

АДМИНИСТРАЦИЯ ГОРОДА НОВОШАХТИНСКА
муниципальное бюджетное учреждение города Новошахтинска
«Многофункциональный центр предоставления
государственных и муниципальных услуг»

ПРИКАЗ № 18

г. Новошахтинск

17 декабря 2012 г.

Об утверждении Положения по организации и проведению работ по обработке и защите персональных данных, обрабатываемых в информационной системе персональных данных муниципального бюджетного учреждения города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг» от 17 декабря 2012 года.

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением 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»

ПРИКАЗЫВАЮ:

1. Утвердить Положение по организации и проведению работ по обработке и защите персональных данных, обрабатываемых в информационной системе персональных данных муниципального бюджетного учреждения города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг» согласно Приложению № 1.

2. Назначить главного специалиста-программиста Бурук Д.Н.

3. Главному специалисту-программисту Бурук Д.Н. - ознакомить под расписку работников учреждения и прикомандированных сотрудников органов, заключивших соглашения о взаимодействии в процессе предоставления государственных и муниципальных услуг, с вышеназванными правовыми актами.

Директор МБУ г. Новошахтинска «МФЦ»

« 12 » 12 2012г.

 Бурук Д.Н.

05 11.2014



Синяев П.А.

Приложение №1
к Приказу №18 от „17“ декабря 2012г.
УТВЕРЖДАЮ

Директор

МБУ «Новошахтинска «МФЦ»

И. Н. Некрасова

2012 г.



ПОЛОЖЕНИЕ

ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБРАБОТКЕ И ЗАЩИТЕ
ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ
ПЕРСОНАЛЬНЫХ ДАННЫХ МУНИЦИПАЛЬНОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ
ГОРОДА НОВОШАХТИНСКА «МНОГОФУНКЦИОНАЛЬНЫЙ ЦЕНТР ПРЕДОСТАВЛЕНИЯ
ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ»

г. Ростов-на-Дону

2012 г.

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.....	11
8. КАТЕГОРИРОВАНИЕ ПДН И КЛАССИФИКАЦИЯ ИСПДН.....	15
9. ОЦЕНКА ВОЗМОЖНОСТИ ОПТИМИЗАЦИИ ИСПДН	16
10. МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПДН	17
11. ОБУЧЕНИЕ ПЕРСОНАЛА, УЧАСТВУЮЩЕГО В ОБРАБОТКЕ ПДН.....	18
12. ДОПУСК ПЕРСОНАЛА К ОБРАБОТКЕ ПДН.....	19
13. УНИЧТОЖЕНИЕ ПДН	19
14. ОРГАНИЗАЦИЯ РАБОТЫ С НОСИТЕЛЯМИ ПДН	19
15. КОНТРОЛЬ ИЗМЕНЕНИЙ В СОСТАВЕ И СТРУКТУРЕ ИСПДН	20
16. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ФИЗИЧЕСКОГО ДОСТУПА К ЭЛЕМЕНТАМ ИСПДН.....	20
17. РЕЗЕРВИРОВАНИЕ ПДН.....	21
18. КОНТРОЛЬ ЗА ОБЕСПЕЧЕНИЕМ НЕОБХОДИМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ПДН.....	22
19. РЕАГИРОВАНИЕ НА НЕШТАТНЫЕ СИТУАЦИИ	22
20. НОРМАТИВНЫЕ ССЫЛКИ.....	23
21. КОНТРОЛЬ ВЕРСИЙ ДОКУМЕНТА	25

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 информационной системе персональных данных (далее - ИСПДн) Муниципального бюджетного учреждения города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг» (далее - Учреждение) 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 информационной системе персональных данных Учреждения;
- защита персональных данных, обрабатываемых в Учреждении, от несанкционированного доступа и от других несанкционированных действий;
- снижение уровня регуляторных рисков в отношении Учреждения.

1.3. Ответственность и область применения

Настоящий документ обязаны знать и использовать в работе руководители и сотрудники структурных подразделений Учреждения, имеющие доступ к персональным данным.

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
ТЗ	Техническое задание

Таблица 2. Перечень терминов

Наименование термина	Определение термина
Безопасность информации	Состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.
Блокирование персональных данных	Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
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.

