной обработкой С неавтоматизированной обработкой
1.2.	определение существенной информации об ИСПДн	На данном этапе производится: ▪ определение перечня ПДн, которые будут обрабатываться в ИСПДн; ▪ определение целей обработки ПДн, действий выполняемых с ПДн, допустимых сроков хранения ПДн; ▪ определение перечня типов технических средств, предполагаемые к использованию в ИСПДн, перечня системных и прикладных программных средств; ▪ определение степени участия персонала в обработке ПДн, характер взаимодействия персонала между собой и с системой.	С автоматизированной обработкой С неавтоматизированной обработкой
1.3.	определение предварительной категории ПДн	Детализация проводимых работ приведена в разделе 8	С автоматизированной обработкой С неавтоматизированной обработкой
1.4.	определение предварительного класса ИСПДн	Детализация проводимых работ приведена в разделе 8	С автоматизированной обработкой
1.5.	оценивается возможность оптимизации ИСПДн	Детализация проводимых работ приведена в разделе 9	С автоматизированной обработкой С неавтоматизированной обработкой
1.6.	юридическая оценка возможности создания ИСПДн	На данном этапе производится юридическая оценка: ▪ целей обработки ПДн; ▪ операций, которые будут выполняться с ПДн; ▪ наличия (возможности сбора) согласий на обработку ПДн, необходимости сбора согласий на обработку ПДн; ▪ степени участия контрагентов Комитета в обработке ПДн и необходимые юридические основания для такой обработки; ▪ соответствия предполагаемых процессов обработки ПДн принципам их обработки (см. раздел 4).	С автоматизированной обработкой С неавтоматизированной обработкой
1.7.	проведение оценки возможных затрат на создание СЗПДн по срокам и стоимости	Оцениваются возможные затраты на создание СЗПДн, которые должны учитываться при защите проекта и планировании проекта	С автоматизированной обработкой С неавтоматизированной обработкой
2.	**Реализация проекта ИСПДн – концепция реализации ИСПДн/СЗПДн**		

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
2.1.	определяется необходимость корректировки «Перечня ПДн», при необходимости проводится его корректировка		С автоматизированной обработкой С неавтоматизированной обработкой
2.2.	построение модели информационных потоков персональных данных	Разработка модели информационных потоков должно производиться на основании соответствующего стандарта	С автоматизированной обработкой С неавтоматизированной обработкой
2.3.	определение перечня актуальных угроз безопасности ПДн в конкретных условиях функционирования (разработка модели угроз и нарушителя безопасности ПДн)	Детализация проводимых работ приведена в разделе 10	С автоматизированной обработкой
2.4.	определение категорий ПДн и класса ИСПДн	Детализация проводимых работ приведена в разделе 8	С автоматизированной обработкой
2.5.	определение необходимости создания СЗПДн	На данном этапе на основе класса ИСПДн определяется необходимость создания СЗПДн[5]	С автоматизированной обработкой
2.6.	разработка технического (специального технического) задания на разработку СЗПДн	На данном этапе определяются требования к техническим, программным, программно-аппаратным и организационным средствам и мерам обеспечения безопасности ПДн.	С автоматизированной обработкой
3.	**Реализация проекта ИСПДн – проектирование ИСПДн**		
3.1.	разработка эскизного проекта на СЗПДн	На данном этапе разрабатывается: ▪ пояснительная записка; ▪ структурная схема комплекса технических средств.	С автоматизированной обработкой
3.2.	проработка форм документов предполагающих включение в них ПДн	На данном этапе производится: ▪ определение форм документов, в которых будут содержаться ПДн; ▪ оценка соответствия форм требованиям, предъявляемым к ним нормативными документами РФ в области защиты ПДн; ▪ производится корректировка форм.	С неавтоматизированной обработкой
3.3.	разработка эксплуатационной документации на ИСПДн	Производится разработка политик, регламентов, инструкций, определяющих частный порядок защиты ПДн в данной ИСПДн	С автоматизированной обработкой С неавтоматизированной обработкой
4.	**Реализация проекта ИСПДн – производство ИСПДн**		
4.1.	внедрение комплекса средств и мер защиты ПДн	Производятся монтажные, пуско-наладочные работы средств защиты информации. Производится реализация комплекса организационно-технических мероприятий по защите ПДн.	С автоматизированной обработкой
4.2.	реализация требований по физической защите компонентов ИСПДн и носителей ПДн	Производятся монтажные работы средств физической защиты (замков, шкафов, сейфов и т.п.)	С автоматизированной обработкой С неавтоматизированной обработкой
4.3.	заключаются договора с контрагентами, которые будут осуществлять	На данном этапе определяются договора, в которые должны быть внесены изменения. В данные договора вносятся требования по обеспечению	С автоматизированной обработкой С неавтоматизированной

