РАСПОРЯЖЕНИЕ
главы администрации Октябрьского района города Ставрополя Ставропольского края

17.01 .2019 № 4-р

О внесении изменений в распоряжение главы администрации Октябрьского района города Ставрополя от 11.08.2017 №171 «Об организации работ с персональными данными»

В соответствии с Федеральными законами от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства РФ от 15 июля 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

1. Внести в Положение о персональных данных администрации Октябрьского района города Ставрополя, утвержденное приложением 2 к распоряжению главы администрации Октябрьского района города Ставрополя от 11.08.2017 № 171 «Об организации работ с персональными данными» следующие изменения:

1) пункт 1.1. изложить в следующей редакции:

«1.1. Настоящее Положение разработано на основании ст.ст. 86-90 Трудового кодекса Российской Федерации, Федеральный закон от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных», Федеральный закон от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации», Решение Ставропольской городской думы от 25.04.208 №81 «Об уставе муниципального образования города Ставрополя Ставропольского края.»;

2) пункт 1.5. изложить в следующей редакции:

«1.5. К субъектам персональных данных (далее – субъекты) относятся лица – носители персональных данных, персональные данные которых переданы администрации (как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов) для обработки (в том числе передачи), в том числе:

- граждане Российской Федерации,
- работники, состоящие в трудовых отношениях с администрацией Октябрьского района города Ставрополя.»;

3) пункт 4.2. изложить в следующей редакции:

«4.2. Обработка персональных данных субъекта персональных данных

может осуществляться с целью обработки, регистрации, систематизации сведений, необходимых для реализации полномочий органов местного самоуправления; а так же сбор, запись. систематизация, накопление, хранение, уточнение, (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.».

2. Внести изменения в пункт 1.1.1. Перечня персональных данных, обрабатываемых администрацией Октябрьского района города Ставрополя, утвержденный приложением 3 к распоряжению главы администрации Октябрьского района города Ставрополя от 11.08.2017 № 171 «Об организации работ персональными данными» изложив его в следующей редакции:

«1.1.1. Перечень персональных данных субъектов Пдн

Персональные данные субъектов ПДн включают:

Фамилия, имя, отчество;

Место, год и дата рождения;

Имущественное положение;

Адрес регистрации;

Адрес места фактического проживания (пребывания);

Паспортные данные (серия, номер паспорта, кем и когда выдан);

Телефонный номер (домашний, рабочий, мобильный);

Семейное положение и состав семьи (муж/жена, дети);

Данные о состоянии здоровья;

Социальное положение;

Образование;

Профессия;

Доходы;

Другая необходимая информация (ИНН, медицинский полис, страховое свидетельство)».

3. Настоящее распоряжение вступает в силу со дня его подписания.

4. Контроль исполнения настоящего распоряжения оставляю за собой.

Глава администрации
Октябрьского района
города Ставрополя А.А. Ломанов

РАСПОРЯЖЕНИЕ
главы администрации Октябрьского района города Ставрополя Ставропольского края

11 .08 .2017 № 171

Об организации работ с персональными данными

В соответствии с Федеральными законами от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также постановлением Правительства РФ от 15 июля 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

ПРИКАЗЫВАЮ:

1. Утвердить Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации Октябрьского района города Ставрополя (далее – администрация района) согласно приложению 1.

1. Утвердить Положение о персональных данных администрации района согласно приложению 2.

2. Утвердить Перечень персональных данных, обрабатываемых в администрации района согласно приложению 3.

3. Утвердить Положение о порядке обеспечения безопасности персональных данных с использованием средств криптографической защиты информации согласно приложению 4.

4. Утвердить Порядок парольной защиты в информационных системах персональных данных администрации района согласно приложению 5.

5. Утвердить Инструкцию о порядке обработки персональных данных в администрации района согласно приложению 6.

6. Утвердить Инструкцию администратора информационной безопасности информационной системы персональных данных администрации района согласно приложению 7.

7. Утвердить Инструкцию по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем персональных данных администрации района согласно приложению 8.

8. Утвердить Инструкцию пользователя информационных систем персональных данных администрации района согласно приложению 9.

9. Утвердить Инструкцию по действиям пользователей информационных систем персональных данных администрации района в нештатных ситуациях согласно приложению 10.

10. Утвердить Инструкцию по организации антивирусной защиты информационных систем персональных данных администрации района согласно приложению 11.

11. Утвердить Инструкцию по резервному копированию защищаемой информации в информационных системах персональных данных администрации района согласно приложению 12.

12. Утвердить Инструкцию по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных администрации района согласно приложению 13.

13. Утвердить Регламент учета средств защиты, документации и электронных носителей персональных данных администрации района согласно приложению 14.

14. Утвердить Инструкцию по порядку проведения проверок состояния защиты персональных данных администрации района согласно приложению 15.

15. Утвердить Регламент доступа в помещения с компонентами информационных систем персональных данных и на территории администрации района согласно приложению 16.

16. Утвердить форму журнала регистрации письменных запросов граждан на доступ к своим персональным данным согласно приложению 17.

17. Настоящее распоряжение вступает в силу со дня его подписания.

18. Контроль исполнения настоящего приказа оставляю за собой.

Глава администрации
Октябрьского района
города Ставрополя А.А. Ломанов

8. Утвердить Инструкцию пользователя информационных систем персональных данных администрации района согласно приложению 9.

9. Утвердить Инструкцию по действиям пользователей информационных систем персональных данных администрации района в нештатных ситуациях согласно приложению 10.

10. Утвердить Инструкцию по организации антивирусной защиты информационных систем персональных данных администрации района согласно приложению 11.

11. Утвердить Инструкцию по резервному копированию защищаемой информации в информационных системах персональных данных администрации района согласно приложению 12.

12. Утвердить Инструкцию по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных администрации района согласно приложению 13.

13. Утвердить Регламент учета средств защиты, документации и электронных носителей персональных данных администрации района согласно приложению 14.

14. Утвердить Инструкцию по порядку проведения проверок состояния защиты персональных данных администрации района согласно приложению 15.

15. Утвердить Регламент доступа в помещения с компонентами информационных систем персональных данных и на территории администрации района согласно приложению 16.

16. Утвердить форму журнала регистрации письменных запросов граждан на доступ к своим персональным данным согласно приложению 17.

17. Настоящее распоряжение вступает в силу со дня его подписания.

18. Контроль исполнения настоящего распоряжения оставляю за собой.

Глава администрации
Октябрьского района
города Ставрополя А.А. Ломанов

Приложение № 1
к приказу главы администрации
Октябрьского района города Ставрополя
от «16» 08 2017 г. № 141

Положение
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации Октябрьского района города Ставрополя

г. Ставрополь

2017

СОДЕРЖАНИЕ

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 администрации Октябрьского района города Ставрополя (далее – Администрация) 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 Администрации;
- защита персональных данных, обрабатываемых в Администрации, от несанкционированного доступа и от других несанкционированных действий;
- снижение уровня регуляторных рисков в отношении Администрации.

1.3.Ответственность и область применения

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

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
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.

Наименование термина	Определение термина
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 Управления 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.
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.

Наименование термина	Определение термина
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 Администрации в области его деятельности, обеспечение непрерывности деятельности Администрации.

Требования Положения распространяются на все отделы Администрации, 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 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»;
- Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 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 Администрации 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 Администрации;
- 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 Администрации, регламентирующих защиту и работу с ПДн.

При работе с персональными данными, во всех случаях, не урегулированных нормативными документами Администрации, 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];
- адекватности[3].

---

[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.

[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).

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 Администрации (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;
- 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 Администрации 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 Администрации;
- проведения контрольных и проверочных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

Обработка персональных данных в Администрации осуществляется только с согласия субъектов персональных данных. Форма журнала представлена с Инструкцией о порядке обработки персональных данных в администрации Октябрьского района города Ставрополе.

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 Администрации к соответствующим категориям информации представляет собой процесс обоснованного установления (документального оформления и утверждения главой администрации Октябрьского района города Ставрополя) критериев их выделения из всей совокупности сведений, находящихся в обращении.

В качестве таких критериев в отношении персональных данных в Администрации разрабатывается и утверждается «Перечень персональных данных, обрабатываемых в администрации Октябрьского района города Ставрополя».

Перечень персональных данных, обрабатываемых в администрации Октябрьского района города Ставрополя, утверждается главой Администрации».

6. ОРГАНИЗАЦИОННАЯ СТРУКТУРА СЗПДН

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

Основу организационной структуры СЗПДн составляют:

- руководство;
- отдел правового обеспечения и приема граждан:
- общий отдел;
- ответственные за обеспечение безопасности ПДн;
- администраторы ИСПДн[4];
- владельцы ИСПДн и процессов обработки ПДн;
- отделы, участвующие в процессах обработки ПДн;
- сотрудники администрации Октябрьского района города Ставрополя.

Глава администрации Октябрьского района города Ставрополя 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 Администрации»;
- назначает ответственного за обеспечение безопасности ПДн;
- рассматривает и утверждает нормативные документы администрации Октябрьского района города Ставрополя по защите ПДн;

---

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

- заслушивает при необходимости ответственных за обеспечение безопасности ПДн и других должностных лиц о состоянии работ по защите ПДн.

Отделы правового и кадрового обеспечения осуществляет следующие основные функции:

- дают юридическую оценку возможности создания (модернизации) ИСПДн.
- проводят ознакомление сотрудников с нормативными документами в области защиты ПДн и делают 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 Администрации»;
- 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 Администрации;
- 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 администрации Октябрьского района города Ставрополя, классификации ИСПДн, Уведомления об обработке ПДн и других коллегиальных решений по обработке и обеспечению безопасности ПДн в Администрации;
- определяют необходимость обучения сотрудников вопросам обеспечения безопасности ПДн, а также определяют формы и программы обучения сотрудников Администрации 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 Администрации;
- 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 Администрации 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 Администрации, 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 Администрации 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 Администрации могут создаваться рабочие группы, в состав которых должны входить представители руководства всех заинтересованных отделов Администрации.

Распределение ролей, полномочий, ответственности по обеспечению безопасности ПДн осуществляется в соответствии с нормативными документами Администрации, 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 Управления 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**		
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

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
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 обработку ПДн Администрации, 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.	С автоматизированной обработкой С неавтоматизированной обработкой
4.4.	определение отдела и назначение лиц, ответственных за эксплуатацию средств защиты информации		С автоматизированной обработкой С неавтоматизированной обработкой

[5] Для ИСПДн 4 класса создание СЗПДн не обязательно (по решению главы Администрации)

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
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
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,	Учет средств защиты информации, эксплуатационной документации производится администраторами ИСПДн,	С автоматизированной обработкой

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
		мероприятий по защите ПДн	
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 Администрации 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.

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.

---

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

№	Стадия существования ИСПДн, работы по защите ПДн	Детализация проводимых работ по защите ПДн	На какие типы ИСПДн распространяется
	эксплуатационной документации к ним	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	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**		
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	С автоматизированной обработкой С неавтоматизированной обработкой

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 Администрации, так и для Администрации 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 Администрации».

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 Администрации 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 Администрации и т.п.

19. РЕАГИРОВАНИЕ НА НЕШТАТНЫЕ СИТУАЦИИ

Для эффективного реагирования на нештатные ситуации, возникающие при обработке ПДн, в Администрации 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 Администрации 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 Администрации в нештатных ситуациях.

20. КОНТРОЛЬ ЛОЯЛЬНОСТИ ПЕРСОНАЛА

В Администрации 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 Администрации.

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».
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».

№ п/п	Наименование документа
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.
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.

№ п/п	Наименование документа
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				

23. ПРИЛОЖЕНИЕ 2 – ФОРМА АКТА КЛАССИФИКАЦИИ ИСПДН

УТВЕРЖДАЮ
Глава администрации
Октябрьского района
города Ставрополя

_____ А.А. Ломанов
«___»_____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

Председатель: _____

Члены комиссии:
_____
_____
_____

УТВЕРЖДАЮ

Глава Администрации Октябрьского района города Ставрополя

_____ А.А. Ломанов

«___»_____20__ г.

Исходные данные классификации информационных систем персональных данных управления

Наименование информационной системы персональных данных	Исходные данные классификации информационной системы							Примечание
	Категория персональных данных	Объем обрабатываемых персональных данных (количество субъектов персональных данных)	Структура информационной системы персональных данных	Наличие подключений к сетям и системам общего пользования и сетям международного информационного обмена (Интернет)	Режим обработки персональных данных	Разграничение доступа пользователей	Нахождение информационной системы (ее составных частей) за пределами России	

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

Глава Администрации Октябрьского района города Ставрополя

_____ А.А. Ломанов

«___»_____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.
(прописью) (цифрами)

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)

Приложение №2
к приказу главы Администрации
Октябрьского района города Ставрополя

от «11» 08 2017 г. № 171

Положение

о персональных данных Администрации Октябрьского района города Ставрополя

г. Ставрополь
2017 г.

1. Общие положения

1.1. Настоящее разработано на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и других нормативно-правовых актов Российской Федерации.

1.2. Настоящим Положением определяется порядок обработки, т.е. действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных работников и посетителей Администрации Октябрьского района города Ставрополя с использованием средств автоматизации или без использования таких средств.

1.3. Целью настоящего Положения является обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных работников, посетителей Управления, а также персональных данных иных лиц, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных источниках персональных данных.

1.4. Основные термины и определения, применяемые в настоящем Положении:

1.4.1. **Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации, Перечнем ПДн, обрабатываемых в Администрации Октябрьского района города Ставрополя, настоящим Положением и локальными актами администрации.

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

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

1.4.4. **Использование персональных данных** – действия (операции) с

персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

1.4.6. **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.

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

1.4.8. **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.

1.4.9**. Конфиденциальная информация** – информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем.

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

Обеспечения конфиденциальности персональных данных не требуется:

– в случае обезличивания персональных данных;

– в отношении общедоступных персональных данных.

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

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных (Приложение № 6) могут включаться фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные данным субъектом.

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по

требованию субъекта или по решению главы Администрации Октябрьского района города Ставрополя, либо по решению суда или иных уполномоченных государственных органов.

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

1.4.13. **Работники** – лица, состоящие в трудовых отношениях с Администрации Октябрьского района города Ставрополя, либо кандидаты на вакантную должность, вступившие в отношения по поводу приема на работу.

1.4.14. **Оператор** – лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

1.5. **К субъектам персональных данных** (далее – субъекты) относятся лица – носители персональных данных, персональные данные которых переданы администрации (как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов) для обработки (в том числе передачи), в том числе:

– работники Администрации Октябрьского района города Ставрополя, включая совместителей, а также лица, выполняющие работы по договорам гражданско-правового характера;

– иные лица, предоставляющие персональные данные администрации.

1.6. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями Администрации Октябрьского района города Ставрополя.

1.7. Обработка персональных данных субъекта персональных данных без письменного его согласия не допускается, если иное не определено законом. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении сроков хранения, если иное не определено законом.

1.8. Сотрудники Администрации Октябрьского района города Ставрополя, в обязанности которых входит обработка персональных данных субъектов персональных данных, обязаны обеспечить каждому субъекту персональных данных возможность ознакомления со своими персональными данными, если иное не предусмотрено законом.

1.9. Персональные данные не могут быть использованы в целях:

– причинения имущественного и морального вреда гражданам;

– затруднения реализации прав и свобод граждан Российской Федерации.

1.10. Настоящее Положение и изменения к нему утверждаются главой Администрации Октябрьского района города Ставрополя, являются

обязательным для исполнения всеми сотрудниками Администрации Октябрьского района города Ставрополя, имеющими доступ к персональным данным субъектов персональных данных Администрации Октябрьского района города Ставрополя.

Все сотрудники Администрации Октябрьского района города Ставрополя, имеющие доступ к персональным данным, должны быть ознакомлены под роспись с настоящим Положением в редакции, действующей на момент указанного ознакомления (Приложение № 1).

2. Принципы обработки персональных данных

2.1. Обработка персональных данных в Администрации Октябрьского района города Ставрополя осуществляется на основе следующих принципов:

– 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 Администрации Октябрьского района города Ставрополя;

– 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.

2.2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Персональные данные подлежат уничтожению по достижению целей обработки или в случае утраты необходимости в их достижении.

2.3. Субъект персональных данных является собственником своих персональных данных и самостоятельно решает вопрос передачи Администрации Октябрьского района города Ставрополя своих персональных данных.

2.4. Держателем персональных данных является Администрация Октябрьского района города Ставрополя, которой субъект персональных данных передает свои персональные данные. Администрация Октябрьского района города Ставрополя выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

2.5. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику и (или) держателю персональных данных за получением необходимых сведений и

пользующиеся ими с соблюдением требований по обеспечению безопасности персональных данных.

3. Понятие и состав персональных данных

3.1. Под персональными данными субъектов персональных данных понимается информация, необходимая Администрации Октябрьского района города Ставрополя в связи с трудовыми отношениями и касающаяся конкретного субъекта персональных данных (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное и имущественное положение, образование, профессия, доходы, другая информация), а также сведения о фактах, событиях и обстоятельствах жизни субъекта, позволяющие идентифицировать его личность. К персональным данным относятся следующие сведения:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы работника;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате работника, иных выплатах субъектам персональных данных (включая стипендии);
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства (пребывания), номер домашнего телефона;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора (контракта);
- состав декларируемых сведений о доходах, об имуществе и обязательствах имущественного характера;
- любые сведения о состоянии здоровья;
- рекомендации, характеристики;
- фотографии;
- копии отчетов, направляемые в органы статистики;
- другая информация.

3.2. Документы, содержащие персональные данные, являются конфиденциальными.

4. Получение, обработка и хранение персональных данных

4.1. Администрация получает сведения о персональных данных субъектов персональных данных из следующих источников:

– паспорта или иного документа, удостоверяющего личность;

– трудовой книжки;

– страхового свидетельства государственного пенсионного страхования;

– свидетельства о постановке на учет в налоговом органе, содержащего сведения об идентификационном номере налогоплательщика;

– документов воинского учета, содержащих сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу;

– документов об образовании, содержащих сведения о профессии, о квалификации или о наличии специальных знаний или специальной подготовки;

– анкет, заполняемых собственноручно при приеме на работу, или при подаче документов на участие в конкурсе на замещение вакантных должностей, предполагающих конкурсный отбор;

– иных документов и сведений, получаемых от субъекта или передаваемых от третьих лиц.

Субъект персональных данных обязан представлять администрации достоверные сведения о себе. Администрация Октябрьского района города Ставрополя имеет право проверять достоверность указанных сведений в порядке, не противоречащем законодательству Российской Федерации.

4.2. Обработка персональных данных субъекта персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении, продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы, обеспечения сохранности имущества.

4.3. При определении состава обрабатываемых персональных данных субъектов персональных данных Администрации Октябрьского района города Ставрополя руководствуется нормами действующего законодательства.

4.4. Как правило, персональные данные субъекта персональных данных Администрация Октябрьского района города Ставрополя получает непосредственно от субъекта персональных данных. Сотрудник, ответственный за документационное обеспечение кадровой и иной производственной деятельности, принимает от субъекта персональных данных материальные носители персональных данных (документы, копии документов), сверяет копии документов с подлинниками.

4.5. Если персональные данные субъекта персональных данных возможно получить исключительно у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (Приложение № 3). Администрация Октябрьского района города Ставрополя должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и

последствиях отказа субъекта представить письменное согласие на их получение (Приложение № 4). В случае, если субъект персональных данных уже дал письменное согласие на обработку своих персональных данных, дополнительное уведомление не требуется.

4.6. Условием обработки персональных данных субъекта персональных данных является его письменное согласие (Приложение № 5). Письменное согласие субъекта на обработку его персональных данных должно включать в себя:

– фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– наименование и адрес оператора персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Управлением способов обработки персональных данных;

– срок, в течение которого действует согласие, а также порядок его отзыва.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в соответствии с положением статьи 9 Федерального закона «О персональных данных».

4.7. Согласия субъекта на обработку его персональных данных не требуется в следующих случаях:

– обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

– обработка персональных данных осуществляется в целях исполнения трудового или иного договора или соглашения между работником и Администрацией;

– обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта, если получение его согласия при данных обстоятельствах невозможно;

– обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

– осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами.

4.8. Для обработки персональных данных, содержащихся в согласии в

письменной форме субъекта персональных данных на обработку его персональных данных, дополнительное согласие не требуется.

4.9. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных в письменной форме дает его законный представитель.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных при необходимости дает в письменной форме один из его наследников, если такое согласие не было дано субъектом персональных данных при его жизни.

4.10. В случае, если администрация на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

4.11. Администрация не имеет права осуществлять обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной, частной жизни, а также о членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, когда:

– субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

– персональные данные являются общедоступными;

– персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;

– обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

– обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

– обработка персональных данных необходима в связи с осуществлением правосудия;

– обработка персональных данных осуществляется в соответствии с

законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, работодатель вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

Обработка специальных категорий персональных данных должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась их обработка.

4.12. Защита персональных данных субъекта персональных данных от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральным законодательством Российской Федерации.