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

Наименование термина	Определение термина
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	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.
Конфиденциальность персональных данных	Обязательное требование к операторам и иным лицам, получившим доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
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	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Обработка персональных данных	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

Наименование термина	Определение термина
Оператор	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
Ответственный за разработку нормативного документа	Должностное лицо или структурное подразделение, 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.
Структурное подразделение	Официально выделенная в организационной структуре Учреждения группа сотрудников, выполняющая определенные функции и задачи, предусмотренные Положением о структурном подразделении.
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.
Уничтожение персональных данных	Действия в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (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.

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

Наименование термина	Определение термина
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 информационной системе персональных данных, направленные на защиту интересов Учреждения в области его деятельности.

Требования Положения распространяются на все структурные подразделения Учреждения, в которых осуществляется автоматизированная и неавтоматизированная обработка персональных данных, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение функционирования информационной системы персональных данных.

Настоящее Положение разработано 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 Учреждения.

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 структурных подразделений Учреждения 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.

**Положение по организации и проведению работ
по обработке и защите ПДн 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, подразделений Учреждения;
- 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 Учреждения, регламентирующих защиту и работу с ПДн.

При работе с персональными данными, во всех случаях, не урегулированных нормативными документами Учреждения, 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.

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 относятся:

- 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 Учреждении (Приложение 1);
- контроль целей обработки ПДн, состава обрабатываемых ПДн целям обработки;
- уничтожение ПДн;
- оптимизация информационных процессов обработки ПДн;
- управление взаимодействиями с внешними контрагентами по вопросам обработки ПДн;

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

- 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.

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:

- обработка персональных данных должна осуществляться на законной и справедливой основе;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры, либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

В Учреждении 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 Учреждения;
- проведения контрольных и проверочных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

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

В качестве таких критериев в отношении персональных данных в Учреждении разрабатывается и утверждается «Перечень персональных данных, обрабатываемых в Муниципальном бюджетном учреждении города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг».

«Перечень персональных данных, обрабатываемых в Муниципальном бюджетном учреждении города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг» утверждается Директором Учреждения.

6. ОРГАНИЗАЦИОННАЯ СТРУКТУРА СЗПДн

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

Основу организационной структуры СЗПДн составляют:

- руководство;
- ответственный за обеспечение безопасности ПДн;
- администратор информационной безопасности ИСПДн;
- сотрудники Учреждения, участвующие в процессах обработки ПДн.

Директор, заместитель директора Учреждения (Руководство Учреждения) осуществляют следующие основные функции в области обеспечения безопасности ПДн:

- обеспечивают общую организацию работ по защите ПДн;
- издают приказы по вопросам организации СЗПДн;
- утверждают «Перечень персональных данных, обрабатываемых в Муниципальном бюджетном учреждении города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг»;
- назначают ответственного за обеспечение безопасности ПДн;
- рассматривают и утверждают нормативные документы Учреждения по защите ПДн;
- заслушивают при необходимости ответственных за обеспечение безопасности ПДн и других должностных лиц о состоянии работ по защите ПДн.

Ответственный за обеспечение безопасности ПДн осуществляет следующие основные функции:

- разрабатывает «Перечень ПДн, обрабатываемых в Муниципальном бюджетном учреждении города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг»;
- проводит классификацию ИСПДн;
- распределяет ответственность по вопросам обработки и защиты ПДн;
- определяет допустимые сроки хранения ПДн по каждой категории ПДн;
- организует подачу Уведомлений в Уполномоченный орган по защите прав субъектов ПДн;