[5] Для ИСПДн 4 класса создание СЗПДн не обязательно (по решению руководства Комитета)

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
	обработку ПДн Комитета, с учетом требований по защите ПДн (при необходимости)	конфиденциальности ПДн контрагентами, которые будут иметь к ним доступ.	обработкой
4.4.	определение отдела и назначение лиц, ответственных за эксплуатацию средств защиты информации		С автоматизированной обработкой С неавтоматизированной обработкой
5.	**Реализация проекта ИСПДн – передача системы в опытно-промышленную эксплуатацию**		
5.1.	проводится обучение сотрудников по направлению обеспечения безопасности ПДн	Детализация проводимых работ приведена в разделе 11	С автоматизированной обработкой С неавтоматизированной обработкой
5.2.	проводится ознакомление сотрудников с нормативными документами в области защиты ПДн		С автоматизированной обработкой С неавтоматизированной обработкой
6.	**Реализация проекта ИСПДн – опытная эксплуатация ИСПДн**		
6.1.	начинает производиться сбор согласий на обработку ПДн с субъектов ПДн (в случае необходимости их сбора определенной в п. 1.6)		С автоматизированной обработкой С неавтоматизированной обработкой
6.2.	оценивается необходимость изменения Уведомления об обработке ПДн	На данном этапе производится: ▪ определение необходимости изменения Уведомления об обработке ПДн; ▪ производится подготовка, согласование и отправка нового Уведомления об обработке ПДн в Уполномоченный орган по защите прав субъектов ПДн. Форма, состав Уведомления определяется в соответствии с нормативными документами Уполномоченного органа по защите прав субъектов ПДн	С автоматизированной обработкой С неавтоматизированной обработкой
6.3.	проводится опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн		С автоматизированной обработкой
6.4.	разрабатывается программа и методика приемочных испытаний		С автоматизированной обработкой
6.5.	проводятся приемочные испытания СЗПДн	Приемочные испытания СЗПДн проводятся в соответствии с программой и методикой приемочных испытаний	С автоматизированной обработкой
7.	**Эксплуатация ИСПДн**		
7.1.	допуск персонала к обработке ПДн	Детализация проводимых работ приведена в разделе 12	С автоматизированной обработкой С неавтоматизированной обработкой

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
7.2.	производится уничтожение ПДн	Детализация проводимых работ приведена в разделе 13	С автоматизированной обработкой С неавтоматизированной обработкой
7.3.	производится работа с носителями ПДн	Детализация проводимых работ приведена в разделе 14	С автоматизированной обработкой С неавтоматизированной обработкой
7.4.	производится учет средств защиты информации, эксплуатационной документации к ним	Учет средств защиты информации, эксплуатационной документации производится администраторами ИСПДн, порядок учета должен быть регламентирован в соответствующем документе	С автоматизированной обработкой
7.5.	осуществляется контроль изменений в составе и структуре ИСПДн	Детализация проводимых работ приведена в разделе 15	С автоматизированной обработкой С неавтоматизированной обработкой
7.6.	обеспечивается защита от несанкционированного физического доступа к элементам ИСПДн	Детализация проводимых работ приведена в разделе 16	С автоматизированной обработкой С неавтоматизированной обработкой
7.7.	осуществляется резервирование ПДн	Детализация проводимых работ приведена в разделе 17	С автоматизированной обработкой
7.8.	осуществляется эксплуатация системы защиты ПДн в соответствии с документацией на нее	Эксплуатация системы защиты осуществляется в соответствии с проектом, регламентами и стандартами. Состав системы защиты ПДн и мероприятий по защите ПДн определяется дифференцированно для различных ИСПДн, в зависимости от результатов разработки Модели угроз и ТЗ (СТЗ) на СЗПДн	С автоматизированной обработкой
7.9.	осуществляется контроль за обеспечением необходимого уровня защищенности ПДн	Детализация проводимых работ приведена в разделе 18	С автоматизированной обработкой
7.10.	производится реагирование на нештатные ситуации	Детализация проводимых работ приведена в разделе 19	С автоматизированной обработкой С неавтоматизированной обработкой
7.11.	производится контроль лояльности персонала	Детализация проводимых работ приведена в разделе 20	
7.12.	проводится обучение персонала правилам обеспечения безопасности ПДн	Детализация проводимых работ приведена в разделе 11	С автоматизированной обработкой
7.13.	осуществляется взаимодействие с субъектами ПДн по вопросам обработки их ПДн	Взаимодействие с субъектами ПДн производится в порядке, определенном законодательством РФ	С автоматизированной обработкой С неавтоматизированной обработкой
7.14.	отслеживается необходимость получения лицензий ФСТЭК России и ФСБ России	В рамках данного процесса производится отслеживание сроков действия имеющихся лицензий ФСТЭК России и ФСБ России касающихся защиты ПДн. При необходимости производится инициация работ по повторному получению данных лицензий.	С автоматизированной обработкой С неавтоматизированной обработкой
7.15.	осуществляется взаимодействие с регуляторными органами по вопросам защиты ПДн		С автоматизированной обработкой С неавтоматизированной обработкой
8.	**Модернизация ИСПДн**		