4.13. Субъекты персональных данных и их представители должны быть ознакомлены под роспись с документами Администрации Октябрьского района города Ставрополя, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

4.14. Основными источниками, содержащими персональные данные работников Администрации Октябрьского района города Ставрополя, являются их личные дела.

Личные дела хранятся уполномоченным лицом на бумажных носителях. Помимо этого персональные данные могут храниться в виде электронных документов, баз данных. Личное дело пополняется на протяжении всей трудовой деятельности работника в Администрации Октябрьского района города Ставрополя.

Письменные доказательства получения оператором согласия субъекта персональных данных на их обработку хранятся в личном деле.

4.15. При обработке персональных данных глава Администрации Октябрьского района города Ставрополя вправе определять способы обработки, документирования, хранения и защиты персональных данных на базе современных информационных технологий.

4.16. Перечень лиц, допущенных к обработке персональных данных, определяется приказом главы Администрации Октябрьского района города Ставрополя.

4.17. Обработка персональных данных, осуществляется уполномоченными работниками Администрации Октябрьского района города Ставрополя, определенными приказом главы Администрации Октябрьского района города Ставрополя, которые действуют на основании инструкций, предусматривающих выполнение комплекса мероприятий по обеспечению безопасности персональных данных.

4.18. Ответственность за контроль соблюдения требований по обработке персональных данных отделами, контроль соблюдения отделами прав и свобод субъектов персональных данных возлагается на руководителей отделов администрации.

4.19. Обеспечение техническими средствами обработки (ПЭВМ, серверами и т.д.) и их исправной работой организуется руководителем отдела автоматизации Администрации Октябрьского района города Ставрополя.

4.20. Помещения, в которых обрабатываются и хранятся персональные данные субъектов персональных данных, оборудуются надежными замками. Должно быть исключено бесконтрольное пребывание посторонних лиц в этих помещениях.

Для хранения персональных данных используются специально оборудованные шкафы или сейфы, которые запираются на ключ.

Помещения, в которых обрабатываются и хранятся персональные данные субъектов персональных данных, в рабочее время при отсутствии в них работников должны быть закрыты.

Проведение уборки помещений, в которых хранятся персональные данные, должно производиться в присутствии соответствующих работников.

5. Права и обязанности сторон в области защиты персональных данных

5.1. Субъект персональных данных обязан:

– передать Администрации Октябрьского района города Ставрополя или ее представителю комплекс достоверных, документированных персональных данных, состав которых установлен трудовым законодательством, иными нормативно-правовыми актами Российской Федерации, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и др.

– своевременно, в срок, не превышающий 5 рабочих дней, сообщать в общий отдел об изменении своих персональных данных.

5.2. Субъект персональных данных имеет право:

– на получение сведений о администрации, о месте его нахождения, о наличии у Администрации Октябрьского района города Ставрополя персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными, за исключением случаев, если предоставление персональных данных нарушает конституционные права и свободы других лиц;

– на свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральными законами;

– получать информацию, касающуюся обработки его персональных данных, в том числе содержащую:

а) подтверждение факта обработки персональных данных администрацией, а также цель такой обработки;

б) способы обработки персональных данных, применяемые оператором;

в) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

г) перечень обрабатываемых персональных данных и источник их получения;

д) сроки обработки персональных данных, в том числе сроки их хранения;

е) сведения о том, какие юридические последствия для него может повлечь за собой обработка его персональных данных.

– обжаловать в судебном порядке любые неправомерные действия или бездействие администрации при обработке и защите персональных данных.

– требовать об извещении Администрации Октябрьского района города Ставрополя всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта персональных данных, обо всех произведенных в них исключениях, исправлениях или дополнениях.

– требовать от Администрации Октябрьского района города Ставрополя исключения, исправления или уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации, Федерального закона «О персональных данных».

– при отказе оператора исключить или исправить персональные данные субъекта, заявить в письменной форме оператору (Администрации Октябрьского района города Ставрополя) о своем несогласии с соответствующим обоснованием такого несогласия, при отклонении оператором указанного обращения (несогласия), обжаловать действия оператора в порядке, предусмотренном законодательством Российской Федерации.

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю при личном обращении либо при получении запроса (Приложение № 7).

Сведения о персональных данных должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

5.3. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия субъекта персональных данных в письменной форме (Приложение № 5) или в случаях, предусмотренных Федеральными законами.

5.4. Администрация обязана разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого

решения, а также разъяснить порядок защиты своих прав и законных интересов (Приложение № 4).

5.5. Администрация обязана рассмотреть возражение субъекта персональных данных в течение семи рабочих дней со дня его получения и уведомить его о результатах рассмотрения такого возражения.

5.6. Если обязанность предоставления персональных данных субъектом персональных данных установлена федеральным законом (включая налоговое, трудовое право), Администрации Октябрьского района города Ставрополя обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

5.7. Если персональные данные были получены не от субъекта персональных данных (за исключением случаев, если персональные данные были предоставлены Администрации Октябрьского района города Ставрополя на основании федерального закона или если персональные данные являются общедоступными), Администрации Октябрьского района города Ставрополя до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию (Приложение № 8):

– наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

– цель обработки персональных данных и ее правовое основание;

– предполагаемые пользователи персональных данных;

– права субъекта персональных данных в области защиты персональных данных.

5.8. Администрация Октябрьского района города Ставрополя обязан безвозмездно предоставить субъекту персональных данных возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить соответствующего субъекта персональных данных и третьих лиц, которым персональные данные этого субъекта персональных данных были переданы (Приложение № 9).

Администрация Октябрьского района города Ставрополя обязана сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа в установленные нормативно-правовыми актами Российской Федерации сроки.

5.9. В случае выявления недостоверных персональных данных или неправомерных действий с ними Администрация Октябрьского района города Ставрополя обязана осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента

получения такой информации на период проверки. В случае подтверждения факта недостоверности персональных данных администрации на основании соответствующих документов обязан уточнить персональные данные и снять их блокирование.

5.10. В случае выявления неправомерных действий с персональными данными администрация в срок, не превышающий трех рабочих дней с даты такого выявления, обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Администрация Октябрьского района города Ставрополя в срок, не превышающий десяти рабочих дней с даты выявления неправомерности действий с персональными данными, обязана уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Администрация Октябрьского района города Ставрополя обязана уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, – также указанный орган (Приложение № 9).

5.11. В случае достижения цели обработки персональных данных Администрация обязана незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных (Приложение № 9).

5.12. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Администрация обязана прекратить обработку персональных данных и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий 90 дней с даты поступления указанного отзыва. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных (Приложение № 9).

5.13. До начала обработки персональных данных Администрация обязана уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев обработки персональных данных:

– относящихся к субъектам персональных данных, которых связывают с Администрацией трудовые отношения;

– полученных Администрацией Октябрьского района города Ставрополя в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются Администрацией Октябрьского района города Ставрополя исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

– относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующим общественным

объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

– являющихся общедоступными персональными данными;

– включающих в себя только фамилии, имена и отчества субъектов персональных данных;

– необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится Администрация Октябрьского района города Ставрополя, или в аналогичных целях;

– включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

– обрабатываемых без использования средств автоматизации в соответствии с федеральными законами и иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных.

5.14. Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации. Уведомление должно содержать следующие сведения:

– адрес Администрации;

– цель обработки персональных данных;

– категории субъектов, персональных данных которых обрабатываются;

– правовое основание обработки персональных данных;

– перечень действий с персональными данными, общее описание используемых Администрацией способов обработки персональных данных;

– описание мер, которые Администрация Октябрьского района города Ставрополя обязуется осуществлять при обработке персональных данных по обеспечению безопасности персональных данных при их обработке;

– дата начала обработки персональных данных;

– срок и условия прекращения обработки персональных данных.

6. Доступ к персональным данным субъекта персональных данных и их передача

6.1. Внутренний доступ (доступ внутри Администрации Октябрьского района города Ставрополя) к персональным данным субъектов персональных данных имеют сотрудники отделов Администрации Октябрьского района

города Ставрополя, которым эти данные необходимы для выполнения должностных обязанностей.

Право доступа к персональным данным субъекта персональных данных имеют:

– глава Администрации Октябрьского района города Ставрополя;

– заместители главы Администрации Октябрьского района города Ставрополя;

– руководитель и сотрудники отделов правового и кадрового обеспечения;

– руководители отделов по направлению деятельности субъекта персональных данных (исключительно работников данного отдела; за исключением сведений имущественного характера);

– руководитель нового отдела при переводе работника из одного отдела в другое (за исключением сведений имущественного характера);

– непосредственно субъект персональных данных;

– другие сотрудники Администрации Октябрьского района города Ставрополя с письменного согласия самого субъекта персональных данных.

После прекращения юридических отношений с субъектом персональных данных (увольнения работника и т.п.) документы, содержащие его персональные данные, хранятся в Администрации Октябрьского района города Ставрополя в течение сроков, установленных архивным и иным законодательством Российской Федерации.

6.2. Внешний доступ к персональным данным субъектов персональных данных имеют массовые потребители персональных данных и контрольно-надзорные органы.

6.2.1. К числу массовых потребителей персональных данных вне Администрации относятся следующие государственные и негосударственные структуры:

– налоговые органы;

– правоохранительные органы;

– органы лицензирования и сертификации;

– органы прокуратуры и ФСБ;

– органы статистики;

– страховые агентства;

– военные комиссариаты;

– органы социального страхования;

– пенсионные фонды;

– подразделения государственных и муниципальных органов управления.

6.2.2. Надзорно-контрольные органы имеют доступ к информации исключительно в сфере своей компетенции.

6.3. Внешний доступ со стороны третьих лиц к персональным данным субъекта персональных данных осуществляется с его письменного согласия, за исключением случаев, когда такой доступ необходим в целях предупреждения

угрозы жизни и здоровью субъекта персональных данных или других лиц, и иных случаев, установленных законодательством Российской Федерации.

6.4. Администрация Октябрьского района города Ставрополя обязана сообщать персональные данные субъекта персональных данных по надлежащим оформленным запросам суда, прокуратуры иных правоохранительных органов.

6.5. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только на основании письменного запроса на бланке организации, с приложением копии заявления работника.

6.6. Персональные данные субъекта персональных данных могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта персональных данных.

6.7. При передаче персональных данных Администрация Октябрьского района города Ставрополя должна соблюдать следующие требования:

– не сообщать персональные данные субъекта персональных данных третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных федеральными законами;

– не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;

– предупреждать лиц, получающих персональные данные субъекта персональных данных, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено, за исключением случаев, когда обмен персональными данными осуществляется в порядке, установленном федеральными законами;

– не запрашивать информацию о состоянии здоровья субъекта персональных данных, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

– передавать персональные данные субъекта персональных данных представителям работников и иных категорий субъектов персональных данных в порядке, установленном Трудовым кодексом Российской Федерации и Федеральным законом от 27 июля 2006 г. № 152-ФЗ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций;

– разрешать доступ к персональным данным, исключительно специально уполномоченным лицам (при этом указанные лица должны иметь право получать лишь те персональные данные, которые необходимы для выполнения конкретных функций);

– уполномоченные лица должны подписать обязательство о неразглашении персональных данных (Приложение № 2).

6.8. Передача персональных данных от держателя или его представителей в другие предприятия, учреждения и организации может допускаться в

минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.9. Ответы на правомерные письменные запросы других предприятий, учреждений и организаций даются с разрешения главы Администрации Октябрьского района города Ставрополя в письменной форме, в том объеме, который позволяет не разглашать излишний объем персональных данных.

6.10. Не допускается передача персональных данных по открытым каналам связи, в том числе по телефону.

6.11. В сопроводительном письме к сведениям, передаваемым в письменной форме, указывается, что в прилагаемых документах содержатся персональные данные субъектов персональных данных Администрации.

6.12. Осуществление трансграничной передачи осуществляется в соответствии со статьей 12 Федерального Закона «О персональных данных».

6.12.1. До начала осуществления трансграничной передачи персональных данных Администрация обязана убедиться, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъекта персональных данных.

6.12.2. Трансграничная передача персональных данных на территории иностранных государств, обеспечивающих адекватную защиту персональных данных, осуществляется в соответствии с Федеральным законом «О персональных данных» и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

6.12.3. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты персональных данных субъектов персональных данных, может осуществляться в случаях:

– наличия согласия субъекта персональных данных в письменной форме;

– предусмотренных международными договорами Российской Федерации об оказании правовой помощи по гражданским, семейным и уголовным делам;

– предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства;

– исполнения договора, стороной которого является субъект персональных данных;

– защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме.

7. Защита персональных данных

7.1. Комплекс мер по защите персональных данных направлен на

предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе управленческой и производственной деятельности Администрации.

7.2. Администрация при обработке персональных данных обязана принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий в соответствии с требованиями к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, установленными Правительством Российской Федерации.

7.3. Мероприятия по защите персональных данных определяются Положением по организации и проведению работ по обработке и защите персональных данных в информационных системах персональных данных, приказах, инструкциях и других внутренних документах Администрации.

7.4. Для защиты персональных данных в Администрации применяются следующие принципы и правила:

– ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные;

– строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

– рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;

– знание сотрудниками требований нормативно-методических документов по защите персональных данных;

– распределение персональной ответственности между сотрудниками, участвующими в обработке персональных данных, за выполнение требований по обеспечению безопасности персональных данных.

– оборудование помещений и установление режима конфиденциальности в соответствии с требованиями по обеспечению безопасности персональных данных при работе с конфиденциальными документами и базами данных;

– определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится соответствующая вычислительная техника;

– организация порядка уничтожения информации;

– своевременное выявление нарушений требований разрешительной системы доступа сотрудниками Администрации Октябрьского района города Ставрополя;

– воспитательная и разъяснительная работа с сотрудниками отделов по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

– регулярное обучение работников по вопросам, связанным с обеспечением безопасности персональных данных.

– ограничение доступа к техническим средствам и системам обработки информации, на которых содержатся персональные данные.

– создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией;

– резервирование защищаемых данных (создание резервных копий).

8. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

8.1. Персональная ответственность является одним из главных требований к организации функционирования системы защиты персональных данных и обязательным условием обеспечения эффективности функционирования данной системы.

8.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут предусмотренную законодательством Российской Федерации ответственность за нарушение режима защиты, обработки и порядка использования этой информации.

8.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта персональных данных, несут предусмотренную законодательством Российской Федерации ответственность.

8.4. Каждый сотрудник Администрации Октябрьского района города Ставрополя, получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность полученной информации.

8.5. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

Приложение № 1

ЛИСТ ОЗНАКОМЛЕНИЯ

с «Положением о персональных данных Администрации Октябрьского района города Ставрополя»

№ п/п	Фамилия, инициалы сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении

Приложение № 2

ОБЯЗАТЕЛЬСТВО

о неразглашении конфиденциальной информации(персональных данных),
не содержащей сведений, составляющих государственную тайну

Я, _____, исполняющий(ая)
Ф.И.О. сотрудника (государственного гражданского служащего, работника)
должностные обязанности по замещаемой должности _____
(должность, наименование структурного подразделения)
_____
Администрации Октябрьского района города Ставрополя предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к конфиденциальной информации (персональным данным[1]), не содержащей сведений, составляющих государственную тайну (далее - конфиденциальные сведения).

Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать[2] (не передавать и не раскрывать) третьим лицам[3] конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. Не использовать конфиденциальные сведения иначе как в интересах управления.
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному руководителю, а также лицу, ответственному в администрации за организацию защиты информации.
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых и локальных актов, регламентирующих вопросы защиты конфиденциальных сведений.
6. В случае прекращения работы в Администрации Октябрьского района города Ставрополя, сразу же возвратить все документы и другие материалы, полученные в ходе выполнения своих служебных обязанностей, содержание которых отнесено к конфиденциальным сведениям
7. В течение 3 лет после прекращения права на допуск к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к предусмотренной законодательством Российской Федерации ответственности.

_____ _____
(подпись) (Ф.И.О.)

"__" _____ 200_ г.

---

[1] 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 (пункт 1 статьи 3 Федерального закона «О персональных данных»)

[2] Под разглашением понимается умышленное или неумышленное (неосторожное) действие лица, приведшие к ознакомлению (оглашению) с конфиденциальными сведениями лиц, не имеющих в установленном порядке допуска к конфиденциальным сведениям.

[3] Третьи лица - лица, не имеющие в установленном порядке допуска к конфиденциальным сведениям

Приложение № 3

Согласие
субъекта персональных данных
на получение его персональных данных у третьих лиц

Я, _____
(должность,

_____,
фамилия, имя, отчество)

согласен на получение оператором (администрацией Октябрьского района города Ставрополя) от

_____
(Ф.И.О. или наименование третьего лица)

следующей информации _____

_____
(виды запрашиваемой информации и (или) документов)

_____ _____ _____
дата подпись расшифровка подписи

Приложение № 4

Уведомление

Уважаемый _____
(Ф.И.О.)

В связи с _____
(указать причину)

у администрации Октябрьского района города Ставрополя возникла необходимость получения следующей информации, составляющей Ваши персональные данные _____

_____
(перечислить информацию)

Просим Вас предоставить указанные сведения _____

_____
(кому)

в течение трех рабочих дней с момента получения настоящего уведомления.

В случае невозможности предоставить указанные сведения просим в указанный срок дать письменное согласие на получение оператором (администрацией Октябрьского района города Ставрополя) необходимой информации из следующих источников:

_____,
(указать источники)

следующими способами: _____
(автоматизированная обработка, иные способы)

По результатам обработки указанной информации оператором планируется принятие следующих решений, которые будут доведены до Вашего сведения _____

_____

_____
(указать решения и иные юридические последствия обработки информации)

Против принятого решения Вы имеете право заявить свои письменные возражения в _____ срок.

Информируем Вас о последствиях Вашего отказа дать письменное согласие на получение оператором указанной информации

_____
(перечислить последствия)

Информируем Вас о Вашем праве в любое время отозвать свое письменное согласие на обработку персональных данных.

_____ _____ _____
дата подпись расшифровка подписи

Настоящее уведомление на руки получил:

_____ _____ _____
дата подпись расшифровка подписи

Приложение № 5

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Ставрополь _____
дата

1. Субъект персональных данных (Далее – «Работник»)
Фамилия, имя, отчество _____
Адрес _____
Паспорт № _____
Выдан: орган/дата _____
Код подразделения _____

2. Оператор: «администрация Октябрьского района города Ставрополя»
Адрес: Россия, 355006, г. Ставрополь ул. Голенева, 21

3. Цели обработки Персональных данных: Кадровый учет.

4. Работник настоящим дает согласие своей волей и в своем интересе на обработку перечисленных ниже Персональных данных

4.1. Фамилия, имя, отчество, год, месяц, дата и место рождения, пол, возраст, адрес, гражданство, сведения об образовании, контактная информация (домашний(е) адрес(а), номера домашнего и мобильного телефонов, адрес электронной почты, профессия и др.), фотографии;

4.2. Сведения, содержащиеся в документах, удостоверяющих личность, в том числе паспортные данные, ИНН и номер страхового свидетельства государственного пенсионного страхования, фотокопии паспортов, виз, разрешений на работу, водительских удостоверений, служебных удостоверений, других личных документов;

4.3. Сведения о трудовой деятельности, включая занимаемые должности и должностные полномочия и обязанности, информация о работодателях;

4.4. Сведения о семейном положении Работника;

4.5. Любые иные данные, которые могут потребоваться Оператору в связи с осуществлением целей, указанных в п. 3 согласия (Далее – **«Персональные данные»**).

5. Работник настоящим дает согласие на совершение с Персональными данными перечисленных ниже действий:

5.1. Обработку Персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, **блокирование, уничтожение персональных данных.**

5.2. Общее описание используемых Оператором способов обработки персональных данных

5.2.1. При обработке Персональных данных Оператор принимает 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.

5.2.2. Обработка Персональных данных Оператором осуществляется в соответствии с Положением о персональных данных управления труда и социальной поддержки населения по осуществлению отдельных государственных полномочий в городе Ставрополе.

5.2.3. Работник уведомлен о том, что он (она) в любой момент времени, письменно обратившись к Оператору, вправе запросить перечень имен и адресов любых получателей Персональных данных, ознакомиться с Персональными данными, обратиться с просьбой о предоставлении дополнительной информации в отношении хранения и обработки Персональных данных или же потребовать внесения любых необходимых изменений в Персональные данные для их уточнения.

6. Срок, порядок отзыва. Настоящее согласие действует до ликвидации Администрации. Работник может отозвать настоящее согласие путем направления Оператору письменного уведомления не менее чем за 90 (девяносто) дней до предполагаемой даты отзыва настоящего согласия. Работник соглашается на то, что в течение указанного срока Оператор не обязан прекращать обработку персональных данных и уничтожать персональные данные Работника. Отзыв не будет иметь обратной силы в отношении Персональных данных, прошедших обработку до вступления в силу такого отзыва.