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

- заслушивает руководителей структурных подразделений о принимаемых мерах по состоянию и совершенствованию СЗПДн;
- организует работы по разработке, изменению и уточнению политик, регламентов, стандартов в части защиты ПДн;
- осуществляет организацию плановых и внеплановых проверочных мероприятий;
- организует выполнение требований по защите ПДн в Учреждении;
- проводит разработку и актуализацию нормативных документов, регламентирующих защиту ПДн;
- разрабатывает и актуализирует Модели угроз безопасности ПДн и технические задания на СЗПДн;
- разрабатывает (актуализирует) проектную документацию на СЗПДн;
- подготавливает проекты решений по изменению «Перечня персональных данных, обрабатываемых в Учреждении, классификации ИСПДн, Уведомления об обработке ПДн и других коллегиальных решений по обработке и обеспечению безопасности ПДн в Учреждении;
- определяет необходимость обучения сотрудников вопросам обеспечения безопасности ПДн, а также определяет формы и программы обучения сотрудников Учреждения в области защиты ПДн;
- организует работы по сбору сведений об изменениях в составе и структуре ИСПДн;
- осуществляет контроль соответствия изменений в составе и архитектуре ИСПДн требованиям нормативных документов Российской Федерации по защите ПДн, а также внутренних организационно-распорядительных документов Учреждения;
- контролирует исполнение требований по уничтожению ПДн;
- разрабатывает рекомендации по оптимизации существующих и новых информационных процессов обработки ПДн по критериям соответствия требованиям по защите ПДн и минимизации затрат на создание и эксплуатацию системы защиты ПДн;
- контролирует исполнение требований нормативных документов Учреждения в области обеспечения безопасности ПДн, структурными подразделениями и сотрудниками;
- организует и осуществляет взаимодействие с регуляторами по вопросам защиты ПДн;
- организует получение лицензий ФСТЭК России и ФСБ России по технической и криптографической защите конфиденциальной информации, необходимые в целях защиты ПДн;
- проводит работы по классификации ИСПДн;
- отслеживает необходимость и организует работы по сертификации (подтверждению сертификата), применяемых средств и систем защиты ПДн;
- управляет проектами по внедрению систем и средств защиты ПДн;
- контролирует ввод в действие, эксплуатацию СЗПДн;
- проводит расследования инцидентов, связанных с нарушением безопасности ПДн, правил обработки ПДн, принимает меры по недопущению повторения нештатных ситуаций;
- 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 4.

Администратор ИБ ИСПДн осуществляет следующие основные функции:

- осуществляет сопровождение средств и систем защиты ПДн;
- проводит оперативный контроль функционирования средств и систем защиты ПДн;

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

- проводит резервирование ПДн;
- контролирует факты обращений пользователей ИСПДн к персональным данным, зарегистрированные в электронном журнале обращений пользователей к соответствующим ресурсам ИСПДн;
- осуществляет выявление и регистрацию попыток НСД к компонентам ИСПДн, информационным ресурсам;
- контролирует соответствие технических, программных и программно-аппаратных средств ИСПДн требованиям, предъявляемым к ним средствами и системой защиты ПДн;
- проводит оценку эффективности принятых мер и применяемых средств защиты ПДн;
- проводит занятия с сотрудниками по изучению организационно-распорядительных документов по всему комплексу вопросов защиты ПДн;
- осуществляет учет применяемых средств защиты ПДн, эксплуатационной и технической документации к ним;
- контролирует выполнение сотрудниками подразделения требований по защите ПДн;
- участвует в расследованиях причин возникновения нештатных ситуаций;
- готовит предложения по совершенствованию системы защиты ПДн;
- выполняет комплекс мероприятий по защите информации при проведении ремонтных и регламентных работ;
- обеспечивает защиту ПДн при выводе из эксплуатации компонентов ИСПДн.

Сотрудники Учреждения 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 подразделения;
- ведут учет носителей персональных данных;
- соблюдают требования нормативных документов по защите ПДн;
- осуществляют обработку ПДн в соответствии с заданием и предоставленными полномочиями.

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

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;

**Положение по организации и проведению работ
по обработке и защите ПДн в 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
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
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.
1.3.	определение предварительной категории ПДн	Детализация проводимых работ приведена в разделе 8
1.4.	определение предварительного класса ИСПДн	Детализация проводимых работ приведена в разделе 8
1.5.	оценивается возможность оптимизации ИСПДн	Детализация проводимых работ приведена в разделе 9
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 Учреждения в обработке ПДн и необходимые юридические основания для такой обработки; ▪ соответствия предполагаемых процессов обработки ПДн принципам их обработки (см. раздел 4).
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
2.	Реализация проекта ИСПДн – концепция реализации ИСПДн/СЗПДн	
2.1.	определяется необходимость корректировки «Перечня ПДн», при необходимости проводится его корректировка	
2.2.	построение модели информационных потоков персональных данных	
2.3.	определение перечня актуальных угроз	Детализация проводимых работ приведена в разделе 10