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
8.1.	осуществляется управление изменениями в ИСПДн	Детализация проводимых работ приведена в разделе 15	С автоматизированной обработкой С неавтоматизированной обработкой
8.2.	производится оценка существенности предполагаемой модернизации ИСПДн	Проводится анализ: ▪ Возможности изменения класса ИСПДн, актуальных угроз, требований к СЗПДн ▪ Необходимости корректировки документации на СЗПДн ▪ Необходимости проведения дополнительных мероприятий по защите ПДн	С автоматизированной обработкой С неавтоматизированной обработкой
8.3.	на основе оценки существенности модернизации, проводится необходимый объем мероприятий[6]		С автоматизированной обработкой С неавтоматизированной обработкой
9.	**Вывод из эксплуатации ИСПДн**		
9.1.	производится уничтожение ПДн	Детализация проводимых работ приведена в разделе 13	С автоматизированной обработкой С неавтоматизированной обработкой
9.2.	производится уведомление субъектов ПДн (а при необходимости и Уполномоченный орган по защите прав субъектов ПДн) об уничтожении ПДн	Взаимодействие с субъектами ПДн производится в порядке, определенном законодательством РФ	С автоматизированной обработкой С неавтоматизированной обработкой

8. КАТЕГОРИРОВАНИЕ ПДН И КЛАССИФИКАЦИЯ ИСПДН

Категорирование ПДн и классификация ИСПДн должны проводиться для ИСПДн с автоматизированной обработкой персональных данных.

Классификация ИСПДн и категорирование ПДн проводятся в соответствии с Порядком проведения классификации информационных систем персональных данных (утвержденным Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20).

Процесс категорирования ПДн и классификации ИСПДн является основой для определения требований к уровню защиты ПДн.

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» оператор ПДн «обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий». Таким образом, в соответствии с Порядком проведения классификации информационных систем персональных данных (утвержденным Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20):

- все ИСПДн Комитета с автоматизированной обработкой относятся к категории специальных ИСПДн (ИСПДн, для которых требуется обеспечить не только конфиденциальность ПДн);
- класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных.

[6] Объем необходимых мероприятий определяется ответственными за обеспечение безопасности ПДн

Классификация ИСПДн и категорирование ПДн проводятся путем:

- приведения исходных характеристик, влияющих на класс и категорию ПДн;
- указания предположений, влияющих на категорию ПДн и классификацию ИСПДн;
- логического обоснования предполагаемого класса ИСПДн и категорий ПДн.

Исходные характеристики, предположения и обоснования, а также выводы о классе ИСПДн и категории ПДн приводятся в Модели угроз безопасности ПДн,

Модель угроз безопасности ПДн может быть разработана на несколько ИСПДн сразу или на какую-либо конкретную ИСПДн.

Оценка необходимости пересмотра класса ИСПДн должна осуществляться каждый раз, когда изменились характеристики, учитываемые при классификации ИСПДн.

Результаты работы по классификации ИСПДн оформляются актом классификации. Форма акта приведена в Приложении 2.

9. ОЦЕНКА ВОЗМОЖНОСТИ ОПТИМИЗАЦИИ ИСПДН

Оценка возможности оптимизации ИСПДн имеет своей целью такую реструктуризацию ИСПДн, выполнение требований по защите ПДн в которой может быть обеспечено с минимальным уровнем затрат на создание и эксплуатацию системы защиты ПДн.