В подтверждение вышеизложенного, нижеподписавшийся Работник подтверждает свое согласие на обработку своих Персональных данных в соответствии с тем, как это описано выше.

Подпись: _____ _____
(Подпись) Дата

Приложение № 6

Согласие
субъекта персональных данных на включение информации
о его персональных данных в

_____
(справочник, каталог и др. общедоступные источники)

Я, _____
(должность,

_____,
фамилия, имя, отчество)

согласен на включение оператором (Администрацией Октябрьского района города Ставрополя) в корпоративный справочник _____ (иные источники) следующей информации, содержащей мои персональные данные: фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии

_____
_____
_____
_____ иные персональные данные.

_____ _____ _____
дата подпись расшифровка подписи

Приложение № 7

Запрос
о доступе субъекта персональных данных к своим персональным данным

_____
(наименование и адрес оператора)

От _____.
(фамилия, имя, отчество,

_____

номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе)

Прошу предоставить мне для ознакомления следующую информацию (документы), составляющие мои персональные данные: _____
_____.
(перечислить)

_____ _____ _____
дата подпись расшифровка подписи

Приложение № 8

Уведомление

Уважаемый _____
(фамилия, имя, отчество)

на основании _____ Администрация Октябрьского района города Ставрополя (оператор) получило от _____
(наименование организации, адрес)

следующую информацию, содержащую Ваши персональные данные: _____
_____
(перечислить)

Указанная информация будет обработана и использована оператором в целях:_____
_____

Вы имеете право на полную информацию о своих персональных данных, содержащуюся у оператора, свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей Ваши персональные данные, за исключением случаев, предусмотренных действующим законодательством; требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав, получать иную информацию, касающуюся обработки Ваших персональных данных.

_____ _____ _____
дата подпись расшифровка подписи

Настоящее уведомление на руки получил:

_____ _____ _____
дата подпись расшифровка подписи

Приложение № 9

Уведомление об уничтожении,
(изменении, прекращении обработки, устранении нарушений персональных данных)

Уважаемый _____.
(фамилия, имя, отчество)

В связи с _____
_____
(недостоверностью, выявлением неправомерных действий с Вашими персональными данными, достижением цели обработки, отзывом Вами согласия на обработку, другие причины)

сообщаем Вам, что обработка Ваших персональных данных о _____
_____
(перечислить)

прекращена и указанная информация подлежит уничтожению (изменению).

_____ _____ _____
дата подпись расшифровка подписи

Настоящее уведомление на руки получил:

_____ _____ _____
дата подпись расшифровка подписи

Приложение № 3
к приказу главы администрации
Октябрьского района города Ставрополя

от «11» 08 2017 г. № 171

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых администрации Октябрьского района города Ставрополя

г. Ставрополь
2017 г.

ВВЕДЕНИЕ

Настоящий Перечень персональных данных (далее – Перечень), обрабатываемых в администрации Октябрьского района города Ставрополя (далее - Администрация), разработан в соответствии законодательством Российской Федерации, а также со спецификой деятельности Администрации.

Перечень содержит список категорий данных, безопасность которых должна обеспечиваться системой защиты персональных данных (СЗПДн) Администрации.

1. Общие положения

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты.

Объекты защиты каждой ИСПДн включают:

1) Обрабатываемая информация:
- персональные данные субъектов ПДн;
- персональные данные сотрудников;

2) Технологическая информация.

3) Программно-технические средства обработки.

4) Средства защиты ПДн.

5) Каналы информационного обмена и телекоммуникации.

6) Объекты и помещения, в которых размещены компоненты ИСПДн.

1. 1. Обрабатываемая в Администрации информация

1.1.1. Перечень персональных данных субъектов Пдн

Персональные данные субъектов ПДн включают:
- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Контактный телефон;
- Адрес регистрации;
- Адрес места фактического проживания (пребывания);
- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Телефонный номер (домашний, рабочий, мобильный);
- Семейное положение и состав семьи (муж/жена, дети);
- Данные о состоянии здоровья.

1.1.2. Перечень персональных данных сотрудников Администрации

Персональные данные сотрудников Администрации включают:
- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Адрес регистрации;
- Адрес места фактического проживания (пребывания);
- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- Информация о трудовой деятельности до приема на работу;
- Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
- Телефонный номер (домашний, рабочий, мобильный);
- Семейное положение и состав семьи (муж/жена, дети);
- Информация о знании иностранных языков;
- Форма допуска;

- Оклад;
- Данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- ИНН;
- Данные об аттестации работников;
- Данные о повышении квалификации;
- Данные о наградах, медалях, поощрениях, почетных званиях;
- Информация о приеме на работу, перемещении по должности, увольнении;
- Информация об отпусках;
- Информация о командировках;
- Информация о болезнях;
- Информация о негосударственном пенсионном обеспечении.

2. Технологическая информация

Технологическая информация, подлежащая защите, включает:
- управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

3. Программно-технические средства обработки

Программно-технические средства включают в себя:
- общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);
- резервные копии общесистемного программного обеспечения;

- инструментальные средства и утилиты систем управления ресурсами ИСПДн;
- аппаратные средства обработки ПДн (АРМ и сервера);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

4. Средства защиты ПДн

Средства защиты ПДн состоят из аппаратно-программных средств, включают в себя:

- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства антивирусной защиты;
- средства межсетевого экранирования;
- средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

5. Каналы информационного обмена и телекоммуникации

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

6. Объекты и помещения, в которых размещены компоненты ИСПДн

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

ПРИЛОЖЕНИЕ

УТВЕРЖДЕНО
приказом
от _____ № _____

ПОЛОЖЕНИЕ
о порядке обеспечения безопасности персональных данных с использованием средств криптографической защиты информации

1 Общие положения

1.1 Положение о порядке обеспечения безопасности персональных данных с использованием средств криптографической защиты информации (далее - Положение) разработано в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152 «О персональных данных», определяет порядок организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для защиты персональных данных при их обработке в информационной системе администрации Октябрьского района города Ставрополя (далее - Администрация).

1.2 В документе используются положения следующих нормативных актов:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

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

– Приказ ФСБ от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– приказ ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

– «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», утвержденная приказом ФАПСИ от 13.06.2001 № 152;

– «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015).

1.3 Требования Положения обязательны к исполнению всеми уполномоченными на работу со средствами криптографической защиты информации работниками администрации Октябрьского района города Ставрополя (далее – Пользователи криптосредств).

1.4 Используемые термины, определения и сокращения.

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

– Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

– Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну.

– Криптографический ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

– Ключевые документы – материальные носители информации, содержащие криптографические ключи.

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

– Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

– Режимные помещения – помещения, где установлены криптосредства или хранятся ключевые документы к ним.

– СКЗИ – средство криптографической защиты информации.

– ПЭВМ – персональная электронная вычислительная машина.

1.5 Настоящее Положение вступает в силу с момента его утверждения руководителем администрации и действует бессрочно до замены его новым Положением.

1.6 Пересмотр Положения производится в следующих случаях:

– при изменении процессов и технологий обработки персональных данных в администрации;

– по результатам проверок органа по защите прав субъектов персональных данных, выявившим несоответствия требованиям законодательства РФ по обеспечению безопасности персональных данных;

– при изменении требований законодательства РФ к порядку обработки и обеспечению безопасности персональных данных;

– в случае выявления существенных нарушений по результатам внутренних проверок системы защиты персональных данных.

1.7 Ответственным за пересмотр данного Положения является сотрудник администрации, назначенный Приказом главы администрации ответственным за организацию обработки персональных данных в администрации. Измененное Положение утверждается Приказом Главы администрации.

2 Организация и обеспечение безопасности обработки персональных данных с использованием криптосредств

2.1 Пользователи криптосредств допускаются к работе с ними на основании приказа главы администрации.

2.2 Обеспечение функционирования и безопасности криптосредств возлагается на ответственного пользователя криптосредств, имеющего необходимый уровень квалификации, назначаемого приказом главы администрации (далее – Ответственный пользователь криптосредств).

2.3 Допускается возложение функций Ответственного пользователя криптосредств на:

– одного из пользователей криптосредств;

– на структурное подразделение или должностное лицо (работника), ответственных за защиту информации, назначаемых аднистрацией.

2.4 Пользователи криптосредств обязаны:

– соблюдать конфиденциальность при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним;

– выполнять требования по обеспечению безопасности персональных данных;

– обеспечивать надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

– своевременно выявлять попытки посторонних лиц получить сведения о защищаемых персональных данных, об используемых криптосредствах или ключевых документах к ним;

– немедленно принимать меры по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.;

– строго соблюдать правила пользования криптосредств, к эксплуатации которых допущен;

– не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

– не допускать записи на ключевой носитель посторонней информации;

2.5 Пользователи криптосредств, должны быть ознакомлены с настоящим Положением и другими документами, регламентирующими организацию и обеспечение безопасности персональных данных при их обработке в информационных системах, под расписку и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

2.6 На Ответственного пользователя криптосредств возлагаются обязанности по:

– текущему контролю за организацией и обеспечением функционирования криптосредств;

– проведению разбора конфликтных ситуаций, возникающих при эксплуатации криптосредств;

– ведению учета экземпляров криптосредств, эксплуатационной и технической документации к ним, ключевых документов.

3 Порядок обращения с криптосредствами и криптоключами к ним. Мероприятия при компрометации криптоключей

3.1 При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи криптоключей не допускается.

3.2 Криптосредства, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

3.3 Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов». (Форма журнала представлена в Приложении 1).

3.4 Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3.5 Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в Журнале поэкземплярного учета

пользователям криптосредств, несущим персональную ответственность за их сохранность.

3.6 Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) Ответственным пользователем криптосредств под расписку в соответствующем Журнале поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована Ответственным пользователем криптосредств.

3.7 Пользователи криптосредств должны хранить инсталлирующие криптосредства, носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.8 Пользователи криптосредств также обязаны раздельно хранить действующие и резервные ключевые документы, предназначенные для применения в случае компрометации действующих ключевых документов.

3.9 Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, должны быть опечатаны. Место опечатывания (опломбирования) должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

3.10 При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от Ответственного пользователя криптосредств.

3.11 Получение криптосредств, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено Ответственному пользователю криптосредств в соответствии с порядком, указанным в сопроводительном письме. Ответственный пользователь криптосредств обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

3.12 Указание на изготовление очередных ключевых документов для своевременной замены действующих ключевых документов следует производить заблаговременно. Указание о вводе в действие очередных ключевых документов может быть дано ответственным пользователем криптосредств только после поступления от всех заинтересованных пользователей криптосредств подтверждения о получении ими очередных ключевых документов.

3.13 Неиспользованные или выведенные из действия ключевые документы подлежат возвращению Ответственному пользователю криптосредств или по его указанию должны быть уничтожены на месте.

3.14 Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

3.15 Криптоключи (исходную ключевую информацию) необходимо уничтожать (стирать) по технологии регламентированной эксплуатационной и технической документацией к криптосредствам.

3.16 Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к криптосредствам.

3.17 Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожают путем сжигания или с помощью любых бумагорезательных машин.

3.18 Намеченные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к криптосредствам процедура удаления программного обеспечения криптосредств.

3.19 Ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующем Журнале поэкземплярного учета. Хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

3.20 Ключевые документы уничтожаются либо пользователями криптосредств, либо Ответственным пользователем криптосредств под расписку в соответствующем Журнале поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) Ответственного пользователя криптосредств для списания уничтоженных документов с их Лицевых счетов.

3.21 Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. В акте указывается что уничтожается и в каком количестве. В

конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих криптосредства носителей, эксплуатационной и технической документации (Приложение 2). Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующем Журнале поэкземплярного учета.

3.22 Криптоключи, в отношении которых, возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного пользователя криптосредств, согласованного с оператором, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

3.23 О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием персональных данных, пользователи криптосредств обязаны сообщать Ответственному пользователю криптосредств.

3.24 Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

3.25 В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

3.26 Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет Ответственный пользователь криптосредств.

3.27 Изготавливают ключевые документы пользователи криптосредств, применяя штатные криптосредства, в строгом соответствии с эксплуатационной и технической документацией к криптосредствам.

4 Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

4.1 Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее – режимные помещения), должны обеспечивать сохранность персональных данных, криптосредств и ключевых документов к ним.

4.2 При оборудовании режимных помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

4.3 Перечисленные в настоящем документе требования к режимным помещениям могут не предъявляться, если это предусмотрено правилами пользования криптосредствами, согласованными с ФСБ России.

4.4 Режимные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, должны быть оборудованы металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

4.5 Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

4.6 Двери режимных помещений должны быть закрыты на ключ в нерабочее время и могут открываться только для санкционированного прохода сотрудников. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в режимные помещения, под расписку в «Журнале учета хранилищ СКЗИ и ключей к ним» (Приложение 3). Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе пользователя криптосредств.

4.7 Блоки ПЭВМ с установленными СКЗИ должны быть опечатаны (опломбированы) с внесением информации в Журнал опломбирования ПЭВМ (Приложение 4), кроме того, в техническом (аппаратном) журнале отражаются также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на СКЗИ не заводится если нет прямых указаний о его ведении Форма технического (аппаратного) журнала приведена в Приложении 5.

4.8 Для предотвращения просмотра извне режимных помещений их окна должны быть защищены (занавешены плотными шторами или жалюзи).

4.9 Режимные помещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному пользователю криптосредств совместно с представителем службы охраны или дежурным по организации. Результаты проверки исправности фиксируются в Журнале учета проверок сигнализации (Приложение 6).

4.10 Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и приспособлениями для опечатывания. Хранение эксплуатационной и технической документации, инсталлирующих криптосредства носителей осуществляет Ответственный пользователь криптосредств.

4.11 Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе Ответственного пользователя криптосредств.

4.12 По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты на ключ. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале Ответственному пользователю криптосредств, который хранит эти ключи в личном или специально выделенном хранилище.

4.13 Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.

4.14 При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает Ответственный пользователь криптосредств.

4.15 В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища, могут быть вскрыты только пользователями криптосредств, Ответственным пользователем криптосредств или Администратором ИБ ИС.

4.16 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено Ответственному пользователю криптосредств. Прибывший Ответственный пользователь криптосредств должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

4.17 Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

4.18 На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с Ответственным пользователем криптосредств необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

5. Организация доступа в режимные помещения, в которых размещены используемые СКЗИ, в том числе носители ключевой, аутентифицирующей и парольной информации СКЗИ

5.1. Для режимных помещениях, в которых размещены используемые СКЗИ, в том числе носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения) организуется режим обеспечения безопасности, при котором обеспечивается сохранность СКЗИ, ключевой информации и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

5.2. В Помещения допускаются работники администрации, указанные в Перечне лиц, имеющих право доступа в Помещения, в которых размещены СКЗИ (далее – Перечень).

5.3. Помимо лиц, указанных в Перечне (далее – лица, имеющие право доступа в Помещение) право самостоятельного пребывания в Помещениях, для которых введен режим безопасности, имеют непосредственно ответственные за организацию обработки персональных данных, ответственный за защиту информации и обеспечение безопасности персональных данных, администратор информационной безопасности информационных систем, администраторы информационных систем, ответственный пользователь СКЗИ.

5.4. Сотрудники, не внесенные в Перечень (далее – лица, не имеющие право доступа в Помещение), являются посторонними лицами и могут находиться в Помещениях только в присутствии лиц, имеющих права доступа в Помещения.

5.5. Сторонние лица, не являющиеся работниками администрации, имеют право пребывать в Помещении только в присутствии лиц, имеющих право доступа в Помещение, и в течение ограниченного количества времени, необходимого для решения вопросов, связанных с исполнением функций и (или) осуществлением полномочий по предоставлению государственных и муниципальных услуг.

5.6. Доступ в Помещения разрешается только в рабочее время, в нерабочее время режимное помещение должно закрываться.

5.7. В течение рабочего времени лица, имеющие право доступа в Помещение:

при оставлении Помещения закрывают дверь Помещения на ключ (при этом запрещается оставлять ключ в замке Помещения);

– не покидают Помещение, если в нем находятся лица, не имеющие право доступа в Помещение;

– при обнаружении фактов нарушения режима безопасности Помещения ставят в известность ответственного пользователя СКЗИ и Администратора информационной безопасности ИС;

– при посещении Помещения сторонними лицами с целью проведения контрольных, проверочных мероприятий, а также работ по обслуживанию Помещения и его инженерно-технических средств ставят в известность об этом ответственного пользователя СКЗИ, администратора информационной безопасности ИС и руководителя подразделения.

5.8. Доступ в Помещение при возникновении нештатной ситуации в нерабочее время осуществляется в присутствии администратора информационной безопасности

5.9. При обслуживании Помещения (уборка или различный ремонт Помещения, инженерно-технического оборудования):

– обслуживающий персонал находится в Помещении только в присутствии лиц, имеющих право доступа в Помещение.

– ключи от замков дверей Помещения обслуживающему персоналу и другим лицам, не имеющим права доступа в Помещение, без согласования с Ответственным за организацию обработки персональных данных, не выдаются.

– сотрудники подразделения, обеспечивающие контроль действий обслуживающего персонала в Помещении, обязаны не допускать несанкционированных действий в отношении компонентов информационной системы и материальных носителей информации ограниченного доступа.

– капитальный или иной ремонт может проводиться и в отсутствие лиц, имеющих право доступа в Помещение, при условии того, что компоненты информационной системы и материальные носители информации ограниченного доступа будут вынесены из ремонтируемого Помещения в другое контролируемое помещение, и по окончании ремонта будут сменены замки. Организует и контролирует исполнение Ответственный за организацию обработки персональных данных.

5.10. Лица, имеющие право доступа в Помещение, несут ответственность за нерегламентированное пребывание в Помещении работников, не имеющих права доступа в Помещение, и сторонних лиц.

6. Допуск в помещения, в которых ведётся эксплуатация СКЗИ

6.1. Доступ посторонних лиц в помещения, в которых ведётся эксплуатация СКЗИ, должен осуществляется только ввиду служебной необходимости. При этом на момент присутствия посторонних лиц в помещении должны быть приняты меры по недопущению ознакомления посторонних лиц с информацией ограниченного доступа.

6.2. Допуск сотрудников в помещения, в которых ведётся эксплуатация СКЗИ, оформляется после подписания сотрудником обязательства о неразглашении и проведении инструктажа ответственным пользователем СКЗИ, либо администратора информационной безопасности.

6.3. В нерабочее время помещения, в которых осуществляется функционирования СКЗИ, должны опечатываться или ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, ключевые документы, должны быть убраны в запираемые шкафы (сейфы), средства вычислительной техники выключены либо заблокированы.

7. Допуск в серверные помещения с СКЗИ

7.1. Доступ в серверные помещения разрешён только списку сотрудников, имеющих допуск в соответствии с приказом главы администрации. Уборка серверных помещений происходит только при строгом контроле указанных лиц.

7.2. Серверное помещение в обязательном порядке оснащается опечатывающим устройством, либо охранной сигнализацией.

7.3. Доступ в серверные помещения посторонних лиц допускается строго по согласованию с вышеперечисленными лицами.

7.4. Нахождение в серверных помещениях посторонних лиц без сопровождающего не допустимо.

ПРИЛОЖЕНИЕ 1 К ПОЛОЖЕНИЮ

ЖУРНАЛ ПОЭКЗЕМПЛЯРНОГО УЧЕТА КРИПТОСРЕДСТВ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ

№ п/п	Наименование	Регистрационные номера	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Выдано		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				от кого получены	дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	подпись пользователя СКЗИ и дата	Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	дата подключения (установки) и подписи лиц, произведших подключение (установку)	номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие	Номер акта или расписка об уничтожении	
1	КриптоПро 3.9	3939Z-Q0000-01EZP-G7K0L-9LAG6		УЦ Федерального казначейства	22.01.2015	Кваша Т.Л.		Приходько Д. В.	22.01.2015					
2	КриптоПро 3.6	3636B-50000-01MP4-V4Q0L-WBHY0			04.07.2012	Вишнякова Н.Ю.		Приходько Д. В.	04.07.2012					

3	КриптоПро CSP	3636G-13010-0167L-G7UTE-EAG38			19.04.2011	Лихманова М.И.		Приходько Д. В.	19.04.2011		
4	КриптоПро 3.9	3939Y-30000-01TEA-TMV75-NG6BY			22.01.2015	Морозова Г.П.		Приходько Д. В.	22.01.2015		
5	КриптоПро 4.0	4040E-E0000-01EEY-2663B-P7BLP			21.03.2017	Лукьянцев а И.В.		Приходько Д. В.	21.03.2017		
6	КриптоПро 4.0	40407-90000-0181Q-R647X-ZH22W			21.03.2017	Федотова М.С.		Приходько Д. В.	21.03.2017		
7	КриптоПро 4.0	4040U-20000-01Q61-95RV2-UDMPD			21.03.2017	Аспатян К.О.		Приходько Д. В.	21.03.2017		
8	КриптоПро 4.0	4040L-70000-01V3W-8H4XU-HWFF3			21.03.2017	Давыдова Е.К.		Приходько Д. В.	21.03.2017		
9	КриптоПро JCP	CF104-18000-04RQT-TDNZY-UDQKW			05.07.2013	Морозова Г.П		Приходько Д. В.	05.07.2013		

10	КриптоПро JCP	CF10A-B8000-0476M-WBT1A-G9GAD		УЦ Федерально го казначейств а	№2133/395 23.04.2018	07.05.2013	Давыдова Е.К.	Вишнякова Н.Ю.		Приходько Д. В.	07.05.2013
11	Континент АП 3.7	351E2-009995/2133/223									№2133/395 23.04.2018

ПРИЛОЖЕНИЕ 2 К ПОЛОЖЕНИЮ

Акт уничтожения ключевых документов

Комиссия, в составе:

председатель комиссии:

_____

члены комиссии:

_____

_____

провела уничтожение

_____

_____

_____

цифрами и прописью о количестве наименований и экземпляров уничтожаемых ключевых документов,

инсталлирующих криптосредства носителей, эксплуатационной и технической документации

путем

_____

разрезания, демонтажа, измельчения, сдачи для уничтожения предприятию по утилизации вторичного сырья

_____

Председатель комиссии:

_____ _____

(ФИО) (дата, подпись)

Члены комиссии:

_____ _____

(ФИО) (дата, подпись)

_____ _____

(ФИО) (дата, подпись)

Приложение № 5
Приложение к приказу главы Администрации Октябрьского района города Ставрополя

от «11» 08 2017 г. № 171

П О Р Я Д О К

ПАРОЛЬНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ ОКТЯБРЬСКОГО РАЙОНА ГОРОДА СТАВРОПОЛЯ

г. Ставрополь
2017 г.