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн
	безопасности ПДн в конкретных условиях функционирования (разработка модели угроз и нарушителя безопасности ПДн)	
2.4.	определение категорий ПДн и класса ИСПДн	Детализация проводимых работ приведена в разделе 8
2.5.	определение необходимости создания СЗПДн	На данном этапе на основе класса ИСПДн определяется необходимость создания СЗПДн ¹
2.6.	разработка технического задания на разработку СЗПДн	На данном этапе определяются требования к техническим, программным, программно-аппаратным и организационным средствам и мерам обеспечения безопасности ПДн.
3.	Реализация проекта ИСПДн – проектирование ИСПДн	
3.1.	разработка эскизного проекта на СЗПДн	На данном этапе разрабатывается: ▪ пояснительная записка; ▪ схема структурная комплекса технических средств.
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.
3.3.	разработка эксплуатационной документации на ИСПДн	Производится разработка положений, регламентов, инструкций, определяющих частный порядок защиты ПДн в данной ИСПДн
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.
4.2.	реализация требований по физической защите компонентов ИСПДн и носителей ПДн	Производятся монтажные работы средств физической защиты (замков, шкафов, сейфов и т.п.)
4.3.	заключаются договора с контрагентами, которые будут осуществлять обработку ПДн Учреждения, с учетом требований по защите ПДн (при необходимости)	На данном этапе определяются договора, в которые должны быть внесены изменения. В данные договора вносятся требования по обеспечению конфиденциальности ПДн контрагентами, которые будут иметь к ним доступ.
4.4.	определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации	
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

¹ Для ИСПДн 4 класса создание СЗПДн не обязательно (по решению руководства Учреждения)

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн
5.2.	проводится ознакомление сотрудников с нормативными документами в области защиты ПДн	
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)	
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
6.3.	проводится опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн	
6.4.	проводятся приемочные испытания СЗПДн	
7.	Эксплуатация ИСПДн	
7.1.	допуск персонала к обработке ПДн	Детализация проводимых работ приведена в разделе 12
7.2.	производится уничтожение ПДн	Детализация проводимых работ приведена в разделе 13
7.3.	производится работа с носителями ПДн	Детализация проводимых работ приведена в разделе 14
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
7.5.	осуществляется контроль изменений в составе и структуре ИСПДн	Детализация проводимых работ приведена в разделе 15
7.6.	обеспечивается защита от несанкционированного физического доступа к элементам ИСПДн	Детализация проводимых работ приведена в разделе 16
7.7.	осуществляется резервирование ПДн	Детализация проводимых работ приведена в разделе 17
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 на СЗПДн
7.9.	осуществляется контроль за обеспечением	Детализация проводимых работ приведена в разделе 18

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн
	необходимого уровня защищенности ПДн	
7.10.	производится реагирование на нештатные ситуации	Детализация проводимых работ приведена в разделе 19
7.11.	проводится обучение персонала правилам обеспечения безопасности ПДн	Детализация проводимых работ приведена в разделе 11
7.12.	осуществляется взаимодействие с субъектами ПДн по вопросам обработки их ПДн	Взаимодействие с субъектами ПДн производится в порядке, определенном законодательством РФ
7.13.	осуществляется взаимодействие с регуляторными органами по вопросам защиты ПДн	
8.	Модернизация ИСПДн	
8.1.	осуществляется управление изменениями в ИСПДн	Детализация проводимых работ приведена в разделе 15
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
8.3.	на основе оценки существенности модернизации, проводится необходимый объем мероприятий ²	
9.	Вывод из эксплуатации ИСПДн	
9.1.	производится уничтожение ПДн	Детализация проводимых работ приведена в разделе 13
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

8. КАТЕГОРИРОВАНИЕ ПДн И КЛАССИФИКАЦИЯ ИСПДн

Классификация ИСПДн и категорирование ПДн проводятся в соответствии с Порядком проведения классификации информационных систем персональных данных (утвержден 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.

² Объем необходимых мероприятий определяется ответственным за обеспечение безопасности ПДн

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

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 (утвержден Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20):

- все ИСПДн Учреждения 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.

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:

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

- 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 сотрудников 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 структурных подразделений, 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 ответственным 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 структурных подразделений Учреждения, так и для Учреждения 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 структурным подразделениям. Состав группы не должен превышать 20-25 человек.

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

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 структурных подразделений 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.