При проведении оптимизации ИСПДн должна оцениваться возможность:

- снижения категории обрабатываемых ПДн;
- обезличивания ПДн;
- придания ПДн статуса общедоступных;
- изменения структуры и состава технических и программных средств ИСПДн, технологических процессов обработки ПДн.

Снижение категории ПДн, в общем случае, позволяет снизить класс ИСПДн и, соответственно, уровень требований к ИСПДн.

Обезличивание персональных данных и отнесение ПДн к общедоступным – это эффективный способ обеспечения их безопасности, так как для обезличенных и общедоступных персональных данных не требуется обеспечение их конфиденциальности.

Отсутствие необходимости защиты конфиденциальности ПДн не снимает необходимости защиты других характеристик безопасности (целостности, доступности и т.п.).

Необходимость защиты других характеристик безопасности определяется посредством оценки возможности ущерба для субъектов ПДн при нарушении этих характеристик безопасности. При наличии такого ущерба, в отношении таких ИСПДн, должен применяться комплекс мероприятий по их защите в полном объеме, в соответствии с разделом 7 настоящего Положения.

Среди мероприятий по обезличиванию ПДн, можно выделить следующие:

- разделение ПДн – ПДн, позволяющих идентифицировать субъекта ПДн и остальной информации по разным ИСПДн, базам или массивам данных;
- удаление ПДн, позволяющих идентифицировать субъекта ПДн, в технологических процессах, в которых не требуется однозначного определения физического лица.

Придание ПДн статуса общедоступных возможно в следующих случаях:

- при наличии федерального закона, определяющего, что этот состав ПДн является общедоступным;
- при наличии возможности сбора согласий на общедоступность их ПДн с субъектов ПДн.

Изменение структуры и состава технических и программных средств ИСПДн, технологических процессов обработки ПДн может проводиться, в том числе, с целью:

- уменьшения количества компонентов ИСПДн, на которые потребуется установка средств защиты;

- изменения возможности, степени опасности угроз для ИСПДн и, соответственно, уменьшения перечня актуальных угроз;
- изменения требований к характеристикам средств защиты информации, в результате которого возможно использование более оптимальных по стоимости средств и т.п.

10. МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПДН

СЗПДн внедряется для нейтрализации актуальных угроз безопасности персональных данных.

Оценка актуальности угроз производится посредством разработки модели угроз безопасности персональных данных (далее модель угроз) и модели нарушителя.

Методической базой для разработки Модели угроз и нарушителя безопасности ПДн является:

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 года;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 года;
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.

Результатом разработки Модели угроз и нарушителя безопасности ПДн должен являться:

- перечень актуальных угроз;
- вывод о классе ИСПДн;
- вывод о типе нарушителя, существующем в ИСПДн и требуемом классе средств криптографической защиты информации.

Модель угроз и нарушителя безопасности ПДн должна содержать:

- описание структуры и состава ИСПДн (состав обрабатываемых ПДн, состав технических средств и программного обеспечения, существующие процессы обработки ПДн, схему организации связи и т.п.);
- обоснование характеристик безопасности ПДн (конфиденциальность, целостность, доступность и т.п.), нарушение которых ведет к ущербу для субъектов ПДн;
- модель угроз (перечень угроз, оценку вероятностей угроз, показатели опасности угроз для ИСПДн, оценки возможностей реализации угроз, выводы об актуальности угроз);
- модель нарушителя (объекты атак, возможные типы нарушителей, предположения о возможностях нарушителей, предположения об ограничениях на эти возможности, предположения о каналах атак и средствах атак, выводы о типе нарушителя).

Модель угроз и нарушителя безопасности ПДн должна пересматриваться каждый раз, когда изменяются характеристики, влияющие на актуальность угроз, класс ИСПДн, тип нарушителя.

11. ОБУЧЕНИЕ ПЕРСОНАЛА, УЧАСТВУЮЩЕГО В ОБРАБОТКЕ ПДН

Должно проводиться регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн.

В общем случае, для различных категорий сотрудников форматы обучения должны отличаться.

Определены следующие форматы обучения:

- полные курсы (длительностью 5 дней и более);

- кратковременные курсы (длительностью от 1 до 3 дней);
- внешние и внутренние семинары;
- конференции;
- инструктажи;
- учения.

Полные и кратковременные курсы, конференции, внешние семинары проводятся во внешних специализированных организациях для следующих категорий сотрудников:

- ответственных за обеспечение безопасности ПДн;
- администраторов ИСПДн.