СПИСОК СОКРАЩЕНИЙ

РМ	Автоматизированное рабочее место
СПДн	Информационная система персональных данных
ВС	Локально-вычислительная сеть
Дн	Персональные данные
ЭВМ	Персональная электронная вычислительная машина
ВТ	Средства вычислительной техники
ИО	Фамилия имя отчество

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Порядок парольной защиты (далее – Порядок) включает в себя взаимоувязанный комплекс организационно-технических мер, регламентирующих генерацию и/или выбор, использование, хранение, уничтожение парольной информации в информационных системах персональных данных администрации Октябрьского района города Ставрополя.

1.2. Требования настоящего Порядка являются неотъемлемой частью комплекса мер безопасности и защиты информации в администрации Октябрьского района города Ставрополя.

1.3. Требования настоящего Порядка распространяются на всех должностных лиц и сотрудников подразделений администрации Октябрьского района города Ставрополя, использующих в работе ИСПДн, а также всех видов программного обеспечения (ПО), эксплуатируемого в Администрации.

1.4. Ознакомление сотрудников администрации Октябрьского района города Ставрополя с требованиями Порядка проводит Администратор безопасности ИСПДн под роспись в журнале или на самом документе.

1.5. В целях закрепления знаний по вопросам практического исполнения требований Порядка, разъяснения возникающих вопросов, проводятся (при необходимости) персональные инструктажи пользователей ИСПДн администрации Октябрьского района города Ставрополя.

1.6. В случае невозможности исполнения требований настоящего Порядка в полном объеме, например:

- в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний;
- злоумышленных действий.

Практическая «глубина» исполнения настоящего Порядка определяется Администратором безопасности ИСПДн по согласованию с ответственным по защите ПДн администрации Октябрьского района города Ставрополя.

2. ФУНКЦИИ СОТРУДНИКОВ

1.1. Непосредственное исполнение, организация и контроль исполнения требований настоящего Порядка в Администрации Октябрьского района города Ставрополя осуществляется всеми пользователями ИСПДн, а именно:

- Пользователь ИСПДн:
  - регулярная (с частотой, установленной настоящим Порядком) смена используемой в работе парольной информации;
  - выбор парольной информации с качеством, установленным настоящим Порядком;
- Администратор безопасности ИСПДн:
  - организационно-методическое обеспечение процессов генерации, смены и удаления паролей в ИСПДн администрации Октябрьского района города Ставрополя;
  - разработка всех необходимых инструкций по вопросам парольной защиты ИСПДн администрации Октябрьского района города Ставрополя;
  - организация доведения до пользователей ИСПДн администрации Октябрьского района города Ставрополя требований по парольной защите;

- организация периодического и выборочного контроля исполнения сотрудниками Администрации требований настоящего Порядка;
- согласование выдачи управляющих учетных записей к ИСПДн;
- текущий контроль действий персонала администрации Октябрьского района города Ставрополя по работе с паролями (автоматизированный контроль качества паролей – при наличии программно-технических средств);
- техническое обеспечение (при наличии программно-технических средств) процессов генерации/выбора, смены и удаления паролей, соответствующая конфигурация ИСПДн.

3. КАЧЕСТВО И ОБРАЩЕНИЕ ПАРОЛЬНОЙ ИНФОРМАЦИИ

3.1. Пароли доступа к аппаратно-программным вычислительным средствам, информационным ресурсам Администрации формируются (выбираются) пользователями этих ресурсов с учетом следующих требований к качеству парольной информации:

№ п/п	Параметр качества пароля	Администратор	Пользовател
1.	Минимальная длина пароля в символах	10	8[1]
2.	Максимальная длина пароля в символах	32	16
3.	Содержание в пароле букв верхнего и нижнего регистра	да	да
4.	Содержание в пароле специальных символов (@, #, $, &, * и т.п.) и цифр	обязательно	рекомендуетс я
5.	Содержание в пароле личных имен, фамилий, кличек домашних животных, № телефонов, дат рождения, географических названий, именований АРМ и т.п.	нет	нет
6.	Содержание в пароле общепринятых сокращений (ПЭВМ, ЛВС, USER, SYSOP и т.д.)	нет	нет
7.	Минимальное отличие нового пароля от предыдущего (в позициях)	3	3
8.	Максимальный срок действия пароля	30 дней	60 дней
9.	Минимальный срок действия пароля	нет	нет
10.	Дополнительный (типа ТМ, eToken[2] или другие электронные ключи) идентификатор	рекомендуется	рекомендуетс я

[1] При использовании электронных ключей (USB, Touch Memory) не менее 6 символов.

[2] При использовании электронного ключа такого типа требования вышеприведенной таблицы актуальны только по пунктам №1 и №9.

№ п/п	Параметр качества пароля	Администратор	Пользовател
11.	Пароль на заставку монитора	да	да

3.2. Хранение сотрудником (администратором, пользователем) личных паролей допускается только в личном сейфе (запираемом шкафу, ящике), либо в сейфе (запираемом шкафу, ящике) администратора, либо в сейфе (запираемом шкафу, ящике) руководителя отдела. При этом бумажный носитель должен быть упакован в отдельный опечатанный конверт.

3.3. Личные пароли и/или дополнительные идентификаторы (электронные ключи) пользователи и администраторы самостоятельно никому не имеют права сообщать и(или) передавать[3];

3.4. Внеплановая смена/удаление пароля (и при возможности учетной записи) пользователя или администратора автоматизированной системы администрации Октябрьского района города Ставрополя в случае прекращения его полномочий должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

3.5. Внеплановая полная смена паролей должна производиться в случае прекращения полномочий Администратора безопасности ИСПДн, других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению ИСПДн, либо полномочия по управлению подсистемой защиты информации ИСПДн[4].

3.6. В случае компрометации пароля доступа в ИСПДн Администратором безопасности ИСПДн должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля и обстоятельств компрометации.

3.7. Все сотрудники администрации Октябрьского района города Ставрополя обязаны по первому требованию Администратора безопасности ИСПДн предъявить значения действующего личного пароля для контроля соответствия установленным требованиям, а после проверки провести немедленную его смену.

3.8. Администратор безопасности ИСПДн, по согласованию с ответственным за обеспечение безопасности ПДн проводит ежеквартальный выборочный контроль выполнения сотрудниками администрации Октябрьского района города Ставрополя требований Порядка с отметками в отдельном журнале. О фактах несоответствия качества паролей и/или условий обеспечения их сохранности Администратор ИСПДн докладывает ответственному за обеспечение безопасности ПДн.

---

[3] Сотрудники администрации Октябрьского района города Ставрополя раскрывают значение своего пароля и/или передают физический идентификатор только своим непосредственным руководителям в случае производственной необходимости и/или при проведении контрольно-проверочных мероприятий. По окончанию производственных и/или контрольно-проверочных работ сотрудники производят немедленную смену значений раскрытых паролей

[4] Смена паролей производится для учетных записей систем, в которых не используется аутентификация посредством дополнительных идентификаторов (Touch Memory, eToken и т.п.)

4. ОБРАЩЕНИЕ ДОПОЛНИТЕЛЬНЫХ ИДЕНТИФИКАТОРОВ

4.1. В целях усиления процедур идентификации и аутентификации в ИСПДн Администрации, пользователи ИСПДн могут использовать дополнительные индивидуальные электронные идентификаторы (смарт-карты, eToken и т.д.) совместно с личным паролем доступа.

4.2. Дополнительные идентификаторы выдаются и учитываются в соответствии с «Инструкцией по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем персональных данных»:

- сотрудники получают дополнительные идентификаторы под роспись;
- Администратор безопасности ИСПДн, по обращению к нему сотрудников, регистрирует дополнительные идентификаторы в ИСПДн администрации Октябрьского района города Ставрополя и инструктирует сотрудников с учетом требований настоящего порядка и правил эксплуатации для дополнительных идентификаторов.

4.3. Сотрудники администрации Октябрьского района города Ставрополя, получившие в пользование дополнительные идентификаторы, лично обеспечивают надежное круглосуточное безопасное хранение и использование идентификаторов. Оставление идентификатора без присмотра запрещается.

4.4. В случае утери дополнительного идентификатора сотрудники немедленно ставят об этом в известность Администратора безопасности ИСПДн и своего непосредственного руководителя. Администратор организуют немедленную блокировку утерянных ключей в автоматизированных системах.

5. ПЕРЕСМОТР ПОРЯДКА

5.1. Порядок подлежит полному пересмотру в случае приобретения администрацией Октябрьского района города Ставрополя новых (дополнительных к имеющимся штатным) автоматизированных средств управления парольной защитой и(или) генерации/выбора паролей.

5.2. В остальных случаях Порядок подлежит частичному пересмотру.

5.3. Полный пересмотр данного Порядка проводится с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн Администрации.

5.4. Изменения в Порядке (сведения о них) фиксируется в листе регистрации изменений (Приложение 1).

5.5. Вносимые изменения не должны противоречить другим положениям Порядка. При получении изменений к данному Порядку, руководители отделов администрации Октябрьского района города Ставрополя в течение трех рабочих дней вносят свои предложения и/или замечания к поступившим изменениям.

6. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ПОРЯДКА

6.1. Ответственность за соблюдение требований настоящего Порядка возлагается на всех сотрудников администрации Октябрьского района города Ставрополя.

6.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам парольной защиты возлагается на Администратора безопасности ИСПДн.

6.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности ПДн администрации Октябрьского района города Ставрополя.

ПРИЛОЖЕНИЕ 1. ФОРМА РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В ИНСТРУКЦИИ

ЛИСТ № _____ регистрации изменений в Порядке

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (олжность, подпись)

Приложение № 6
к приказу главы администрации
Октябрьского района
города Ставрополя
от «11» 08 2017 г. № 171

ИНСТРУКЦИЯ
о порядке обработки персональных данных в администрации Октябрьского района города Ставрополя

г. Ставрополь
2017 г.

1. Общие положения

1.1. Настоящая Инструкция разработана на основании требований Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и устанавливает порядок обработки, распространения и использования персональных данных в администрации Октябрьского района города Ставрополя.

1.2. Основные понятия:

персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место его рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

оператор - государственный или муниципальный орган, юридическое или физическое лицо, организующие и осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

обработка персональных данных - действия с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение, использование, распространение, обезличивание, блокирование, уничтожение персональных данных;

распространение персональных данных - действия, направленные на передачу определенному кругу лиц или ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо другим способом;

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

конфиденциальность персональных данных - обязательное для соблюдения оператором требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

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

2. Конфиденциальность персональных данных

2.1. Операторами должна обеспечиваться конфиденциальность персональных данных, за исключением:

1) в случае обезличивания персональных данных;

2) в отношении общедоступных персональных данных.

Общедоступные источники персональных данных могут включать с письменного согласия субъекта его фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

2.2. Оператор при обработке персональных данных 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.

3. Условия обработки персональных данных

3.1. Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

4) обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4. Порядок обработки персональных данных

4.1. В администрации Октябрьского района города Ставрополя на основании представленных руководителями структурных подразделений заявок составляется перечень разрабатываемых в данном подразделении документов, включающих персональные данные граждан.

В заявку включаются сведения:

- наименование структурного подразделения;
- цель обработки персональных данных;
- перечень обрабатываемых персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- должность и фамилия лица, осуществляющего действия с персональными данными.

4.2. Обработка персональных данных может производиться с использованием средств автоматизации или без использования таковых.

4.3. Сбор и обработка персональных данных осуществляются только с согласия в письменной форме субъекта персональных данных, согласно Приложению к настоящей инструкции.

4.4. Обработка, использование и распространение персональных данных должны производиться в строгом соответствии с полномочиями администрации Октябрьского района города Ставрополя.

5. Меры по защите информации, содержащей персональные данные

5.1. Учет документов по обработке персональных данных без использования автоматизированных систем должен производиться отдельным делопроизводством. На документах должна указываться пометка «Персональные данные». Документы должны храниться в надежно запираемых шкафах и сейфах. Ключи от них, а также от помещений должны находиться у ответственных за данную работу лиц.

5.2. При эксплуатации автоматизированных систем необходимо соблюдать следующие требования:

- к работе допускаются только лица, назначенные соответствующим распоряжением;
- на ПЭВМ, дисках, папках и файлах, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы);
- на период обработки защищаемой информации в помещении могут находиться лица, допущенные в установленном порядке к обрабатываемой информации; допуск других лиц может осуществляться с разрешения главы администрации Октябрьского района города Ставрополя;
- в случае размещения в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации;
- по окончании обработки информации оператор обязан произвести стирание остаточной информации на жестком диске и в оперативной памяти;

- при увольнении или перемещении оператора автоматизированной системы ответственным за обеспечение безопасности персональных данных в администрации Октябрьского района города Ставрополя должны быть приняты организационные меры по оперативному изменению паролей (идентификаторов);

- учет съемных носителей информации с персональными данными допускается учитывать совместно с другими документами по установленным для этого учетным формам; при этом работникам, ответственным за их учет, на этих носителях информации предварительно проставляются любым доступным способом следующие учетные реквизиты: учетный номер и дата, пометка «Персональные данные», подпись этого работника;

- носители информации должны храниться в местах, недоступных для посторонних лиц.

Запрещаются обработка и хранение сведений о персональных данных на ПЭВМ, подключенной к сети имеющей доступ к информационно-телекоммуникационной сети «Интернет» без межсетевого экрана, а также их передача по незащищенным каналам связи.

Приложение 1

СОГЛАСИЯ
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Фамилия, имя и отчество субъекта _____

_____

Адрес _____

_____

Предъявленный документ _____ серия _____ № _____

выдан «___»_____ 20__ г. кем_____

2. Наименование Оператора - Администрация Октябрьского района города Ставрополя, 355006, г. Ставрополь, ул. Голенева, 21

3. Цель обработки персональных данных – предоставление государственных (муниципальных) услуг.

4. Перечень персональных данных, на обработку которых дается согласие: фамилия, имя, отчество, год, месяц, дата и место рождения, пол, возраст, адрес, гражданство, сведения об образовании, контактная информация (домашний(е) адрес(а), номера домашнего и мобильного телефонов), паспортные данные, сведения о семейном положении, о наименовании организаций, в которых осуществлялась трудовая деятельность, о суммах страховых взносов (прочие сведения, имеющиеся в выписке из индивидуального лицевого счета), любые иные данные, которые могут потребоваться Оператору в связи с осуществлением целей, указанных в п. 3 настоящего документа (далее – «Персональные данные».

5. Перечень действий с персональными данными - обработка Персональных данных, включая сбор (получение), систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

При обработке Персональных данных Оператор принимает 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.

Заявитель уведомлен о том, что он (она) в любой момент времени, письменно обратившись к Оператору, может ознакомиться с Персональными данными, обратиться с просьбой о предоставлении дополнительной информации в отношении хранения и обработки Персональных данных или же потребовать внесения любых необходимых изменений в Персональные данные для их уточнения.

6. Срок действия согласия — бессрочно.

7. Порядок отзыва согласия - Заявитель может отозвать настоящее согласие путем направления Оператору письменного уведомления не менее чем за 90 (Девяносто) дней до предполагаемой даты отзыва настоящего согласия. Заявитель соглашается на то, что в течение указанного срока Оператор не обязан прекращать обработку персональных данных и уничтожать персональные данные Заявителя. Отзыв не будет иметь обратной силы в отношении Персональных данных, прошедших обработку до вступления в силу такого отзыва. По истечении данного периода Оператор прекращает обработку Персональных данных Заявителя, и удаляет их из электронной базы данных, Персональные данные, содержащиеся на бумажных носителях (личные дела отдельных категорий граждан), хранятся в архивах Оператора до истечения срока, установленного для хранения данного вида документов действующим законодательством Российской Федерации.

«___»_____ 20__ г. _____

(Ф.И.О.)

Приложение 2

ЗАПРОС
СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ ОБ ОТЗЫВЕ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____
(Фамилия, имя, отчество)

Документ, удостоверяющий личность _____
(Вид документа)

Серия, номер _____Выдан _____
(Кем и когда выдан)

_____

прошу прекратить обработку моих персональных данных в «Название компании»
(юридический адрес:_____)
по следующими причинам:

_____

_____

_____ _____ «___»_____ 20__ г
(Ф.И.О.) (подпись)

Приложение № 4
к приказу главы Администрации
Октябрьского района города
Ставрополя

от «11» 08 2017 г. №174

ИНСТРУКЦИЯ

АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ ОКТЯБРЬСКОГО РАЙОНА ГОРОДА СТАВРОПОЛЯ

г. Ставрополь
2017 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Администратор информационной безопасности (ИБ) информационной системы персональных данных (ИСПДн) Администрации Октябрьского района города Ставрополя назначается приказом главы Администрации Октябрьского района города Ставрополя и функционально подчиняется руководителю подразделения, в штате которого он состоит. Администратор ИБ ИСПДн руководствуется требованиями нормативных документов Российской Федерации, нормативных актов Администрации Октябрьского района города Ставрополя, настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

Администратор ИБ ИСПДн в пределах своих функциональных обязанностей обеспечивает работоспособность ИСПДн, безопасность информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (СВТ) в ИСПДн Администрации.

Должностные лица Администрации Октябрьского района города Ставрополя, задействованные в обеспечении функционирования ИСПДн, могут быть ознакомлены с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

В случае увольнения администратор ИБ ИСПДн Администрации Октябрьского района города Ставрополя обязан передать руководителю подразделения, в штате которого он состоит, все носители защищаемой информации Администрации Октябрьского района города Ставрополя (рукописи, черновики, чертежи, диски, дискеты, распечатки с принтеров, модели, материалы, изделия и пр.), которые находились в его распоряжении в связи с выполнением им служебных обязанностей во время работы в Администрации Октябрьского района города Ставрополя.

2. ОБЯЗАННОСТИ АДМИНИСТРАТОРА ИБ ИСПДН

Администратор ИБ ИСПДн обязан:

- знать перечень установленных в подразделении СВТ и перечень задач, решаемых с их использованием;
- обеспечивать работоспособность средств вычислительной техники ИСПДн Управления, проводить организационно-технические мероприятия по их обслуживанию;
- устанавливать и настраивать элементы ИСПДн и средства защиты информации, а также выполнять другие возложенные на него работы в соответствии с распорядительными, инструктивными и методическими материалами в части, его касающейся;
- рассматривать целесообразность применения новых технологий для повышения эффективности функционирования ИСПДн Администрации Октябрьского района города Ставрополя;

- подготавливает обоснования и спецификации для закупки, заказывает новые элементы ИСПДн и расходные материалы; поддерживает резерв расходных материалов; изучает рынок программных средств и предоставляет рекомендации по приобретению и внедрению системного и прикладного программного обеспечения;

- выполнять своевременное обновление программного обеспечения элементов ИСПДн и средств защиты персональных данных (СЗПДн) по мере появления таких обновлений;

- выполнять резервное копирование и восстановление данных;

- обеспечивать контроль за выполнением пользователями требований «Инструкции пользователю ИСПДн»;

- осуществлять контроль за работой пользователей автоматизированных систем, выявление попыток НСД к защищаемым информационным ресурсам и техническим средствам ИСПДн Администрации Октябрьского района города Ставрополя;

- осуществлять настройку средств защиты, выполнять другие действия по изменению элементов ИСПДн;

- осуществлять учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в специальный журнал (учетную карточку). Учтенные носители информации выдавать пользователям под роспись;

- осуществлять текущий и периодический контроль работы средств и систем защиты информации;

- осуществлять текущий контроль технологического процесса обработки защищаемой информации;

- периодически осуществлять тестирование всех функций системы защиты с помощью тестовых программ, имитирующих попытки НСД, при изменении программной среды и персонала ИСПДн;

- в случае возникновения нештатных ситуаций (сбоев в работе СЗПДн) немедленно докладывать ответственному за обеспечение безопасности ПДн;

- участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации;

- участвовать в проведении работ по восстановлению работоспособности средств и систем защиты информации;

- вести «Журнал учета нештатных ситуаций», учитывать факты вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ПЭВМ. Форма журнала приведена в «Инструкции по действиям персонала в нештатных ситуациях»;

- проводить обучение персонала и пользователей вычислительной техники правилам работы с СВТ и средствами защиты информации с отметкой в карточке инструктажа (Приложение 2);

- участвовать в разработке нормативных и методических материалов, связанных с функционированием СВТ и применением средств защиты

информации, выполнением мероприятий по обеспечению защиты информации;

- регулярно анализировать работу любых элементов АС, электронных системных журналов средств защиты для выявления и устранения неисправностей, а также для оптимизации ее функционирования.