Форма Перечня должностных лиц, имеющих доступ к персональным данным представлена в Приложении 3.

Перечни должностных лиц составляются и ведутся на основании данных о должностных лицах, допущенных к ПДн, подаваемых руководителями структурных подразделений.

Доступ конкретных лиц к ПДн и ИСПДн осуществляется на основании служебных записок (заявок). Служебные записки на доступ учитываются и хранятся у Администратора ИБ ИСПДн.

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 Муниципального бюджетного учреждения города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг».

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 Муниципальном бюджетном учреждении города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг».

Решение об уничтожении ПДн, организацию и проведение уничтожения принимает и осуществляет постоянная комиссия, назначенная приказом директора.

После проведенного уничтожения должен быть подготовлен акт об уничтожении ПДн, форма акта приведена в Приложении 5.

14. ОРГАНИЗАЦИЯ РАБОТЫ С НОСИТЕЛЯМИ ПДН

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

- оформление носителей, содержащих персональные данные;

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

- 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 внутренних организационно-распорядительных 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

**Положение по организации и проведению работ
по обработке и защите ПДн в 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 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 работники), должно допускаться только в присутствии работников, 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 на создание СЗПДн.

Мероприятия по контролю доступа на территорию должны исключить неконтролируемое нахождение посетителей на территории Учреждения.

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 Муниципального бюджетного учреждения города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг».

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 администратора ИБ ИСПДн.

Ответственность за плановый контроль эффективности обеспечения безопасности ПДн возлагается на ответственного за обеспечение безопасности ПДн.

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

Внезапные проверки эффективности при необходимости могут проводиться специальными группами по решению ответственного 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, 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 Учреждении.

19. РЕАГИРОВАНИЕ НА НЕШТАТНЫЕ СИТУАЦИИ

Для эффективного реагирования на нештатные ситуации, возникающие при обработке ПДн, в Учреждении 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 1-2 раз в год) проверяться посредством проведения учений с корректировкой порядков по результатам проведенных проверок.

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

В рамках данного процесса должны решаться следующие задачи:

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

- 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 персонала в нештатных ситуациях Муниципального бюджетного учреждения города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг».

20. НОРМАТИВНЫЕ ССЫЛКИ

Таблица 20.1. 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 06.04.2011 N 63-ФЗ "Об электронной 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».
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».

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

№ п/п	Наименование документа
20	Положение о государственном лицензировании деятельности в области защиты информации от 27 апреля 1994 № 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.
35	РД Гостехкомиссии России. «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных 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, 1994г.
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 года № 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.

**Положение по организации и проведению работ
по обработке и защите ПДн в ИСПДн**

№ п/п	Наименование документа
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.

21. КОНТРОЛЬ ВЕРСИЙ ДОКУМЕНТА

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

Дата 29.12.2017

№ 80

г. Новошахтинск

муниципальное
бюджетное учреждение
города Новошахтинска
«Многофункциональный
центр предоставления
государственных и
муниципальных услуг»

ул. Садовая, д.32,
корп.1,
г. Новошахтинск,
Тел. 8(86369) 2-03-19
Факс 8(86369) 2-08-94
Эл. почта
mfc-nov@mail.ru

О внесении изменений в приказ от 17.12.2012 № 18
«Об утверждении Положения по организации и проведению работ
по обработке и защите персональных данных, обрабатываемых в
информационной системе персональных данных муниципального
бюджетного учреждения города Новошахтинска
«Многофункциональный центр предоставления
государственных и муниципальных услуг»
от 17 декабря 2012 года.»

В целях приведения локальных правовых актов в соответствие
требованиям законодательства, регулирующего отношения, связанные с
обработкой персональных данных,

ПРИКАЗЫВАЮ:

1. Внести изменения в приказ от 17.12.2012 № 18 «Об утверждении Положения по организации и проведению работ по обработке и защите персональных данных, обрабатываемых в информационной системе персональных данных муниципального бюджетного учреждения города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг» от 17 декабря 2012 года.» согласно приложению к приказу.
2. Настоящий приказ вступает в силу с момента его подписания.
3. Контроль исполнения приказа оставляю за собой.