Для руководителей отделов, участвующих в процессах обработки ПДн, могут проводиться кратковременные курсы во внешних специализированных организациях.

Для обучения остальных категорий персонала, участвующих в процессах обработки ПДн, должны проводиться:

- внутренние семинары;
- инструктажи.

Внутренние семинары проводятся ответственными за обеспечение безопасности ПДн, приглашенными специалистами, а также другими подготовленными лицами. На всех семинарах следует использовать презентации.

Обучение каждой категории сотрудников должно проводиться не реже одного раза в год.

Инструктажи проводятся в отношении отдельных лиц, по мере необходимости Администраторами ИСПДн, ответственными за обеспечение безопасности ПДн.

Учения проводятся для закрепления практических навыков реагирования на возникающие угрозы и могут проводиться как для отдельных отделов Комитета, так и для Комитета в целом.

Учения проводятся не реже одного раза в год.

При необходимости должны разрабатываться инструкции, описывающие особенности обработки ПДн в каждой ИСПДн, для отдельных категорий (групп) персонала.

Для проведения семинаров создаются учебные группы по отделам. Состав группы не должен превышать 20-25 человек.

Инструкторы учебных групп должны в первый год, а в дальнейшем не реже 1 раза в 3 года проходить подготовку в специализированных учебно-методических центрах по вопросам защиты ПДн.

Руководители отделов обязаны оказывать организационную, техническую и методическую помощь инструкторам учебных групп и осуществлять постоянный контроль за подготовкой и проведением занятий.

12. ДОПУСК ПЕРСОНАЛА К ОБРАБОТКЕ ПДН

При допуске к ПДн необходимо руководствоваться Приказом о допуске к обработке ПДн.

Перечни должностных лиц составляются и ведутся владельцами ИСПДн и процессов обработки ПДн, на основании данных о должностных лицах, допущенных к ПДн.

Доступ конкретных лиц к ПДн и ИСПДн осуществляется на основании служебных записок (заявок).

Конкретный регламент предоставления доступа должен быть определен в Инструкции по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационной системы персональных данных.

13. УНИЧТОЖЕНИЕ ПДН

В соответствии с нормативными актами РФ ПДн должны быть уничтожены:

- по требованию субъекта ПДн, в определенных законом случаях;
- при истечении срока хранения;
- в случае выявления неправомерных действий с персональными данными и невозможности устранения допущенных нарушений;
- в случае достижения цели обработки ПДн;
- в случае утраты необходимости достижения цели обработки.

Контроль сроков хранения, целей обработки ПДн производится на основании допустимых сроков хранения и допустимых целей, указанных для конкретных категорий ПДн в «Перечне персональных данных, обрабатываемых в Комитете».

Решение об уничтожении ПДн, организацию и проведение уничтожения принимают и осуществляют владельцы ИСПДн и процессов обработки ПДн.

Об уничтожении ПДн должен быть уведомлен субъект ПДн.

После проведенного уничтожения должен быть подготовлен акт об уничтожении ПДн, форма акта приведена в Приложении 4.

14. ОРГАНИЗАЦИЯ РАБОТЫ С НОСИТЕЛЯМИ ПДН

Для организации документооборота связанного с ПДн в Комитете должны быть упорядочены и регламентированы следующие работы, связанные с ПДн:

- оформление носителей, содержащих персональные данные;
- учет носителей, содержащих персональные данные;
- обращение с носителями, содержащими персональные данные;
- систематизация носителей, содержащих персональные данные;
- хранение носителей, содержащих персональные данные;
- подготовка носителей, содержащих персональные данные для передачи их в архив;
- подготовка носителей, содержащих персональные данные для их уничтожения;
- проверка наличия носителей, содержащих персональные данные;
- распечатка ПДн.

Должны регламентироваться работы с ПДн в виде документов на следующих носителях:

- бумажных носителях;
- электронных съемных носителях;
- электронных несъемных носителях, используемых в технических средствах ИСПДн.

Порядок работ с носителями ПДн должен быть регламентирован в соответствующих корпоративных документах.

15. КОНТРОЛЬ ИЗМЕНЕНИЙ В СОСТАВЕ И СТРУКТУРЕ ИСПДН

Все изменения в составе и структуре ИСПДн должны контролироваться и регламентироваться.