3. ПРАВА АДМИНИСТРАТОРА ИБ ИСПДН

Администратор ИБ ИСПДн имеет право:

- отключать любые элементы СЗПДн при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке;
- в установленном порядке изменять конфигурацию элементов ИСПДн и СЗПДн;
- требовать от сотрудников Администрации Октябрьского района города Ставрополя соблюдения правил работы в ИСПДн, приведенных в «Инструкции пользователя ИСПДн»;
- требовать от пользователей безусловного соблюдения установленной технологии обработки защищаемой информации и выполнения требований внутренних документов Администрации Октябрьского района города Ставрополя, регламентирующих вопросы обеспечения безопасности и защиты информации;
- обращаться к ответственному за обеспечение безопасности ПДн с требованием о прекращении обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации;
- вносить свои предложения по совершенствованию функционирования ИСПДн Администрации Октябрьского района города Ставрополя;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности в ИСПДн Администрации.

4. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА ИБ ИСПДН

Администратор ИБ ИСПДн несет ответственность:

- за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими инструктивными документами в соответствии с действующим законодательством Российской Федерации, за полноту и качество проводимых им работ по обеспечению защиты информации;
- за правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим законодательством Российской Федерации;

- за разглашение сведений конфиденциального характера и другой защищаемой информации Управления в пределах, определенных действующим законодательством Российской Федерации;

- на администратора ИБ ИСПДн возлагается персональная ответственность за работоспособность и надлежащее функционирование средств обработки ПДн в ИСПДн и средств защиты персональных данных Администрации Октябрьского района города Ставрополя.

5. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн Администрации Октябрьского района города Ставрополя, приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности ПДн Администрации Октябрьского района города Ставрополя.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности ПДн Администрации Октябрьского района города Ставрополя с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн Администрации Октябрьского района города Ставрополя.

Форма регистрации изменений в Инструкцию представлена в Приложении 3.

Вносимые изменения не должны противоречить другим положениям Инструкции.

6. ОТВЕТСТВЕННЫЕ ЗА КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственным за контроль выполнения требований данной Инструкции является ответственный за обеспечение безопасности ПДн.

ПРИЛОЖЕНИЕ 2. ФОРМА РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В ИНСТРУКЦИЮ

ЛИСТ
регистрации изменений в инструкции

№ п.п.	Дата	Внесенное изменение	Основание (наименование, номер и дата документа)	Кем внесено изменение (должность, подпись)

ПРИЛОЖЕНИЕ 1. КАРТОЧКА ИНСТРУКТАЖА

КАРТОЧКА № ____
ПРОВЕДЕНИЯ ИНСТРУКТАЖА
ПО ВОПРОСАМ ЗАЩИТЫ ИНФОРМАЦИИ

Отдел		
Дата		
Фамилия, инициалы инструктируемого	Должность	Роспись
Вид инструктажа (в связи с чем проводится)		
Краткое содержание инструктажа		
Инструктаж провел Администратор ИБ ИСПДн:		

Примечание: Заполненная карточка хранится у Администратора ИБ ИСПДн.

Приложение № 8
к приказу главы Администрации
Октябрьского района города Ставрополя

от «11» 08 2017 г. № 171

ИНСТРУКЦИЯ

ПО ВНЕСЕНИЮ ИЗМЕНЕНИЙ В СПИСКИ ПОЛЬЗОВАТЕЛЕЙ И НАДЕЛЕНИЮ ИХ ПОЛНОМОЧИЯМИ ДОСТУПА К РЕСУРСАМ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ ОКТЯБРЬСКОГО РАЙОНА ГОРОДА СТАВРОПОЛЯ

г. Ставрополь
2017 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Инструкция по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем персональных данных (ИСПДн) Администрации Октябрьского района города Ставрополя устанавливает порядок изменения списка пользователей и порядок изменения их прав в информационных системах персональных данных.

Должностные лица Администрации Октябрьского района города Ставрополя, задействованные в обеспечении функционирования ИСПДн, знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

Ознакомление с требованиями Инструкции пользователей ИСПДн осуществляет администратор информационной безопасности (ИБ) ИСПДн под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

Непосредственное исполнение настоящей Инструкции определяется администратором ИБ ИСПДн, по согласованию с ответственным за обеспечение безопасности персональных данных (ПДн) Администрации Октябрьского района города Ставрополя.

2. ПОРЯДОК ИСПОЛЬЗОВАНИЯ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ

С целью соблюдения принципа персональной ответственности за свои действия, каждому сотруднику, допущенному к работе с ИСПДн должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в системе.

В случае производственной необходимости, некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей).

Использование несколькими сотрудниками при самостоятельной работе в ИСПДн одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

Использование сотрудником имени пользователя, сопоставленного с другим сотрудником (учетной записи другого сотрудника), при работе в ИСПДн ЗАПРЕЩЕНО.

3. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ПОЛЬЗОВАТЕЛЯМ ПРАВ ДОСТУПА К ИСПДн

Процедура регистрации (создания учетной записи) пользователя и предоставления (изменения) ему прав доступа к ресурсам ИСПДн инициируется приказом о допуске сотрудника к работам в ИСПДн или заявкой руководителя подразделения, в котором числится данный сотрудник. Заявка согласовывается с ответственным за обеспечение безопасности ПДн, после чего администратором ИБ ИСПДн создается учетная запись. Форма заявки приведена в Приложении 1.

На основании приказа либо при получении заявки на предоставление (изменение) прав доступа пользователя к ресурсам ИСПДн администратор ИБ ИСПДн в зависимости от характера заявки:

- создает учетную запись;
- производит изменение прав доступа учетной записи;
- осуществляет блокирование учетной записи.

При предоставлении сотруднику прав доступа к ресурсам необходимо руководствоваться принципом предоставления минимальных прав для решения требуемых задач.

Руководители отделов Администрации Октябрьского района города Ставрополя несут ответственность за минимальную достаточность прав доступа имеющихся у пользователей их отделов. В случае наличия у пользователей избыточных для работы прав доступа руководители отделов ставят об этом в известность администратора ИБ ИСПДн, который вносит необходимые изменения в соответствии с настоящей Инструкцией.

При выдаче пользователю персонального идентификатора, факт выдачи должен фиксироваться в соответствующем журнале.

Целесообразно документирование прав доступа в электронном виде, для чего создается специальная база данных, в которой указываются следующие данные:

- фамилия, имя, отчество пользователя;
- отдел Администрации Октябрьского района города Ставрополя;
- учетная запись;
- контролируемый ресурс;
- права доступа;
- отметка об удалении учетной записи при увольнении.

Изменения в конфигурации механизмов защиты информации производятся только администратором ИБ ИСПДн и только в соответствии с документацией на средства защиты информации ПДн.

При изменении статуса пользователя (увольнение, перевод на другую должность и т.п.) руководитель соответствующего отдела, в котором числится данный пользователь, подает заявку об изменении прав доступа пользователя (Приложение 1).

4. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн Администрации Октябрьского района города Ставрополя, приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности ПДн Администрации Октябрьского района города Ставрополя.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности ПДн Комитета с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн Администрации Октябрьского района города Ставрополя.

Форма регистрации изменений в Инструкции представлена в Приложении 3.

Вносимые изменения не должны противоречить другим положениям Инструкции.

5. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников, работающих в ИСПДн Администрации Октябрьского района города Ставрополя.

Ответственность за организацию контрольных и проверочных мероприятий по вопросам управления правами пользователей возлагается на Администратора ИБ ИСПДн.

Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности ПДн Администрации Октябрьского района города Ставрополя.

ПРИЛОЖЕНИЕ 1. ЗАЯВКА НА ВНЕСЕНИЕ ИЗМЕНЕНИЙ В СПИСКИ ПОЛЬЗОВАТЕЛЕЙ

Руководителю управления

(резолюция)

ЗАЯВКА

на внесение изменений в списки пользователей

_____

_____

(наименование автоматизированной системы, ПЭВМ)

и наделение пользователя полномочиями доступа к ресурсам системы

Прошу *зарегистрировать пользователем ИСПДн (исключить из списка пользователей ИСПДн, изменить полномочия пользователя)*

(ненужное зачеркнуть)

_____

(должность с указанием подразделения)

_____,

(фамилия имя и отчество сотрудника)

предоставив ему полномочия (лишив его полномочий), необходимые *(-х)* для решения задач: (ненужное зачеркнуть)

_____

_____

_____

_____

_____

_____

Руководитель отдела _____

(наименование подразделения)

«___» _____ 201__ г. _____ _____

(подпись) (фамилия, инициалы)

Оборотная сторона заявки

Пользователь _____

зарегистрирован (исключен из списка пользователей, изменены полномочия пользователя)

(ненужное зачеркнуть)

Персональный идентификатор номер _____ *выдан (изъят)*

(ненужное зачеркнуть)

Внесены следующие изменения:

_____

_____

_____

_____

_____

_____

_____

_____

Администратор ИБ ИСПДн

«___» _____ 201__ г. _____ _____

(подпись) (фамилия, инициалы)

Учетное имя, *персональный идентификатор* и начальные значения

(при отсутствии зачеркнуть)

паролей получил, о порядке смены пароля при первом входе в систему проинструктирован

Пользователь

_____

(подпись, фамилия, инициалы)

«___» _____ 201__ г.

ПРИЛОЖЕНИЕ 2. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

ЛИСТ
регистрации изменений в Инструкции

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

ЛИСТ ОЗНАКОМЛЕНИЯ

с Инструкцией по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем персональных данных Администрации Октябрьского района города Ставрополя

№ п/п	Фамилия, инициалы сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении

Приложение № 9
к приказу главы администрации
Октябрьского района города Ставрополя

от «11» 08 2017 г. № 174

И Н С Т Р У К Ц И Я

ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ ОКТЯБРЬСКОГО РАЙОНА ГОРОДА СТАВРОПОЛЯ

г. Ставрополь
2017 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Ознакомление сотрудников с требованиями настоящей Инструкции проводит администратор информационной безопасности (ИБ) информационной системы персональных данных (ИСПДн) Администрации Октябрьского района города Ставрополя под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

2. ФУНКЦИИ И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ

Каждый сотрудник Администрации Октябрьского района города Ставрополя, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационных систем персональных данных, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- выполнять свои функциональные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам, техническим средствам, полученным в установленном порядке;
- знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн;
- хранить в тайне свой пароль (пароли);
- исполнять требования «Порядка парольной защиты в автоматизированных системах», «Инструкции по организации антивирусной защиты ИСПДн», а также других документов, регламентирующих вопросы работы в ИСПДн и обеспечение безопасности информации в части, его касающейся;
- немедленно ставить в известность администратора ИСПДн и руководителя подразделения в случае утери личных реквизитов доступа, при компрометации личных паролей, подозрении на совершение попыток несанкционированного доступа (НСД) к персональным электронно-вычислительным машинам (ПЭВМ), обнаружении несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн;
- немедленно ставить в известность администратора ИСПДн при обнаружении отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн, выхода из строя или неустойчивого функционирования устройств ПЭВМ (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных технических средств защиты информации;

- при обработке на ПЭВМ защищаемой информации присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним ПЭВМ в подразделении;
- при обработке на ПЭВМ защищаемой информации и необходимости использовать носители информации, применять только учтенные носители.

2.1. Сотрудникам ЗАПРЕЩАЕТСЯ:

- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;
- хранить и обрабатывать личную информацию на ПЭВМ и серверах ИСПДн;
- при работе в сети Интернет:
  - использовать информационные ресурсы сети Интернет, содержание которых нарушает действующее законодательство Российской Федерации;
  - использовать информационные ресурсы сети Интернет для целей, не связанных с областью производственной деятельности пользователя;
  - использовать информационные ресурсы сети Интернет в личных целях;
  - вносить изменения в состав и/или процесс работы внешних информационных ресурсов, если такие изменения не санкционированы собственником (владельцем) соответствующего ресурса;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства;
- оставлять без присмотра включенную ПЭВМ, не активизировав средства защиты от НСД;
- оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа;
- оставлять без личного присмотра в легкодоступном месте на рабочем месте или где бы то ни было свои машинные носители и распечатки, содержащие сведения ограниченного распространения;
- использовать в работе неучтенные носители информации для обработки защищаемой информации;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, об обнаружении такого рода ошибок – ставить в известность администратора ИБ ИСПДн и руководителя своего отдела.

3. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн Администрации Октябрьского района города Ставрополя, приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности персональных данных (ПДн) администрации Октябрьского района города Ставрополя.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности ПДн администрации Октябрьского района города Ставрополя с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн Управления.

Форма регистрации изменений в Инструкцию представлена в Приложении 1.

Вносимые изменения не должны противоречить другим положениям Инструкции.

4. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников администрации Октябрьского района города Ставрополя.

Ответственность за организацию контрольных и проверочных мероприятий возлагается на администратора ИБ ИСПДн.

Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности ПДн Администрации.

ПРИЛОЖЕНИЕ 1. ФОРМА РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В ИНСТРУКЦИИ

ЛИСТ
регистрации изменений в Инструкцию

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Приложение № 10
к приказу главы Администрации
Октябрьского района города Ставрополя

от «11» 08 2017 г. № 171

ИНСТРУКЦИЯ

ПО ДЕЙСТВИЯМ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ ОКТЯБРЬСКОГО РАЙОНА ГОРОДА СТАВРОПОЛЯ В НЕШТАТНЫХ СИТУАЦИЯХ

г. Ставрополь
2017 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция предназначена для определения порядка действий пользователей информационной системы персональных данных (ИСПДн) Администрации Октябрьского района города Ставрополя при возникновении нештатных ситуаций.

Нештатными ситуациям являются:

1) разглашение информации ограниченного доступа, не составляющей государственную тайну (далее защищаемая информация), сотрудниками Администрации Октябрьского района города Ставрополя, имеющими к ней право доступа, в том числе:

- разглашение информации лицам, не имеющим права доступа к защищаемой информации;
- передача информации по открытым линиям связи;
- обработка информации на незащищенных технических средствах обработки информации;
- опубликование информации в открытой печати и других средствах массовой информации;
- передача носителя информации лицу, не имеющему права доступа к ней;
- утрата носителя с информацией;

2) неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

- несанкционированное изменение информации;
- несанкционированное копирование информации.

3) Несанкционированный доступ к защищаемой информации:

- подключение технических средств к средствам и системам объекта информатизации;
- использование закладочных устройств;
- маскировка под зарегистрированного пользователя;
- использование дефектов программного обеспечения объекта информатизации (ОИ);
- использование программных закладок;
- применение программных вирусов;
- хищение носителя защищаемой информации;
- нарушение функционирования технических средств (ТС) обработки информации;

- блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;

4) дефекты, сбои, отказы, аварии ТС и систем ОИ;
5) дефекты, сбои и отказы программного обеспечения ОИ;
6) сбои, отказы и аварии систем обеспечения ОИ;
7) природные явления, стихийные бедствия:
   - термические, климатические факторы (пожары, наводнения и т.д.);
   - механические факторы (землетрясения и т.д.);
   - электромагнитные факторы (грозовые разряды и т.д.).

В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей инструкцией администратором информационной безопасности (ИБ) ИСПДн, ответственным за обеспечение безопасности персональных данных (ПДн) Администрации Октябрьского района города Ставрополя вырабатывается конкретный план действий с учетом текущей ситуации.

Резервируемые в Администрации Октябрьского района города Ставрополя информационные ресурсы и способы их резервирования представлены в Приложении 1 к настоящей Инструкции.

Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении 2 к настоящей Инструкции.

Для эффективной реализации мероприятий по реагированию в случае нештатных ситуаций должны проводиться регулярные тренировки по различным нештатным ситуациям. По результатам тренировки в случае необходимости проводится уточнение настоящей Инструкции.

Должностные лица Администрации Октябрьского района города Ставрополя знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

Ознакомление с требованиями Инструкции сотрудников Администрации Октябрьского района города Ставрополя осуществляет администратор ИБ ИСПДн под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

2. ПОРЯДОК ДЕЙСТВИЙ ПРИ ОБНАРУЖЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

2.1. Классификация нештатных ситуаций

Нештатные ситуации классифицируются в соответствии с оценками, представленными в таблице 3.1.

Таблица 3.1. Оценки нештатных ситуаций

Нештатная ситуация		**Оценка ситуации (раздел Инструкции)**
Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа		(2.2)
Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации	Несанкционированное копирование конфиденциальной информации	Обнаружился случившийся факт (2.2)
		Производится в текущий момент (2.3)
	Несанкционированное изменение конфиденциальной информации	Обнаружился случившийся факт (2.2)
		Производится в текущий момент (2.3)
Несанкционированный доступ к защищаемой информации	Подключение технических средств к средствам и системам объекта информатизации (ОИ)	Обнаружился случившийся факт (2.2)
		Производится в текущий момент (2.4)
	Установка закладочных устройств	Обнаружение установленных (2.2)
		Устанавливаются в настоящий момент (2.5)
	Маскировка под зарегистрированного пользователя	Внешним злоумышленником в текущий момент (2.6)
		Внутренним злоумышленником, либо производилась в прошлом (2.2)
	Использование дефектов программного обеспечения ОИ	Внешним злоумышленником в текущий момент (2.7)
		Внутренним злоумышленником, либо производилось в прошлом (2.2)
	Использование программных закладок	Внешним злоумышленником в текущий момент (2.8)
		Внутренним злоумышленником, либо производилось в прошлом (2.2)
	Обнаружение программных вирусов	(2.9)
	Хищение носителя защищаемой информации	(2.2)

Нештатная ситуация		Оценка ситуации (раздел Инструкции)
	Нарушение функционирования ТС обработки информации злоумышленником	Производится в текущий момент (2.10)
		Обнаружился случившийся факт (2.11)
	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку	Производится в текущий момент внешним злоумышленником (2.12)
		Производится в текущий момент внутренним злоумышленником (2.13)
		Обнаружился случившийся факт (2.14)
Ошибки пользователей системы при эксплуатации программных средств, ТС, средств и систем защиты информации		Ошибка повлекла утерю или повреждение защищаемой информации (2.15)
		Ошибка привела к нарушению работоспособности ТС и ПО (2.16)
Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ		(2.17)
Сбои, отказы и аварии систем обеспечения ОИ		(2.18)
Природные явления, стихийные бедствия	Несущие угрозу жизни человека	(2.19)
	Не несущие угрозу жизни человека	(2.20)

2.2. Нештатные ситуации, которые повлекли утечку или повреждение защищаемой информации, либо созданы внутренним злоумышленником

При обнаружении нештатных ситуаций, которые повлекли утечку или повреждение защищаемой информации, либо созданы внутренним злоумышленником, создается комиссия.

В первую очередь администратором ИБ ИСПДн предпринимаются действия по сбору и обеспечению сохранности улик незаметно для злоумышленника при нештатных ситуациях, связанных с:

- разглашением конфиденциальной информации;
- обнаружением несанкционированно скопированной или измененной конфиденциальной информации;
- обнаружением подключения технических средств к средствам и системам объекта информатизации;
- обнаружением закладочных устройств;
- маскировкой под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки в прошлом (как внутренним, так и внешним злоумышленником);

- использованием дефектов программного обеспечения ОИ внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);
- использованием программных закладок внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);
- хищением носителя защищаемой информации.

Комиссия, дополнительно к общему порядку действий (в соответствии с разделом 3), должна:

- если это возможно, определить организации, в которые произошла утечка конфиденциальной информации;
- определить возможные контрмеры, призванные уменьшить потери от утечки информации.

2.3. Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней

В случае обнаружения злоумышленника неправомерно копирующего, либо изменяющего защищаемую информацию выполняются следующие действия.

2.3.1. Первоочередные действия

1. Администратор ИБ ИСПДн прерывает несанкционированный процесс.
2. Администратор ИБ ИСПДн блокирует доступ к ИСПДн Администрации Октябрьского района города Ставрополя для злоумышленника.
3. Администратор ИБ ИСПДн совместно с ответственным за обеспечение безопасности ПДн Комитета удаляют нарушителя от средств ИСПДн.
4. Ответственным за обеспечение безопасности ПДн совместно с администратором ИБ ИСПДн предпринимаются действия по сбору и обеспечению сохранности улик.