Директор



И.М. Сидоров

Директор МБУ г. Новошахтинска «МФЦ»



И.М. Сидоров

ИЗМЕНЕНИЯ,

вносимые в приказ от 17.12.2012 № 18

«Об утверждении Положения по организации и проведению работ по обработке и защите персональных данных, обрабатываемых в информационной системе персональных данных муниципального бюджетного учреждения города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг» от 17 декабря 2012 года.»

1. В приказе:

1.1. Наименование изложить в следующей редакции:

«Об утверждении Положения по организации и проведению работ по обработке и защите персональных данных, обрабатываемых в информационной системе персональных данных муниципального бюджетного учреждения города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг»».

1.2. Преамбулу изложить в следующей редакции:

«В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», ПРИКАЗЫВАЮ:».

1.3. В распорядительную часть изложить в следующей редакции:

«1. Утвердить Положение по организации и проведению работ по обработке и защите персональных данных, обрабатываемых в информационной системе персональных данных муниципального бюджетного учреждения города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг» (далее – Положение) согласно приложению.

2. Ответственным за контроль выполнения работниками учреждения Положения определить главного специалиста-программиста МБУ г. Новошахтинска «МФЦ» (П.А. Силаев) (далее – главный специалист-программист).

3. Действия по ознакомлению с Положением под расписку осуществлять:

3.1. Заместителю директора (М.В. Кульбицкая) в отношении вновь принимаемых главных специалистов-программистов.

3.2. Главному специалисту-программисту в отношении работников учреждения».

2. В Приложении («Положение по организации и проведению работ по обработке и защите персональных данных, обрабатываемых в информационной системе персональных данных муниципального бюджетного учреждения города Новошахтинска «Многофункциональный центр предоставления государственных и муниципальных услуг»):

2.1. Пункт 1.3. раздела 1 изложить в следующей редакции:

«1.3. Ответственность

Работники Учреждения, имеющие доступ к персональным данным, несут ответственность за несоблюдение требований, предъявляемым при обработке персональных данных, в соответствии с законодательством Российской Федерации».

2.2. В Пункте 1.4. раздела 1:

2.2.1. После Таблицы 1. «Перечень сокращений» дополнить абзацем в следующей редакции:

«В настоящем Положении используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ)».

2.2.2. В Таблице 2. «Перечень терминов» исключить строки: 2,19, 20,21,22.

2.3. По тексту Приложения слова «Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в соответствующем падеже заменить словами «Федеральный закон № 152-ФЗ» в соответствующем падеже.

2.4. Абзац 3 раздела 2 изложить в следующей редакции:

«Настоящее Положение разработано в соответствии с:

Трудовым кодексом Российской Федерации,

Кодексом Российской Федерации об административных правонарушениях,

Федеральным законом № 152-ФЗ,

Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,

Федеральным законом от 25.12.2008 № 273-ФЗ «О противодействии коррупции»,

Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее – Федеральный закон № 210-ФЗ),

Федеральным законом от 02.09.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»,

постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

иными нормативными документами в сфере обработки ПДн.

2.5. Раздел 8 изложить в следующей редакции:

«8. КАТЕГОРИРОВАНИЕ ПДН И КЛАССИФИКАЦИЯ ИСПДН

Классификация ИСПДН и категорирование ПДн осуществляются в порядке, установленном законодательством Российской Федерации.

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

2.6. Раздел 10 изложить в следующей редакции:

«10. МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПДН

СЗПДн внедряется для нейтрализации актуальных угроз безопасности ПДн.

Оценка актуальности угроз производится посредством разработки модели угроз и нарушителя безопасности ПДн (далее – Модель угроз).

Модель угроз должна содержать:

- перечень актуальных угроз;
- вывод о классе ИСПДн;
- вывод о типе нарушителя, существующем в ИСПДн и требуемом классе средств криптографической защиты информации;
- описание структуры и состава ИСПДн;
- 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 об ограничениях на эти возможности, предположения о каналах атак и средствах атак, выводы о типе нарушителя).».

2.7. Раздел 12 изложить в следующей редакции:

«12. ДОПУСК РАБОТНИКОВ УЧРЕЖДЕНИЯ К ОБРАБОТКЕ ПДН

Предоставление доступа работникам Учреждения к обработке ПДн осуществляется в соответствии с Инструкцией по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ИСПДн Учреждения.

Перечень должностей Учреждения, имеющих доступ к ПДн (ответственных за обработку ПДн) представлена в Приложении 6 к настоящему Положению.»