Контролю подлежат следующие изменения:

- внесение новых устройств в состав ИСПДн (АРМ, серверов, сетевого и телекоммуникационного оборудования и т.п.);
- изменение мест включения существующих компонент ИСПДн;
- удаление устройства из состава ИСПДн;
- изменение мест установки устройства из состава ИСПДн;
- прокладка новых кабельных линий связи СКС и внешних линий связи или удаление старых кабельных линий связи;
- существенное изменение состава и конфигурации системного и прикладного программного обеспечения, участвующего в обработке ПДн;

- создание новых и изменение существующих технологических процессов связанных с обработкой ПДн.

Все запросы на изменения должны быть стандартизированы и выполняться в соответствии с разработанными формальными процедурами. Результаты всех изменений должны оцениваться и документироваться.

Должны применяться процедуры гарантирующие, что все потенциальные изменения оцениваются с точки зрения возможных негативных последствий для эксплуатации системы и ее функциональности.

Должны быть установлены процедуры определяющие необходимость проведения экстренных изменений и процедуры контроля этих изменений.

Каждое изменение состава ИСПДн, типов технических средств, топологии ИСПДн должно отслеживаться и анализироваться на предмет соответствия требованиям по защите ИСПДн. При необходимости должна производиться модернизация СЗПДн.

16. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ФИЗИЧЕСКОГО ДОСТУПА К ЭЛЕМЕНТАМ ИСПДН

Мероприятия по физическому контролю доступа включают:

- контроль доступа на территорию;
- контроль доступа в помещения с оборудованием ИСПДн;
- контроль доступа к техническим средствам ИС;
- контроль перемещений физических компонентов ИСПДн.

Помещения с серверным, телекоммуникационным и сетевым оборудованием ИСПДн должны иметь прочные входные двери с надежными автоматическими замками. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода сотрудников.

Двери помещений, в которых размещаются АРМ пользователей ИСПДн, должны быть оборудованы замками.

Нахождение в помещении лиц, не участвующих в технологических процессах обработки ПДн (обслуживающий персонал, другие сотрудники), должно допускаться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не являющихся пользователями ИСПДн.

В нерабочее время, по окончании рабочего дня двери помещений должны быть закрыты на замок.

При выносе устройств, хранящих ПДн, за пределы контролируемой зоны для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

В отношении некоторых ИСПДн возможны дополнительные, либо более низкие требования по физической защите. Состав таких требований определяется по результатам разработки Модели угроз и нарушителя и ТЗ (СТЗ, ЧТЗ) на создание СЗПДн. Мероприятия по защите таких ИСПДн определяются эксплуатационной (проектной) документацией.

17. РЕЗЕРВИРОВАНИЕ ПДН

Резервирование ПДн должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

В регламенте процесса резервирования должны быть учтены следующие вопросы:

- порядок резервирования;
- ответственные за резервирование;

- порядок восстановления информации после аварий;
- порядок хранения резервных копий.

Резервированию должна подвергаться информация на серверах ИСПДн.

Резервирование должно осуществляться на магнитные ленты или другие носители информации с соответствующим уровнем надежности и долговечности.

Хранение резервных копий должно осуществляться в надежных сейфах (металлических шкафах). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

Доступ к резервным копиям должен быть строго регламентирован.

Резервирование должно осуществляться в соответствии с Регламентом резервного копирования.

18. КОНТРОЛЬ ЗА ОБЕСПЕЧЕНИЕМ НЕОБХОДИМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ПДН

Для обеспечения эффективности процесса обеспечения безопасности ПДн проводится:

- контроль за соблюдением требований по обработке и защите персональных данных;
- контроль за соблюдением условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;
- контроль эффективности средств защиты ПДн.

Контрольные мероприятия могут быть:

- текущими;
- внезапными;
- плановыми внешними;
- плановыми внутренними.

Ответственность за текущий контроль эффективности обеспечения безопасности ПДн возлагается на Администраторов ИСПДн.

Ответственность за плановый контроль эффективности обеспечения безопасности ПДн возлагается на ответственных за обеспечение безопасности ПДн. Данные проверки должны включаться в план аудитов информационной безопасности на год.

Для планового контроля эффективности СЗПДн должны использоваться средства выявления уязвимостей информационной безопасности.

Внезапные проверки эффективности при необходимости могут проводиться специальными группами по решению ответственных за обеспечение безопасности ПДн.

При проведении контроля эффективности в общем случае должно проверяться:

- наличие установленных средств защиты информации;
- корректность настроек средств защиты информации;
- выполнение пользователями и администраторами требований инструктивных материалов по защите ПДн;
- исполнение требований к процедурам обработки ПДн (уничтожению ПДн, сбору согласий, допуску персонала к ПДн и т.п.);
- правильность организации работы с носителями ПДн;
- правильность обращения ключевой информации;
- соответствие системы защиты ПДн реальному положению дел в Комитете и т.п.