2.3.2. Последующие действия

Создается комиссия для расследования инцидента.

2.4. Подключение технических средств к средствам и системам ОИ в текущий момент времени

В случае обнаружения злоумышленника, производящего подключение к техническим средствам и системам ОИ в текущий момент времени, выполняются следующие действия.

2.4.1. Первоочередные действия

1. Администратор ИБ ИСПДн прерывает процесс работы нарушителя.
2. В случае если нарушитель – пользователь ИСПДн, администратор ИБ ИСПДн блокирует доступ в ИСПДн Администрации Октябрьского района города Ставрополя для нарушителя.

2.4.2. Последующие действия

Создается комиссия для расследования инцидента.

2.5. Установка закладочных устройств злоумышленником в текущий момент времени

В случае обнаружения злоумышленника, устанавливающего закладочные устройства, выполняются следующие действия.

2.5.1. Первоочередные действия

Администратор ИБ ИСПДн принимает меры к задержанию злоумышленника.

2.5.2. Последующие действия

Создается комиссия для расследования инцидента.

2.6. Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени

В случае обнаружения внешнего злоумышленника маскирующегося под зарегистрированного пользователя выполняются следующие действия.

2.6.1. Первоочередные действия

Администратор ИБ ИСПДн блокирует доступ к ИСПДн Администрации Октябрьского района города Ставрополя для злоумышленника.

2.6.2. Последующие действия

Создается комиссия для расследования инцидента.

2.7. Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени

В случае обнаружения использования дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени выполняются следующие действия.

2.7.1. Первоочередные действия

Администратор ИБ ИСПДн блокирует доступ из внешних сетей к оборудованию, на котором используется уязвимое ПО.

2.7.2. Последующие действия

Создается комиссия для расследования инцидента.

2.8. Использование программных закладок внешним нарушителем в текущий момент времени

В случае обнаружения использования программных закладок внешним нарушителем в текущий момент времени выполняются следующие действия.

2.8.1. Первоочередные действия

Администратор ИБ ИСПДн блокирует доступ из внешних сетей к оборудованию, на котором установлена программная закладка.

2.8.2. Последующие действия

1. Администратор ИБ ИСПДн определяет возможный ущерб, нанесенный программной закладкой.
2. Администратор ИБ ИСПДн проводит мероприятия по обнаружению внедренных программных закладок и их нейтрализации, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
3. Составляется акт об инциденте.

2.9. Обнаружение программных вирусов

В случае обнаружения программных вирусов выполняются действия предусмотренные Инструкцией по антивирусной защите.

2.10. Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником

В случае обнаружения злоумышленника нарушающего функционирование ТС обработки информации в текущий момент времени выполняются следующие действия.

2.10.1. Первоочередные действия

1. Администратор ИБ ИСПДн принимает меры по немедленному удалению злоумышленника от средств вычислительной техники.
2. В случае если злоумышленник является пользователем системы, Администратор ИБ ИСПДн блокирует доступ к ИСПДн Администрации Октябрьского района города Ставрополя для злоумышленника.

2.10.2. Последующие действия

1. В случае наличия повреждений Администратор ИБ ИСПДн определяет ущерб, нанесенный ТС и информации.
2. Администратор ИБ ИСПДн производит восстановление работоспособности системы.
3. Создается комиссия для расследования инцидента.

2.11. Обнаружение нарушения функционирования ТС обработки информации, произведенного злоумышленником

В случае обнаружения нарушений в функционировании ТС обработки информации, выполняются следующие действия.

1. Администратор ИБ ИСПДн определяет возможный круг лиц, причастных к нарушению функционирования ТС, определяет объем повреждений техническим и информационным ресурсам.
2. Администратор ИБ ИСПДн производит восстановление работоспособности системы.
3. Создается комиссия для расследования инцидента.

2.12. Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени

В случае обнаружения внешней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия.

2.12.1. Первоочередные действия

1. Администратор ИБ ИСПДн выявляет источник ложных заявок.
2. Администратор ИБ ИСПДн вырабатывает решение по блокированию потока ложных заявок и реализует выбранное решение.

2.12.2. Последующие действия

1. Администратор ИБ ИСПДн уведомляет провайдера, от которого идут ложные заявки, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
2. Администратор ИБ ИСПДн составляет акт об инциденте.

2.13. Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени

В случае обнаружения внутренней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия:

1. Администратор ИБ ИСПДн выявляет источник ложных заявок и блокирует доступ к ИСПДн администрации для злоумышленника.
2. Создается комиссия для расследования инцидента.

2.14. Блокировка доступа к защищаемой информации, произошедшая в прошлом

При обнаружении факта блокировки доступа к защищаемой информации, произошедшей в прошлом, выполняются следующие действия.

1. Администратор ИБ ИСПДн выявляет источник ложных заявок.
2. В случае если злоумышленник является внешним, администратор ИБ ИСПДн уведомляет провайдера, от которого идут ложные заявки. Планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
3. В случае если злоумышленник является внешним, администратор ИБ ИСПДн составляет акт об инциденте.
4. Создается комиссия для расследования инцидента.

2.15. Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации

В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации, выполняются следующие действия.

2.15.1. Первоочередные действия

1. Администратор ИБ ИСПДн проводит анализ и идентификацию причин инцидента.
2. В случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.
3. Администратор ИБ ИСПДн определяет ущерб, нанесенный нештатной ситуацией.

4. Администратор ИБ ИСПДн проводит мероприятия по восстановлению работоспособности системы и информации.

2.15.2. Последующие действия

1. Проводится проверка знаний сотрудника, виновного в инциденте, а в случае необходимости его обучение.
2. Администратор ИБ ИСПДн составляет акт об инциденте, в случае необходимости выносит предложение главе Администрации Октябрьского района города Ставрополя о применении дисциплинарной меры в отношении нарушителя.

2.16. Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО

В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО, выполняются следующие действия.

2.16.1. Первоочередные действия

1. Администратор ИБ ИСПДн проводит анализ и идентификацию причин инцидента.
2. В случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.

2.16.2. Последующие действия

1. Администратор ИБ ИСПДн определяет ущерб, нанесенный нештатной ситуацией, восстанавливают работоспособность системы.
2. Администратор ИБ ИСПДн составляет акт об инциденте, в случае необходимости выносит предложение главе Администрации Октябрьского района города Ставрополя о применении дисциплинарной меры в отношении нарушителя.
3. Проводится проверка знаний сотрудника виновного в инциденте, а в случае необходимости его обучение.

2.17. Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ

В случае возникновения дефектов, сбоев, отказов, аварий ТС и систем ОИ выполняются следующие действия.

2.17.1. Первоочередные действия

1. Администратор ИБ ИСПДн выявляют возможные причины проявления дестабилизирующих факторов.

2. В случае наличия злоумышленных действий выполняется порядок действий соответствующего раздела Инструкции.

2.17.2. Последующие действия

1. Администратор ИБ ИСПДн восстанавливает работоспособность систем.
2. В случае потери данных администратором ИБ ИСПДн по возможности проводится восстановление их из резервных копий.
3. Администратором ИБ ИСПДн производится составление акта.

2.18. Сбои, отказы и аварии систем обеспечения ОИ

В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем выполняется следующая последовательность действий.

1. В случае если наблюдается продолжительное отключение электропитания. Администратором ИБ ИСПДн производится отключение серверов до момента истечения резервов системы бесперебойного питания.
2. Ответственным за материально-техническое обеспечение организуются работы по максимально быстрому восстановлению систем обеспечения.
3. В случае потери защищаемых данных Администратором ИБ ИСПДн по возможности проводится восстановление их из резервных копий.
4. Ответственным за материально-техническое обеспечение производится составление акта.

2.19. Природные явления, стихийные бедствия, несущие угрозу жизни человека

В случае проявления стихийных бедствий и природных явлений, которые несут угрозу жизни человека, выполняются следующие действия:

1. Все сотрудники (руководители отделов в том числе) обязаны личные реквизиты защиты (например: металлические и/или электронные ключи, карты-идентификаторы, ключевые дискеты, печати и пр.) собрать и упаковать в водонепроницаемый пакет (непосредственный руководитель обеспечивает заранее) и лично обеспечивать сохранность этого пакета во время эвакуации.
2. По «Списку имущества и(или) документов в личном пользовании сотрудника, подлежащего эвакуации в первую очередь» (разрабатываются сотрудниками заранее и постоянно хранятся на

рабочем месте) произвести сбор, упаковку, опись (в двух экз. – 1 экз. в тару) документов и технических средств в водонепронецаемую тару (обеспечивает заранее непосредственный руководитель). Упакованное имущество сотрудник передает под роспись (на своем экз. описи) лицам, обеспечивающим доставку имущества на эвакопункт, иначе - лично сопровождает груз во время его транспортировки.

3. Сотрудник вкладывает в вышеназванный пакет картонную табличку с указанием текущей даты, своих персональных данных (ФИО, наименование организации, номер служебного телефона) и содержащую опись содержимого пакета, заверенную собственноручной подписью.

Руководители обязаны собрать в помещениях отделов и лично упаковать, (и далее лично хранить, как свои) реквизиты защиты и документы (согласно спискам первой очереди) тех сотрудников, которых на момент эвакуации нет на рабочем месте (болезнь, командировка, учеба, отпуск и т.д.).

Руководители обязаны:

- при подготовке к эвакуации проверить обеспеченность (а при отсутствии – обеспечить) сотрудников отделов и/или администраторов упаковочным материалом, списками документов, дел и имущества, подлежащих эвакуации в первую очередь;
- перед выездом в эвакопункт – проконтролировать исполнение задач эвакуации, приняв соответствующие доклады от сотрудников о готовности к эвакуации, провести выборочную проверку готовности (комплектности) документов, дел, имущества подразделения и/или ИСПДн к эвакуации.

2.20. Природные явления, стихийные бедствия, не несущие угрозу жизни человека

В случае проявления стихийных бедствий и природных явлений, которые не несут угрозу жизни и/или человека, выполняются следующие действия:

1. Сотрудники Администрации Октябрьского района города Ставрополя выключают свои персональные компьютеры.
2. Администратор ИБ ИСПДн выключает серверы и сетевое оборудование.
3. Администратор ИБ ИСПДн принимает меры к эвакуации резервных копий с информацией, системных блоков компьютеров, содержащих особо ценную информацию, документов и другого имущества. В первую очередь эвакуируется имущество по «Списку

имущества и(или) документов в личном пользовании сотрудника, подлежащего эвакуации в первую очередь».

4. В случае локальных пожаров и частичных затоплений Ответственным за материально-техническое обеспечение организуются работы по ликвидации нештатной ситуации и ее последствий.

3. ПРОВЕДЕНИЕ РАССЛЕДОВАНИЙ

Для расследования опасных ситуаций в случаях, предусмотренных настоящей Инструкцией может создаваться комиссия. В состав комиссии должны входить:

- председатель;
- ответственный за обеспечение безопасности ПДн;
- администратор ИБ ИСПДн;
- юрист;
- другие лица по решению председателя комиссии.

Деятельность комиссии должна по возможности происходить в режиме конфиденциальности.

В общем случае комиссия проводит:

- анализ и идентификацию причин инцидента, определение виновных;
- определение ущерба, нанесенного нештатной ситуацией;
- планирование мер для предотвращения повторения, нейтрализации последствий (если это возможно);
- анализ и сохранение доказательств, следов инцидента, улик и свидетельств;
- определение меры взыскания с виновного;
- взаимодействие, при необходимости с правоохранительными органами.

При сохранении улик, если есть возможность, Администратором ИБ ИСПДн производится резервное копирование системной и защищаемой информации технических средств, вовлеченных в инцидент, включая логи (контрольные записи).

По результатам деятельности комиссии составляется акт с описанием ситуации. К акту прилагаются поясняющие материалы (копии экрана, распечатки журнала событий, и др.).

По результатам расследования администраторами организуются мероприятия по реализации предложенных комиссией мер для предотвращения либо уменьшения вероятности проявления, подобных инцидентов в дальнейшем.

При проведении расследований, кроме того, необходимо ответить на следующие вопросы:

- можно ли было предупредить нештатную ситуацию?
- вызвана ли она слабостью средств защиты и регистрации?
- это первая кризисная ситуация такого рода?
- достаточно ли имеющегося резерва?
- есть ли необходимость пересмотра системы защиты?
- есть ли необходимость пересмотра настоящей инструкции?

4. ОТВЕТСТВЕННЫЕ ЗА КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственными за постоянный контроль выполнения требований данной Инструкции являются:

- администратор ИБ ИСПДн в части задач, возложенных на него настоящей инструкцией;
- ответственный за обеспечение безопасности ПДн в части общего контроля информационной безопасности;
- ответственный за материально-техническое обеспечение, в части задач, возложенных на него настоящей инструкцией.

5. ПОРЯДОК ЗАМЕЩЕНИЯ ОТВЕТСТВЕННЫХ ЛИЦ

В случае отсутствия кого-либо из ответственных лиц при нештатной ситуации (отпуск, болезнь и т.п.) производится их замещение в соответствии с последовательностями определенными ниже. Ответственное лицо замещает следующий идущий по списку сотрудник.

Ответственные за информационную безопасность и ИСПДн

1. Администратор ИБ ИСПДн.
2. Ответственный за обеспечение безопасности ПДн.
3. Заместитель главы Администрации Октябрьского района города Ставрополя, глава Администрации Октябрьского района города Ставрополя.

Ответственные за материально-техническое обеспечение

1. Руководитель общего отдела.

2. Заместитель главы Администрации Октябрьского района города Ставрополя.
3. Глава Администрации Октябрьского района города Ставрополя.

6. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

Инструкция подлежит полному пересмотру при изменении приоритетов угроз безопасности ИСПДн Администрации Октябрьского района города Ставрополя, кроме того, полный плановый пересмотр данного документа проводится регулярно, не реже одного раза в год, с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн Администрации Октябрьского района города Ставрополя.

Инструкция подлежит частичному пересмотру в следующих случаях:

- при изменении местоположения, состава и объема информационных ресурсов, подлежащих резервному копированию;
- при определении такой необходимости комиссией по результатам расследования нештатной ситуации;
- в целях повышения эффективности мероприятий определенных в настоящей инструкции;
- при изменении состава, обязанностей и полномочий должностных лиц Администрации Октябрьского района города Ставрополя, которые задействованы в мероприятиях настоящей Инструкции.

Полный пересмотр данного документа проводится администратором ИБ ИСПДн, ответственным за обеспечение безопасности ПДн Администрации Октябрьского района города Ставрополя с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн Администрации Октябрьского района города Ставрополя.

Частичный пересмотр данного документа проводится администратором ИБ ИСПДн. Частичный пересмотр должен проводиться регулярно, не реже одного раза в полгода. При этом могут быть добавлены, удалены или изменены приложения Инструкции с обязательным указанием оснований и внесенных изменений в «Листе регистрации изменений в Инструкции» (Приложение 4) без переутверждения всей Инструкции.

ПРИЛОЖЕНИЕ 1. СРЕДСТВА ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ

Резервному копированию (РК) подлежит следующая информация:

- системные программы и наборы данных - *невозобновляемому (однократному, эталонному) РК*;
- прикладное программное обеспечение и наборы данных - *невозобновляемому РК*;
- наборы данных, генерируемые в течение рабочего дня и содержащие ценную информацию (журналы транзакций, системный журнал и т.д.) - *периодическому возобновляемому РК*.

Резервному копированию в ИСПДн подлежат следующие программные и информационные ресурсы:

Наименование информационного ресурса	**Где размещается ресурс в системе**	**Вид резервного копирования**	**Ответственный за резервное копирование (используемые технические средства)**	**Где хранится резервная копия**	**Частота периодического резервирования**
Информация ИСПДн		Периодическое, возобновляемое	Администратор ИБ ИСПДн		Каждую пятницу
Эталонное программное обеспечение		Невозобновляемое	Администратор ИБ ИСПДн		Обновляется при появлении нового ПО

ПРИЛОЖЕНИЕ 2. ПЛАН ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
Неправомерные действия со стороны лиц допущенных к защищаемой информации					
Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Обнаружение несанкционированно скопированной или измененной конфиденциальной информации		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Несанкционированный доступ к информации					
Обнаружение подключения технических средств к средствам и системам объекта информатизации		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Подключение технических средств к средствам и системам ОИ в текущий момент времени		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Обнаружение закладочных устройств		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

[1] В случае отсутствия лиц, которые должны оповещаться, их замещают лица, определенные в разделе «Порядок замещения ответственных лиц» настоящей Инструкции. Либо могут быть оповещены непосредственные руководители

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1]и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
Установка закладочных устройств злоумышленником в текущий момент времени		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн сразу после обнаружения инцидента	5 минут в рабочее время (1 час в нерабочее)	
Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Использование программных закладок внешним нарушителем в текущий момент времени		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Использование программных закладок внутренним злоумышленником или обнаружение факта использования		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Обнаружение программных вирусов		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента		12 часов

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1]и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
Хищение носителя защищаемой информации		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Нарушена работа одного пользователя	Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня
	Нарушена работа группы пользователей	Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником	Нарушена работа одного пользователя	Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн сразу после обнаружения инцидента		2 дня
	Нарушена работа группы пользователей	Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн сразу после обнаружения инцидента		1 день
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку					
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	7 дней

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день
Обнаружение произошедшего факта блокировки доступа к защищаемой информации		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента		1 день
Ошибки пользователей системы					
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации		Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента	2 часа в рабочее время (12 часов в нерабочее)	1 день
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО	Нарушена работа одного пользователя	Администратору ИБ ИСПДн сразу после инцидента	Администратору ИБ ИСПДн в первый рабочий день после инцидента	20 минут	2 дня
	Нарушена работа группы пользователей	Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн сразу после обнаружения инцидента	20 минут	1 день
Объективные факторы					
Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ	Сбой ТС и систем ОИ	Администратору ИБ ИСПДн сразу после инцидента	Администратору ИБ ИСПДн сразу после инцидента	1 час	2 дня

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
	Отказ ТС и систем ОИ, затронувший работу группы пользователей	Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час в рабочее время (8 часов в нерабочее)	1 день
	Отказ ТС и систем ОИ, затронувший работу одного пользователя	Администратору ИБ ИСПДн сразу после инцидента	Администратору ИБ ИСПДн в первый рабочий день после инцидента	1 час	2 дня
	Авария ТС и систем ОИ	Администратору ИБ ИСПДн сразу после обнаружения инцидента	Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час	1 день
Сбои, отказы и аварии систем обеспечения ОИ	Сбой систем обеспечения ОИ	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента		
	Отказ систем обеспечения ОИ, затронувший работу группы пользователей	Ответственному за материально-техническое обеспечение и Администратору ИБ ИСПДн сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение и Администратору ИБ ИСПДн сразу после обнаружения инцидента		1 день
	Отказ систем обеспечения ОИ, затронувший работу одного пользователя	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента		2 дня

Тип кризисной ситуации	Критерии кризисной ситуации	Кому [1] и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
	Авария систем обеспечения ОИ	Ответственному за материально-техническое обеспечение, Администратору ИБ ИСПДн сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение, Администратору ИБ ИСПДн как можно скорее, в дневное время, но не позднее 8 часов после инцидента		1 день
Природные явления, стихийные бедствия, несущие угрозу жизни человека		Руководителю, заместителям Руководителю, которые оповещают всех своих сотрудников сразу после получения информации	Руководителю, заместителям Руководителю, которые оповещают всех своих сотрудников сразу после получения информации		30 минут
Природные явления, стихийные бедствия, не несущие угрозу жизни человека		Руководителю, заместителям Руководителю, Администратору ИБ ИСПДн	Руководителю, заместителям Руководителю, Администратору ИБ ИСПДн		30 минут

ПРИЛОЖЕНИЕ 3. ЖУРНАЛ УЧЕТА НЕШТАТНЫХ СИТУАЦИЙ

ЖУРНАЛ

учета нештатных ситуаций

№ п/п	Дата, ИСПДн, ПЭВМ, описание ситуации, выполненные работы	Подпись исполнителя	Подпись администратора

ПРИЛОЖЕНИЕ 4. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

ЛИСТ
регистрации изменений в Инструкции

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Приложение № 11
к приказу руководителя Администрации
Октябрьского района города Ставрополя

от «11» 08 2017 г. № 171

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРЦИИ ОКТЯБРЬСКОГО РАЙОНА ГОРОДА СТАВРОПОЛЯ

г. Ставрополь
2017 г.

СПИСОК СОКРАЩЕНИЙ

ИСПДн	Информационная система персональных данных
ИБ	Информационная безопасность
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭВМ	Персональная электронная вычислительная машина
САЗ	Система антивирусной защиты
СВТ	Средства вычислительной техники

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция по организации антивирусной защиты информационных систем персональных данных администрации Октябрьского района города Ставрополя определяет требования к организации защиты информационных систем персональных данных (далее ИСПДн) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (ПО) и устанавливает ответственность руководителей и сотрудников отделов администрации Октябрьского района города Ставрополя, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников отделов Администрации, использующих в работе ИСПДн администрации Октябрьского района города Ставрополя.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов, проводятся организуемые Администратором безопасности ИСПДн семинары и персональные инструктажи (при необходимости) пользователей ИСПДн администрации Октябрьского района города Ставрополя.