2.8. Раздел 13 изложить в следующей редакции:

«13. УНИЧТОЖЕНИЕ ПДН

Уничтожение ПДн осуществляется в следующих случаях:

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

ПДн не уничтожаются в случаях, если:

- договором, соглашением, стороной которого, выгодоприобретателем или поручителем является субъект ПДн, предусмотрен иной порядок обработки ПДн;
- законодательством установлены сроки обязательного архивного хранения материальных носителей ПДн;
- в иных случаях, прямо предусмотренных законодательством.

Уничтожение части ПДн, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих ПДн, с сохранением возможности обработки иных ПДн, зафиксированных на материальном носителе.

В случае выявления недостоверности ПДн, неправомерности действий с ПДн оператор осуществляет блокирование указанных персональных данных и в срок, не превышающий трех рабочих дней с даты такого выявления, устраняет допущенные нарушения.

В случае подтверждения факта недостоверности персональных данных оператор уточняет персональные данные и снимает с них блокирование на основании документов, представленных:

- субъектом ПДн (его представителем);
- уполномоченным органом по защите прав субъектов ПДн;
- иными лицами в соответствии с законодательством.

В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерности действий с ПДн, уничтожает ПДн.

Об устранении допущенных нарушений или об уничтожении ПДн оператор уведомляет субъекта ПДн (его представителя) и (или) уполномоченный орган по защите прав субъектов ПДн в срок, не превышающий десяти рабочих дней с даты устранения допущенных нарушений или уничтожения ПДн.

В случае отзыва субъектом ПДн согласия на обработку своих ПДн оператор прекращает обработку ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожает ПДн в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено законодательством.

Уничтожение документов, содержащих ПДн, утративших свое практическое значение и не подлежащих архивному хранению, производится на основании акта уничтожения ПДн.

Уничтожение по окончании срока обработки ПДн на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление ПДн, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

Контроль сроков хранения, целей обработки ПДн осуществляется на основании сроков хранения и целей, указанных для конкретных категорий ПДн в Перечне ПДн, обрабатываемых в Учреждении.

Решение об уничтожении ПДн, организацию и проведение уничтожения принимает и осуществляет комиссия по уничтожению носителей ПДн (далее – Комиссия) с учетом положений настоящего раздела.

Состав Комиссии, положение о Комиссии утверждается директором Учреждения.».

2.9. В разделе 14 абзац второй исключить.

2.10. Раздел 19 изложить в следующей редакции:

«19. РЕАГИРОВАНИЕ НА НЕШТАТНЫЕ СИТУАЦИИ

Реагирование на нештатные ситуации должно осуществляться в соответствии с Инструкцией по действиям пользователей ИСПДн Учреждения в нештатных ситуациях.».

2.11. В Разделе 20 в таблице 20.1. «Внешние нормативные и распорядительные документы»:

2.11.1. Признать утратившими силу строки: 13, 16, 17, 18, 21, 43.

2.11.2. Строку 23 изложить в следующей редакции:

«23	Приказ Росстандарта от 24.09.2012 № 423-ст «Об утверждении национального стандарта»
-----	---

2.12. Приложение 5 к настоящему Положению изложить в следующей редакции:
«Приложение 5 – ПЕРЕЧЕНЬ должностей работников МБУ г. Новошахтинска «МФЦ», являющихся ответственными за обработку персональных данных в ИСПДн

Должность	Наименование ИСПДн
Ответственный за обеспечение безопасности персональных данных	
Администратор ИСПДн, Администратор информационной безопасности	
Главный специалист-программист	Интегрированная информационная система Единой сети многофункциональных центров предоставления государственных и муниципальных услуг Ростовской области (далее – ИИС ЕС МФЦ РО); 1 С:Предприятие 8.3
Операторы ИСПДн с правами записи	
Специалист-программист	ИИС ЕС МФЦ РО
Директор	
Заместитель директора	
Главный специалист (юрист)	
Начальник контрольно-аналитического сектора	
Ведущий специалист контрольно-аналитического сектора	
Специалист контрольно-аналитического сектора	
Начальник отдела по работе с населением	
Главный специалист отдела по работе с населением	
Главный бухгалтер	1 С:Предприятие 8.3»
Бухгалтер	