19. РЕАГИРОВАНИЕ НА НЕШТАТНЫЕ СИТУАЦИИ

Для эффективного реагирования на нештатные ситуации, возникающие при обработке ПДн, в Комитете должны быть регламентированы следующие вопросы:

- порядок определения нештатной ситуации;

- порядок оповещения сотрудников при возникновении различных нештатных ситуаций;
- порядок действий по нейтрализации нештатных ситуаций, сведения их негативных последствий к минимуму.

Разработанные порядки действий в нештатных ситуациях должны регулярно (не реже 1 раз в год) проверяться посредством проведения учений с корректировкой порядков по результатам проведенных проверок.

В Комитете должны проводиться расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями.

В рамках данного процесса должны решаться следующие задачи:

- расследование инцидентов, связанных с безопасностью ПДн;
- ликвидация последствий инцидентов связанных с безопасностью ПДн;
- принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

Реагирование на нештатные ситуации должно производиться в соответствии с Инструкцией по действиям пользователей информационной системы персональных данных комитета труда и социальной защиты населения администрации города Ставрополя в нештатных ситуациях.

20. КОНТРОЛЬ ЛОЯЛЬНОСТИ ПЕРСОНАЛА

В Комитете должен проводиться комплекс мероприятий направленных на исключение присутствия злоумышленников среди Администраторов ИСПДн и ответственных за обеспечение безопасности ПДн, а также возможность сговора двух и более злоумышленников.

Комплекс мероприятий должен включать, в том числе:

- проверки работников при приеме на работу;
- периодические проверки на лояльность;
- периодический мониторинг действий персонала.

Мероприятия по обеспечению безопасности персонала должны обеспечить невозможность злоумышленного сговора двух или более сотрудников Комитета.

Проверки должны выполняться как в скрытом, так и в явном режиме.

При приеме на работу должны проводиться проверки идентичности личности, точности и полноты биографических фактов и заявляемой квалификации.

21. НОРМАТИВНЫЕ ССЫЛКИ

Таблица 21.1. Внешние нормативные и распорядительные документы

№ п/п	Наименование документа
1	Конституция Российской Федерации, 12 декабря 1993 г.
2	Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». Страсбург, 28 января 1981 г.
3	Федеральный закон Российской Федерации от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
4	Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
5	Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6	Федеральный закон Российской Федерации от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».
7	Федеральный закон Российской Федерации от 08 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности».
8	Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (ТК РФ).
9	Федеральный закон Российской Федерации от 28 ноября 2007 г. № 275-ФЗ «О внесении изменений в статьи 5 и 7 Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

№ п/п	Наименование документа
10	Гражданский кодекс Российской Федерации (ГК РФ) от 30 ноября 1994 № 51-ФЗ.
11	Федеральный закон Российской Федерации от 08 августа 2001 № 129-ФЗ (ред. от 23 декабря 2003) «О государственной регистрации юридических лиц и индивидуальных предпринимателей».
12	Федеральный закон Российской Федерации от 22 октября 2004г. № 125-ФЗ «Об архивном деле в Российской Федерации».
13	Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утверждено Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781.
14	Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждено Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.
15	Постановление Правительства Российской Федерации от 6 июля 2008 г № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
16	Постановление Правительства Российской Федерации от 02 июня 2008 г. № 419 «О федеральной службе по надзору в сфере связи и массовых коммуникаций».
17	Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».
18	Постановление Правительства Российской Федерации от 23 сентября 2002 г. № 691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».
19	Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Перечень сведений конфиденциального характера».
20	Положение о государственном лицензировании деятельности в области защиты информации от 27 апреля 1994 г. № 10.
21	Порядок проведения классификации информационных систем персональных данных, утвержден Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.
22	Перечень типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения, Архивная служба России.
23	ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.
24	Международный стандарт ИСО/МЭК 27001-2005 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования.
25	ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения.
26	ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
27	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.
28	ГОСТ Р ИСО/МЭК 13335 Информационная технология. Методы и средства обеспечения безопасности.
29	ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.
30	Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), Гостехкомиссия России, 2002 г.
31	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.
32	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.
33	РД Гостехкомиссии России. «Защита от несанкционированного доступа к информации. Термины и определения», 1992 г.
34	РД Гостехкомиссии России. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1997 г.