1.4. Доведение Инструкции до сотрудников администрации Октябрьского района города Ставрополя в части их касающейся осуществляется Администратором безопасности ИСПДн под роспись в журнале или на самом документе.

1.5. В случае невозможности исполнения требований настоящей Инструкции в полном объеме, например:

- в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний;
- злоумышленных действий,

практическая «глубина» исполнения настоящей Инструкции определяется Администратором безопасности ИСПДн по согласованию с ответственным за обеспечение безопасности ПДн Администрации Октябрьского района города Ставрополя.

2. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

2.1. Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

2.2. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование).

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

2.4. Установка (обновление и изменение) системного и прикладного программного обеспечения осуществляется в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн Администрации Октябрьского района города Ставрополя».

2.5. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

3. ФУНКЦИИ АДМИНИСТРАТОРА ИСПДН ПО ОБЕСПЕЧЕНИЮ АНТИВИРУСНОЙ БЕЗОПАСНОСТИ

Администратор безопасности ИСПДн обязан:

3.1. При необходимости проводить инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты.

3.2. Настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.

3.3. Предварительно проверять устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов.

3.4. При необходимости производить обновление антивирусных программных средств.

3.5. Производить получение и рассылку (при необходимости) обновлений антивирусных баз.

3.6. При необходимости разрабатывать инструкции по работе пользователей с программными средствами САЗ.

3.7. Проводить работы по обнаружению и обезвреживанию вирусов.

3.8. Участвовать в работе комиссии по расследованию причин заражения ПЭВМ и серверов.

3.9. Хранить эталонные копии антивирусных программных средств.

3.10. Осуществлять периодический контроль за соблюдением пользователями ПЭВМ требований настоящей Инструкции;

3.11. Разрабатывать инструкции по работе пользователей с системой антивирусной защиты информации.

3.12. Проводить периодический контроль работы программных средств системы антивирусной защиты информации на ПЭВМ (серверах).

4. ФУНКЦИИ ПОЛЬЗОВАТЕЛЕЙ

Пользователи ИСПДн:

4.1. Получают по ЛВС или от Администратора безопасности ИСПДн носители с обновлениями антивирусных баз (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.2. Проводят обновления антивирусных баз на ПЭВМ (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с администратором безопасности ИСПДн должен провести внеочередной антивирусный контроль ПЭВМ. При необходимости он должен привлечь Администратора безопасности ИСПДн для определения факта наличия или отсутствия компьютерного вируса.

4.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя отдела администрации Октябрьского района города Ставрополя и Администратора безопасности ИСПДн, а также смежные отделы, использующие эти файлы в работе;
- провести анализ необходимости дальнейшего использования зараженных вирусом файлов;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь Администратора безопасности ИСПДн);
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе Администратору безопасности ИСПДн для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;
- по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору безопасности ИСПДн, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

5. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

5.1. Инструкция подлежит полному пересмотру в случае приобретения администрацией Октябрьского района города Ставрополя новых средств защиты, существенно изменяющих порядок работы с ними.

5.2. В остальных случаях Инструкция подлежит частичному пересмотру.

5.3. Полный пересмотр данной Инструкции проводится с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн администрации Октябрьского района города Ставрополя.

5.4. Изменения в Инструкции (сведения о них) фиксируется в листе регистрации изменений (Приложение 2).

5.5. Вносимые изменения не должны противоречить другим положениям Инструкции. При получении изменений к данному Инструкции, руководители отделов администрации Октябрьского района города Ставрополя в течение трех рабочих дней вносят свои предложения и/или замечания к поступившим изменениям.

6. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

6.1. Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников администрации Октябрьского района города Ставрополя.

6.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам антивирусной защиты возлагается на Администратора безопасности ИСПДн.

6.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности ПДн администрации Октябрьского района города Ставрополя.

ПРИЛОЖЕНИЕ 1 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

ЛИСТ № _____ регистрации изменений в Инструкции

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Приложение № 12
к приказу главы администрации
Октябрьского района города Ставрополя

от «11» 08 2017 г. № 171

ИНСТРУКЦИЯ

ПО РЕЗЕРВНОМУ КОПИРОВАНИЮ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ ОКТЯБРЬСКОГО РАЙОНА ГОРОДА СТАВРОПОЛЯ

г. Ставрополь
2017 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ определяет порядок осуществления резервного копирования информационных ресурсов информационных систем персональных данных (ИСПДн) администрации Октябрьского района города Ставрополя (далее – Администрация).

Процесс резервного копирования обеспечивает сохранение на резервных носителях информации, с целью ее восстановления при потере или порче на основном носителе, и является ключевым элементом защиты от умышленной и неумышленной потери данных.

Регламент составляется администратором информационной безопасности (ИБ) ИСПДн Администрации в соответствии с положениями данной Инструкции.

Регламент должен содержать перечень информационных ресурсов, подлежащих резервному копированию, и график осуществления резервного копирования, составленный с учетом требований руководителей отделов Администрации и администратора ИБ ИСПДн.

Форма Регламента представлена в Приложении 1.

Резервное копирование осуществляется администратором ИБ ИСПДн и контролируется ответственным за обеспечение безопасности персональных данных (ПДн) Администрации.

Должностные лица Администрации, задействованные в осуществлении резервного копирования информационных ресурсов ИСПДн Администрации, знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

2. ПЕРИОДИЧНОСТЬ И СХЕМА РЕЗЕРВНОГО КОПИРОВАНИЯ

При осуществлении резервного копирования используется два типа копирования: полное резервное копирование и инкрементальное резервное копирование.

Резервное копирование информационных ресурсов ИСПДн Администрации осуществляется по трехуровневой схеме ротации.

В соответствии с трехуровневой схемой ротации:

- полное резервное копирование информационных ресурсов выполняется 15-16 числа каждого месяца (архив хранится в течение года и является архивом Уровня 1);
- полное резервное копирование информационных ресурсов выполняется в конце каждой недели (в пятницу) (архив хранится в течение календарного месяца и является архивом Уровня 2);
- полное резервное копирование информационных ресурсов выполняется в начале каждой недели, затем ежедневно на эту

копию выполняется инкрементальное копирование (архив хранится в течение недели и является архивом Уровня 3).

3. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ

Администратор ИБ ИСПДн настраивает задания для ПО, осуществляющего резервное копирование, на автоматическое выполнение в соответствии с перечнем информационных ресурсов подлежащих резервному копированию и графиком резервного копирования.

Перед выполнением задания резервного копирования администратор ИБ ИСПДн проверяет доступность резервного носителя, а также наличие на нем свободного места для записи данных.

После завершения выполнения задачи резервного копирования администратор ИБ ИСПДн должен извлечь резервный носитель, подписать его по формату «число, месяц, год, уровень №» и поместить в сейф.

4. ХРАНЕНИЕ РЕЗЕРВНЫХ КОПИЙ

Хранение резервных копий должно быть организовано в отдельном от копируемых информационных ресурсов помещении, оснащенном соответствующими системами вентиляции, кондиционирования и отопления для поддержки требуемых параметров температуры, влажности и т.п.

Резервные носители должны храниться в кассетах или закрытых коробках на безопасном расстоянии от источников магнитных полей: блоков питания, телефонов, мониторов и т.п.

Доступ к хранилищу резервных копий должны иметь только администратор ИБ ИСПДн и ответственный за обеспечение безопасности ПДн.

5. ВОССТАНОВЛЕНИЕ ПОСЛЕ СБОЯ

В случае потери данных на основном носителе из хранилища извлекается накопитель с резервной копией информационных ресурсов, нуждающихся в восстановлении, от последнего произведенного резервного копирования.

В зависимости от характера и уровня повреждения информационных ресурсов, администратор ИБ ИСПДн восстанавливает либо весь массив резервных данных, либо отдельные поврежденные или уничтоженные файлы и папки.

6. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн Администрации, приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности ПДн Администрации.

Полный плановый пересмотр данного документа также проводится регулярно, раз в год, с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн Администрации.

Частичный пересмотр данного документа проводится по письменному предложению администратора ИБ ИСПДн. Форма регистрации изменений в Инструкции представлена в Приложении 2.

Вносимые изменения не должны противоречить другим положениям Инструкции.

7. ОТВЕТСТВЕННЫЕ ЗА ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственность за выполнение резервного копирования и восстановление данных из резервных копий, а также за соблюдение периодичности и порядка выполнения резервного копирования возлагается на администратора ИБ ИСПДн.

Ответственность за сохранность резервных копий возлагается на ответственного за обеспечение безопасности ПДн Администрации.

Ответственным за постоянный контроль выполнения требований данной Инструкции является ответственный за обеспечение безопасности ПДн Администрации.

ПРИЛОЖЕНИЕ 1 ФОРМА РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В ИНСТРУКЦИИ

ЛИСТ
регистрации изменений в Инструкции

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Лист ознакомления с «Инструкцией по резервному копированию защищаемой информации в информационных системах персональных данных Администрации»

№ п/п	Фамилия, инициалы сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении

Приложение №13
к приказу руководителя Администрации
Октябрьского района города Ставрополя

от «16» 08 2017 г. № 171

ИНСТРУКЦИЯ
ПО УСТАНОВКЕ, МОДИФИКАЦИИ И ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И АППАРАТНЫХ СРЕДСТВ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ ОКТЯБРЬСКОГО РАЙОНА ГОРОДА СТАВРОПОЛЯ

г. Ставрополь
2017 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных (ИСПДн) Администрации Октябрьского района города Ставрополя, включает в себя описание комплекса организационно-технических мер по проведению работ по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн.

Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников отделов Администрации Октябрьского района города Ставрополя, использующих в работе ИСПДн, в которых осуществляется обработка информации ограниченного доступа, не составляющей государственной тайны.

Должностные лица Администрации Октябрьского района города Ставрополя, задействованные в обеспечении функционирования ИСПДн Администрации Октябрьского района города Ставрополя, знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

Ознакомление с требованиями Инструкции пользователей ИСПДн осуществляет администратор информационной безопасности (ИБ) ИСПДн под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

Непосредственное исполнение настоящей Инструкции определяется администратором (ИБ) ИСПДн по согласованию с ответственным за обеспечение безопасности персональных данных (ПДн) администрации Октябрьского района города Ставрополя.

2. ПОРЯДОК ПРОВЕДЕНИЯ РАБОТ

Все изменения конфигурации технических и программных средств рабочих станций администрации Октябрьского района города Ставрополя должны производиться только на основании заявок руководителей отделов Комитета (Приложение 1), согласованных с главой администрации Октябрьского района города Ставрополя. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя отдела администрации Октябрьского района города Ставрополя.

При этом необходимо уведомить об осуществленных изменениях организацию, производившую аттестацию, которая принимает решение о необходимости проведения контроля эффективности аттестованного объекта информатизации.

Все изменения конфигурации технических и программных средств рабочих станций и серверов, входящих в состав аттестованных по

требованиям безопасности ИСПДн администрации Октябрьского района города Ставрополя, отражаются в Техническом паспорте объекта информатизации. ЗАПРЕЩАЕТСЯ изменение состава (в том числе ввод новых) программных средств, осуществляющих обработку ПДн на объектах информатизации, аттестованных по требованиям безопасности информации.

В заявке указываются наименование персональной электронной вычислительной машины (ПЭВМ) и ответственный за нее сотрудник. После чего заявка передается администратору ИБ ИСПДн для исполнения работ по внесению изменений в конфигурацию ПЭВМ ИСПДн администрации Октябрьского района города Ставрополя.

Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций ИСПДн администрации Октябрьского района города Ставрополя предоставляется администратору ИБ ИСПДн, а также ответственному за обеспечение безопасности ПДн. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме администратора ИБ ИСПДн и/или ответственного за обеспечение безопасности ПДн, ЗАПРЕЩЕНО.

Установка и настройка программного средства осуществляется администратором ИБ ИСПДн согласно эксплуатационной документации.

Запрещается установка и использование на ПЭВМ (серверах) программного обеспечения (ПО), не входящего в перечень программного обеспечения, разрешенного к использованию в Комитете.

Руководители отделов администрации Октябрьского района города Ставрополя совместно с администратором ИБ ИСПДн осуществляют контроль за отсутствием на ПЭВМ сотрудников отделов программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

Установка (обновление) ПО (системного, тестового и т.п.) на рабочих станциях и серверах производится с эталонных копий программных средств, хранящихся у администратора ИСПДн. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода в соответствии с «Инструкцией по организации антивирусной защиты ИСПДн Комитета».

После установки (обновления) ПО администратор ИБ ИСПДн должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями к системе защиты информации и, совместно с пользователем ПЭВМ, проверить правильность настройки средств защиты.

В случае обнаружения недекларированных (не описанных в документации) возможностей программного средства, сотрудники немедленно докладывают руководителю своего подразделения и администратору ИБ ИСПДн. Использование программного средства до получения специальных указаний ЗАПРЕЩАЕТСЯ.

После завершения работ по внесению изменений в состав аппаратных средств защищенных ПЭВМ системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) администратором ИБ ИСПДн.

При изъятии ПЭВМ из состава рабочих станций, обрабатывающих информацию ограниченного распространения (защищаемая информация), ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как администратор ИБ ИСПДн снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для затирания (уничтожения) защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора ИСПДн. Форма Акта приведена в Приложении 2.

Допуск новых пользователей к решению задач с использованием вновь развернутого ПО (либо изменение их полномочий доступа) осуществляется согласно «Инструкции по внесению изменений в списки пользователей системы и наделению пользователей полномочиями доступа к ресурсам ИСПДн администрации Октябрьского района города Ставрополя».

Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств ПЭВМ с отметками о внесении изменений в состав аппаратно-программных средств должны храниться у администратора ИБ ИСПДн.

3. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн администрации Октябрьского района города Ставрополя, приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности ПДн администрации Октябрьского района города Ставрополя.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности ПДн администрации с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн администрации Октябрьского района города Ставрополя.

Форма регистрации изменений в Инструкции представлена в Приложении 3.

Вносимые изменения не должны противоречить другим положениям Инструкции.

4. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников администрации Октябрьского района города Ставрополя.

Ответственность за организацию контрольных и проверочных мероприятий по вопросам установки, модификации технических и программных средств возлагается на администратора ИБ ИСПДн.

Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности ПДн администрации Октябрьского района города Ставрополя.

ПРИЛОЖЕНИЕ 1. ЗАЯВКА НА ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Главе администрации
Октябрьского района
города Ставрополя

(резолюция)

ЗАЯВКА

на внесение изменений в состав *программного (аппаратного)* обеспечения

(ненужное зачеркнуть)

_____

(Наименование ПЭВМ)

Прошу дать указания ответственным сотрудникам для организации *установки (изменения настроек)*

(ненужное зачеркнуть)

_____

_____

(перечень ПО (аппаратных средств) и необходимых настроек)

для решения задач:

_____

_____

_____

_____

следующим пользователям:

_____

_____

_____

(фамилия, имя, отчество)

Руководитель отдела _____

(наименование структурного подразделения)

«___» _____ 201__ г. _____ _____

(подпись) (Фамилия, инициалы)

Оборотная сторона заявки

Изменения на ПЭВМ ИСПДн *произведены (не произведены)* по следующей причине:
(ненужное зачеркнуть)

Выполнены следующие работы:

Выполнены следующие изменения в настройках средств защиты:

Администратор ИБ ИСПДн

«___» _____ 201__ г. _____ _____
(подпись) (фамилия, инициалы)

ПРИЛОЖЕНИЕ 2. АКТ ЗАТИРАНИЯ ИНФОРМАЦИИ

АКТ
о затирании остаточной информации, хранившейся на диске компьютера

Все файлы, содержащие подлежащую защите информацию, находившиеся на НЖМД

_____,
(модель, серийный номер)

передаваемого

_____
(с какой целью)

_____
(кому: должность, Ф.И.О.)

ПЭВМ:

_____
(наименование ПЭВМ)

уничтожены (затерты) посредством программы _____.

Администратор ИБ ИСПДн

«___» _____ 201__ г. _____ _____
(подпись) (фамилия, инициалы)

ПРИЛОЖЕНИЕ 3. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В ИНСТРУКЦИИ

ЛИСТ
регистрации изменений в Инструкции

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Приложение №14
к приказу главы администрации
Октябрьского района города Ставрополя
от «11» 08 2017 г. №174

Р Е Г Л А М Е Н Т
УЧЕТА СРЕДСТВ ЗАЩИТЫ, ДОКУМЕНТАЦИИ И ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ ОКТЯБРЬСКОГО РАЙОНА ГОРОДА СТАВРОПОЛЯ

г. Ставрополь
2017 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Регламент учета средств защиты, документации и электронных носителей персональных данных (далее – Регламент) устанавливает:

- порядок учета, ввода в эксплуатацию и изъятия из употребления средств, используемых для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) администрации Октябрьского района города Ставрополя;
- порядок приема, учета, обработки и хранения документов Администрации, содержащих персональные данные;
- порядок учета и хранения электронных носителей информации администрации Октябрьского района города Ставрополя, содержащих персональные данные (далее носители с ПДн).

Требования Регламента распространяются на всех должностных лиц и сотрудников отделов администрации Октябрьского района города Ставрополя, работающих в ИСПДн Администрации.

Ознакомление с требованиями Регламента администраторов информационной безопасности (ИБ) ИСПДн осуществляет ответственный за обеспечение безопасности персональных данных (ПДн) под роспись с выдачей электронных копий соответствующих приложений и разделов Регламента непосредственно для повседневного использования в работе.

Ознакомление с требованиями Регламента руководителей отделов, работающих с ИСПДн, осуществляет администратор ИБ ИСПДн под роспись с выдачей электронных копий соответствующих приложений и разделов Регламента непосредственно для повседневного использования в работе.

Ознакомление сотрудников отделов, работающих с ИСПДн, с требованиями Регламента проводят руководители этих отделов под роспись с выдачей электронных копий Регламента непосредственно для повседневного использования в работе.

2. ПОРЯДОК УЧЕТА И ХРАНЕНИЯ СРЕДСТВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Используемые или хранимые средства защиты персональных данных, эксплуатационная и техническая документация к ним подлежат поэкземплярному учету. Рекомендуемые формы приведены в Приложении № 1. При этом программные средства защиты персональных данных должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные средства защиты персональных данных

подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие средства защиты персональных данных учитываются также совместно с соответствующими аппаратными средствами.

Все полученные экземпляры средств защиты персональных данных, эксплуатационной и технической документации к ним должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям средств защиты персональных данных, несущим персональную ответственность за их сохранность.

Эксплуатационная и техническая документация, а также электронные носители с инсталляционными файлами средств защиты персональных данных должны содержаться в хранилищах (шкафах, ящиках, сейфах и др.), исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Аппаратные средства, с которыми осуществляется штатное функционирование средств защиты персональных данных, должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) должно быть таким, чтобы его можно было визуально контролировать.

Средства защиты персональных данных изымаются из употребления по решению ответственного за обеспечение безопасности персональных данных администрации Октябрьского района города Ставрополя. При этом вносятся необходимые изменения в «Журнал поэкземплярного учета средств защиты персональных данных, эксплуатационной и технической документации к ним», Технический паспорт ИСПДн, в составе которой эксплуатировались изъятые из употребления средства защиты персональных данных. Если эксплуатация средств защиты персональных данных, намеченных к изъятию из употребления, происходит в составе аттестованной ИСПДн, о прекращении эксплуатации средств защиты персональных данных необходимо уведомить организацию, производившую аттестацию данной ИСПДн. При этом средства защиты персональных данных считаются изъятыми из употребления, если исполнена предусмотренная эксплуатационной и технической документацией процедура удаления программного обеспечения средств защиты персональных данных и они полностью отсоединены от аппаратных средств.

3. ПОРЯДОК УЧЕТА ДОКУМЕНТАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Организация обработки всей поступивших и создаваемых документов, содержащих сведения, отнесенные Перечнем персональных данных к защищаемым в администрации Октябрьского района города Ставрополя,

(далее – Документов) осуществляется специально назначенным доверенным сотрудником (сотрудниками), имеющими опыт работы в сфере документооборота (далее – Референт).

Регистрация Документов – фиксация факта создания или поступления документа путем проставления на нем индекса с последующей записью необходимых сведений о Документе в регистрационных формах. Индекс Документа состоит из порядкового номера в пределах регистрируемого массива документов, который, исходя из задач поиска, дополняется индексами по номенклатуре дел, классификатором корреспондентов, исполнителей. В индексе Документа соблюдается следующая последовательность его составных частей: порядковый регистрационный номер, индекс по номенклатуре дел, индекс по используемому классификатору. Составные части индекса отделяются друг от друга косой чертой.