№ п/п	Наименование документа
35	РД Гостехкомиссии России. «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1999 г.
36	РД Гостехкомиссии России. «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» 1992г.
37	РД Гостехкомиссии России. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992 г.
38	Положение по аттестации объектов информатизации по требованиям безопасности информации, Гостехкомиссия России, 1994 г.
39	Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Введена в действие приказом от 13 июня 2001 г. № 152 (ФАПСИ).
40	Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), введено приказом ФСБ России от 9 февраля 2005 г. № 66.
41	Требования к средствам криптографической защиты конфиденциальной информации, ФСБ России.
42	Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 г., № 149/54-144.
43	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, утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 г., № 149/6/6-622.

22. КОНТРОЛЬ ВЕРСИЙ ДОКУМЕНТА

Номер версии	Дата создания версии	Должность ответственного за разработку	ФИО Ответственного за разработку	Краткое описание изменений документа
1				разработка документа

23. ПРИЛОЖЕНИЕ 2 – ФОРМА АКТА КЛАССИФИКАЦИИ ИСПДН

УТВЕРЖДАЮ

_____Г.П. Волкова

«____»_____20__ г.

АКТ
классификации информационных систем персональных данных

Комиссия в составе:
Председатель: _____

Члены комиссии:
_____
_____
_____

рассмотрев исходные данные на информационные системы персональных данных:

- *Наименование ИСПДн 1*,
- *Наименование ИСПДн 2*,

условия их эксплуатации, с учетом характера обрабатываемой информации (Приложение 1 к Акту классификации ИСПДн), в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года № 55/86/20,

РЕШИЛА:
установить следующие классы информационным системам персональных данных Комитета

№ п/п	Наименование ИСПДн	Установленный класс
1		
2		

Председатель: _____

Члены комиссии:
_____
_____
_____

Исходные данные классификации информационных систем персональных данных комитета

п/п	Наименование ИСПДн (ее составной части)	Наименование объекта (полное и сокращенное) Отраслевая принадлежность Адрес объекта	Исходные данные классификации ИСПДн					Класс ИСПДн	Примечание
			Структура ИСПДн	Наличие подключений к	Режим обработки ПДн	Разграничение доступа	Нахождение ИСПДн (ее составных частей) в пределах России		
	2	3	4	5		7	8	9	10

24. ПРИЛОЖЕНИЕ 3 – ФОРМА ЖУРНАЛА ИНСТРУКТАЖА ЛИЦ УЧАСТВУЮЩИХ В ОБРАБОТКЕ ПДН

№ п.п.	Ф.И.О. пользователя ИСПДн	Наименование инструктажа	Дата проведения инструктажа	Оценка	Подпись пользователя ИСПДн	Ф.И.О. инструктора	Подпись инструктора
1	2	3	4	5	6	7	8

25. ПРИЛОЖЕНИЕ 4 – ФОРМА АКТА УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

УТВЕРЖДАЮ

Руководитель комитета

_____ Г.П. Волкова

«___»_____20__ г.

А К Т

уничтожения документов, содержащих персональные данные

« ___ » _____ 20___ года г.
_____

Комиссия в составе: председателя комиссии – _____

_____
(должность, фамилия и инициалы)

и членов комиссии – _____
(должность, фамилия и инициалы)

_____

произвела отбор для уничтожения следующие документы, содержащие персональные данные:

№ п/п	Наименование документа	Регистрационный номер документа	Дата регистрации	Номер экз.	Количество листов документа /приложения
1	2	3	4	5	6

Всего подлежит уничтожению _____ (_____) наименований документов.
(цифрами) (прописью)

Записи акта с учетными данными сверены.

Председатель комиссии _____ _____
(роспись) (инициалы, фамилия)

Члены комиссии _____ _____
(роспись) (инициалы, фамилия)

_____ _____
(роспись) (инициалы, фамилия)

_____ _____
(роспись) (инициалы, фамилия)

После утверждения акта, перед уничтожением отобранные документы с записями в акте сверили и полностью уничтожили путем измельчения в бумагорезательной машине.

Председатель комиссии _____ _____
(роспись) (инициалы, фамилия)

Члены комиссии _____ _____
(роспись) (инициалы, фамилия)

_____ _____
(роспись) (инициалы, фамилия)

_____ _____
(роспись) (инициалы, фамилия)

Отметки об уничтожении документов в формах регистрации проставлены.

Ответственный за учет

_____ _____ _____
(должность) (роспись) (инициалы, фамилия)