Регистрации подлежат все Документы, требующие учета, исполнения и использования в справочных целях, как создаваемые и используемые внутри администрации Октябрьского района города Ставрополя, так и направляемые в другие организации и поступающие из вышестоящих, подведомственных и других организаций и частных лиц.

Содержание создаваемой документации сравнивается с Перечнем персональных данных администрации Октябрьского района города Ставрополя. Если содержание создаваемой документации соответствует хотя бы одной из позиций Перечня, данная документация передается Референту, который вносит её в журнал учета документации, содержащей персональные данные. На учтенном в журнале Документе проставляется порядковый учетный номер с указанием количества листов основного документа и приложений.

При приеме корреспонденции Референт проверяет правильность адресования конверта, пакета, целостность упаковки. В разносной книге, реестре курьёра, почтальона референт проставляет отметку о приеме корреспонденции, дату приема, роспись в приеме. При повреждении упаковки корреспонденции Референт составляет акт, который подписывается им и курьером, почтальоном. Один экземпляр акта вместе с курьером передается отправителю корреспонденции.

Все поступившая в фирму документация, в том числе факсимильная, сравнивается с Перечнем персональных данных Администрации. Если содержание поступившей документации соответствует одной из позиций Перечня, выделенная документация вносится в журнал учета документации, содержащей персональные данные, с целью создания информационной базы, обеспечивающей контроль за сохранностью Документов.

Поступающие и создаваемые Документы вносятся Референтом в журнал учета документации, содержащей персональные данные. Журнал включает следующие графы:

- порядковый учетный номер;
- дата;
- вид документа и заголовок;
- количество экземпляров;
- количество листов основного документа и приложений;
- откуда поступил (кем подготовлен);
- исходящий номер; кому передан и роспись;
- кто принял и роспись;
- местонахождение;
- дата уничтожения и номер акта;
- местонахождение.

На всех поступивших Документах на первом листе проставляется регистрационный (входящий) штамп с указанием наименования фирмы, даты поступления документа, количества листов основного документа и приложений и наличием свободной зоны для входящего номера. На первом листе каждого приложения в правом верхнем углу проставляется штамп с указанием даты поступления, количества листов данного приложения и наличием свободной зоны для внесения входящего номера.

Отправка Документов допускается в исключительных случаях с личного письменного разрешения ответственного за обеспечение безопасности ПДн. Отправка возможна только при наличии письменного договора с корреспондентом о сохранении в конфиденциальности ПДн Администрации. Пересылка Документов осуществляется только в законвертованном виде. Отправку Документов корреспондентам осуществляет Референт.

Уничтожение Документов осуществляется назначаемой приказом комиссией. Отобранные для уничтожения Документы вносятся в акт о выделении к уничтожению конфиденциальных дел и документов, сверяются с учетными формами и уничтожаются путем сжигания.

Акт уничтожения конфиденциальных документов содержит следующие основные графы:

- индекс документа;
- заголовок;
- год документа;
- количество листов;
- срок хранения и номера статей по Перечню персональных данных.

После фактического уничтожения документов соответствующие отметки комиссия делает в акте и журнале учета документации, содержащей персональные данные. Отметки заверяются подписями членов комиссии.

4. ПОРЯДОК УЧЕТА НОСИТЕЛЕЙ

В отделах администрации Октябрьского района города Ставрополя, работающих с ИСПДн, учет носителей с ПДн осуществляется специально назначенными из числа сотрудников отдела лицами (далее – делопроизводителями).

При смене делопроизводителя, составляется акт приема-сдачи носителей с ПДн и всех журналов учета, который утверждается ответственным за обеспечение безопасности персональных данных.

После записи ПДн на носитель, сотрудник, выполнивший запись информации, передает его делопроизводителю для учета.

При получении носителей с ПДн из сторонних организаций они передаются делопроизводителю отдела, являющегося адресатом информации для их учета, после чего могут быть выданы исполнителям для работы.

Ответственным за учет носителя с ПДн является сотрудник, первым записавший ПДн на носитель.

На носителях персональных данных проставляются следующие реквизиты:

- регистрационный номер;
- дата и роспись делопроизводителя.

Учет носителей производится в «Журнале учета носителей информации, содержащих персональные данные».

Движение (выдача и возврат) носителей с ПДн должно отражаться в соответствующем «Журнале учета выдачи и возврата носителей информации, содержащих персональные данные». Выдача носителей, дел сотруднику производится под его личную роспись.

Передача носителей с ПДн другим сотрудникам, имеющим допуск к ним, производится только через делопроизводителя с обязательной записью в «Журнале учета выдачи и возврата носителей информации, содержащих персональные данные».

Листы журналов нумеруются, прошиваются и опечатываются.

5. ПОРЯДОК ХРАНЕНИЯ НОСИТЕЛЕЙ

Документы, дела, издания и другие носители информации с ПДн должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (хранилищах). При этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность.

Запрещается выносить носители с ПДн из служебных помещений для работы с ними на дому, в гостиницах и т.д. В необходимых случаях ответственный за обеспечение безопасности ПДн может разрешить исполнителям вынос из администрации Октябрьского района города Ставрополя носителей с ПДн для их согласования, подписи и т.п.

Сотрудники должны после окончания работы запирать полученные носители с ПДн в личный сейф, а в случае его отсутствия сдавать делопроизводителю.

Проверка наличия носителей информации проводится один раз в год комиссией, назначаемой руководителем Комитета. Результаты проверки оформляются актом.

Проверка наличия носителей ПДн при необходимости может проводиться Администратором ИБ ИСПДн и ответственным за обеспечение безопасности ПДн, а также делопроизводителем.

Раз в год постоянно действующая экспертная комиссия производит ревизию носителей с ПДн и определяет перечень носителей информации, которые можно уничтожить.

Уничтожение ПДн на машинных носителей, утратившей свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

6. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн Администрации, приводящих к существенным изменениям технологии обработки ПДн.

Полный пересмотр данного документа проводится ответственным за безопасность с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн Администрации.

Частичный пересмотр данного документа проводится в остальных случаях. При этом могут быть добавлены, удалены или изменены приложения Регламента с обязательным указанием оснований и внесенных изменений в «Листе регистрации изменений в Регламенте» (Приложение 1) без переутверждения всего Регламента. Частичный пересмотр проводится ответственным за обеспечение безопасности ПДн администрации Октябрьского района города Ставрополя.

Вносимые изменения не должны противоречить другим положениям Регламента.

7. ОТВЕТСТВЕННЫЕ ЗА ВЫПОЛНЕНИЕ РЕГЛАМЕНТА

На пользователей ИСПДн, Референта, делопроизводителей возлагается персональная ответственность за выполнение всех обязанностей, возложенных на них в настоящем Регламенте.

За правонарушения, совершенные в процессе своей деятельности пользователи несут ответственность в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

Ответственными за постоянный контроль выполнения требований данной Регламента сотрудниками, Референтом и делопроизводителями являются:

- Ответственный за обеспечение безопасности ПДн;
- Администратор информационной безопасности информационных систем персональных данных.

ПРИЛОЖЕНИЕ 1 ФОРМА ЖУРНАЛА ПОЭКЗЕМПЛЯРНОГО УЧЕТА СРЕДСТВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ

№ п/п	Наименование средства защиты, эксплуатационной и технической документации	Регистрационные номера средства защиты, эксплуатационной и технической документации	Отметка о выдаче		Отметка о подключении (установке) средства защиты			Отметка об изъятии средства защиты из аппаратных средств		
			Ф.И.О. пользователя средства защиты	Дата и расписка в получении	Ф.И.О. пользователя средства защиты, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены средства защиты	Дата изъятия	Ф.И.О. пользователя средства защиты, производившего изъятие	Расписка об изъятии
1	2	3	4	5	6	7	8	9	10	11

ПРИЛОЖЕНИЕ 2 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ

ЛИСТ
регистрации изменений в Регламенте

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Приложение № 15
к приказу главы администрации
Октябрьского района города Ставрополя

от «11» 08 2017 г. № 134

ИНСТРУКЦИЯ

по порядку проведения проверок состояния защиты персональных данных администрации Октябрьского района города Ставрополя

г. Ставрополь
2017 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет порядок проведения проверок состояния защиты персональных данных (ПДн) администрации Октябрьского района города Ставрополя (далее – Администрации).

1.2. Проведение проверок состояния защиты ПДн осуществляется в целях выявления нарушений требований нормативной документации, установление причин нарушений, разработка плана корректирующих действий направленных на устранение и предотвращение нарушений.

1.3. Проверки осуществляются администратором информационной безопасности (ИБ) информационных систем персональных данных (ИСПДн), ответственным за обеспечение безопасности ПДн, а также руководителями отделов Управления в непосредственно подчиненных им отделов.

1.4. Должностные лица Администрации знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

2. ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕНИХ ПРОВЕРОК

2.1. При проведении внутренней проверки производиться:
- проверка соблюдения требований по обработке и защите персональных данных;
- проверка соблюдения условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;
- проверка эффективности средств защиты ПДн.

2.2. Приказом назначается рабочая группа (комиссия) по проведению проверок состояния защиты ПДн.

2.3. Внутренние проверки проводятся в соответствии с планом внутренних проверок состояния защиты ПДн (далее - План). План формируется в конце текущего года на последующий. Форма Плана представлена в Приложении 1.

2.4. План составляется администратором информационной безопасности (ИБ) ИСПДн Администрации в соответствии с положениями данной Инструкции.

2.5. План должен содержать перечень мероприятий по проверке, перечень проверяемых подразделений и сроки проведения проверок, составленные с учетом требований руководителей отделов, ответственного за обеспечение безопасности ПДн и администратора ИБ ИСПДн.

2.6. Внеплановые проверки могут проводиться в случаях получения жалоб, выявления нарушений системы защиты и подготовки к контролю со стороны уполномоченных федеральных органов, регулирующих деятельность в сфере обработки персональных данных.

2.7. На основании утвержденного Плана внутренних проверок администратором ИБ ИСПДн составляет приказ о проведении проверки деятельности отдела Администрации. Приказ издается не позднее, чем за десять дней до даты проверки.

2.8. В ходе работы в проверяемых отделах должна быть получена объективная и полная информация по состоянию защиты ПДн.

2.9. Проверяющие имеют право, осматривать помещения, где производится обработка ПДн, получать доступ к техническим средствам, участвующим в обработке ПДн, просматривать настройки СЗИ, а также проводить беседы и консультации с работниками отделов.

2.10. При проведении проверок 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;
- соответствие системы защиты ПДн реальному положению дел в Администрации и т.п.

Для проверки эффективности системы защиты персональных данных должны использоваться средства выявления уязвимостей информационной безопасности.

2.11. По результатам проверок составляется акт о результатах внутренней проверки (Приложение 2), выявленных недостатков и нарушений, предложений по их устранению. Руководитель проверяемого отдела должен быть поставлен в известность о выявленных несоответствиях в течение трех дней после проведенной проверки.

3. КОРРЕКТИРУЮЩИЕ МЕРОПРИЯТИЯ И КОНТРОЛЬ ЗА ИХ ИСПОЛНЕНИЕМ

3.1. Руководитель проверяемого отдела анализирует акт о результатах внутренней проверки и в трехдневный срок определяет перечень мероприятий, необходимых для устранения нарушений и их причин.

3.2. Если корректирующие мероприятия касаются других отделов, то к анализу привлекаются специалисты соответствующих подразделений.

3.3. Выполнение корректирующих мероприятий и их достаточность определяется ответственным за обеспечение безопасности ПДн и администратором ИБ ИСПДн.

3.4. Внутренняя проверка считается оконченной после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

4. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

4.1. Полный плановый пересмотр данного документа также проводится регулярно, раз в год, с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн Администрации.

4.2. Частичный пересмотр данного документа проводится по письменному предложению администратора ИБ ИСПДн. Форма регистрации изменений в Инструкцию представлена в Приложении 3.

4.3. Вносимые изменения не должны противоречить другим положениям Инструкции.

5. ОТВЕТСТВЕННЫЕ ЗА ВЫПОЛНЕНИЕ ИНСТРУКЦИИ

Ответственным за выполнения требований данной Инструкции является:

– администратор ИБ ИСПДн в части задач, возложенных на него настоящей инструкцией.

– ответственный за обеспечение безопасности ПДн в части общего контроля информационной безопасности.

УТВЕРЖДАЮ

Глава администрации
Октябрьского района
города Ставрополя

_____ А.А. ломанов

«25» декабря 2018 г.

План внутренних проверок состояния защиты персональных данных на 2019 год

№ п/п	Наименование мероприятия	Наименование отдела	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание
1	Правильность обработки персональных данных информационных систем	Отдел бухгалтерского учета, контроля и отчетности				
2	Правильность обработки персональных данных информационных систем	Отдел правового обеспечения и приёма граждан				
3	Правильность обработки персональных данных информационных систем	Общий отдел				
4	Правильность обработки персональных данных информационных систем	Организационный отдел				
5	Правильность обработки персональных данных информационных систем	Отдел ЖКХ и благоустройства				
6	Правильность обработки персональных данных информационных систем	Отдел социальной работы				

№ п/п	Наименование мероприятия	Наименование отдела	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание

ПРИЛОЖЕНИЕ 2 ФОРМА АКТА ВНУТРЕННЕЙ ПРОВЕРКИ

АКТ

о результатах внутренней проверки _____
наименование структурного подразделения

№_____ от _____

1. Цель проверки_____
2. Основание: _____
3. Время проведения проверки_____
4. Результаты проверки_____

   _____

   _____

   _____
5. Рекомендации по устранению нарушений_____

   _____

   _____

   _____

Члены рабочей группы:

_____

_____

_____

Приложение № 16
к приказу главы Администрации
Октябрьского района
города Ставрополя

от «11» 08 2017 г. № 151

РЕГЛАМЕНТ

доступа в помещения с компонентами информационных систем персональных данных и на территорию администрации Октябрьского района города Ставрополя

г. Ставрополь
2017 г.

СПИСОК СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
СВТ	Средства вычислительной техники
СЗПДн	Система защиты персональных данных

Содержание

1. Общие положения

1.1. Настоящий регламент определяет порядок доступа в помещения, в которых располагаются компоненты (АРМ, серверы, сетевое оборудование и т.п.) информационных систем персональных данных (ИСПДн) и на территорию администрации Октябрьского района города Ставрополя.

1.2. Выполнение требований настоящего Регламента обязательно для всех сотрудников администрации Октябрьского района города Ставрополя, юридических и физических лиц, осуществляющих свою деятельность на территории Администрации.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Регламента, разъяснения возникающих вопросов Администратор ИБ ИСПДн проводит инструктажи (при необходимости) сотрудников.

1.4. Настоящий Регламент не определяет режимные меры в нештатных ситуациях, требующих немедленной эвакуации из помещений персонала, документации, средств вычислительной техники (СВТ) и т.д, таких как:

пожар,
наводнение,
землетрясения, и др.

1.5. В случае невозможности исполнения требований настоящего Регламента в полном объеме, например:

в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок в работе ИСПДн, стихийных бедствий, побочных влияний;
злоумышленных действий.

1.6. Ознакомление с требованиями Регламента администраторов информационной безопасности проводит ответственное лицо за безопасность под роспись, с выдачей электронных копий соответствующих приложений и разделов Регламента непосредственно для повседневного использования в работе.

1.7. Ознакомление руководителей структурных подразделений администрации Октябрьского района города Ставрополя с требованиями Регламента проводит Администратор ИБ ИСПДн под роспись, с выдачей электронных копий Регламента непосредственно для повседневного использования в работе.

1.8. Ознакомление сотрудников структурных подразделений администрации Октябрьского района города Ставрополя с требованиями Регламента проводят руководители этих структурных подразделений под роспись, с выдачей электронных копий Регламента непосредственно для повседневного использования в работе.

Практическая «глубина» исполнения настоящего Регламента может оперативно определяться Администратором ИБ ИСПДн по согласованию с ответственным лицом за защиту ПДн.

2. Порядок пропуска (прохода) лиц на территорию администрации Октябрьского района города Ставрополя

1.9. Доступ сотрудников на территорию администрации Октябрьского района города Ставрополя осуществляется только по предъявлению удостоверения (пропуска).

1.10. Доступ посетителей в вестибюль в рабочее время осуществляется в свободном режиме.

1.11. Доступ посетителей во внутренние помещения администрации Октябрьского района города Ставрополя осуществляется только в рабочее время.

1.12. Порядок доступа в помещения с компонентами ИСПДн определён в разделе 5 настоящего Регламента.

1.13. Доступ сотрудников на территорию и во внутренние помещения администрации Октябрьского района города Ставрополя в нерабочее время осуществляется только по согласованию с руководителем структурного подразделения сотрудника администрации Октябрьского района города Ставрополя, а в помещения с компонентами ИСПДн – по согласованию с руководителем структурного подразделения и ответственным лицом за защиту ПДн. При этом оформляется заявка на доступ, содержащая список сотрудников, для которых планируется доступ и заверенная подписями этих сотрудников и лиц, осуществивших согласование доступа, с указанием требуемых помещений доступа и даты/дат доступа. Заявка передается дежурному и, в течение периода времени доступа, указанного в заявке, является основанием для доступа сотрудника, указанного в заявке, в указанные в заявке помещения при предъявлении этим сотрудником постоянного пропуска.

1.14. Доступ посетителей на территорию и во внутренние помещения Администрации Октябрьского района города Ставрополя в нерабочее

время осуществляется в соответствии с пунктом 1.11 настоящего Регламента и только в сопровождении не менее одного сотрудника администрации Октябрьского района города Ставрополя, имеющего право доступа на территорию и во внутренние помещения администрации Октябрьского района города Ставрополя в соответствии с пунктом 1.13 настоящего Регламента. Доступ посетителей в помещения с компонентами с ИСПДн дополнительно регламентируется разделом 5 настоящего Регламента

1.15. Запрещен проход на территорию администрации Октябрьского района города Ставрополя лиц в состоянии алкогольного, наркотического или иного токсического опьянения.

1.16. О попытках несанкционированного входа на территорию и во внутренние помещения администрации Октябрьского района города Ставрополя, а так же о несанкционированном нахождении лиц на территории и во внутренних помещениях администрации Октябрьского района города Ставрополя дежурный вахтер или сотрудник администрации Октябрьского района города Ставрополя докладывает своему непосредственному руководителю о несанкционированном входе сотрудников или иных лиц в помещения с компонентами с ИСПДн и/или нахождения в помещениях с компонентами с ИСПДн докладывает также и ответственному лицу за защиту ПДн.

3. Внос(ввоз) и вынос (вывоз) материальных ценностей

1.17. На территорию администрации Октябрьского района города Ставрополя запрещается вносить(ввозить):

хозяйственные сумки, чемоданы, свертки и компьютеры без соответствующего разрешения;

взрывчатые вещества;

горючие и легковоспламеняющиеся жидкости и материалы;

алкогольную продукцию, наркотические и психотропные вещества.

1.18. Запрещается несанкционированный вынос (вывоз) или несанкционированное перемещение материальных ценностей администрации Октябрьского района города Ставрополя.

1.19. Запрещается вынос (вывоз) документов, электронных или иных носителей ПДн, а также их передача лицам, не допущенным к обработке ПДн, без согласования с Администратором ИБ ИСПДн или ответственным лицом за защиту ПДн администрации Октябрьского района города Ставрополя.

4. Техническое обеспечение защиты помещений

1.20. Помещения с компонентами ИСПДн (далее - Помещения) оборудуются надежными механическими замками (минимум - с двумя комплектами ключей).

1.21. Помещения с серверным, сетевым оборудованием, оборудованием подсистемы межсетевого экранирования ИСПДн необходимо оборудовать механическими замками или другими средствами разграничения и/или контроля доступа, а также списком лиц, имеющих право находится в помещении самостоятельно.

1.22. Список составляет Администратор ИБ ИСПДн и утверждает руководитель подразделения по форме в Приложении № 1 к настоящему Регламенту. В данные Список вносятся только те сотрудники, право самостоятельного нахождения в Помещении которых обусловлено производственной необходимостью.

1.23. Утвержденный Список вывешивается на основной входной двери Помещения.

5. Режим доступа в помещения

1.24. Сотрудники, фамилии которых, внесены в утвержденные Список, имеют право самостоятельно вскрывать (снимать с охраны) и закрывать (сдавать под охрану) Помещение.

1.25. Лица, не внесённые в Список доступа:
являются посторонними и могут находиться в Помещении только при наличии тех, кто такое право имеет;
обязаны покинуть Помещение при отсутствии в нем сотрудников, которые имеют право самостоятельно находиться в Помещении;

1.26. При доступе в закрытое Помещение (в начале рабочего дня, после обеденного перерыва и т.п.) сотрудники, внесенные в утвержденные Список, перед вскрытием Помещения проверяют целостность пластилиновой печати на двери Помещения. В случае нарушения целостности печати ставится в известность Администратора ИБ ИСПДн, Помещение не вскрывается до принятия им соответствующего решения.

1.27. В течение рабочего дня сотрудники, внесенные в утвержденный Список:

при оставлении последним Помещения - закрывают дверь Помещения («на замок», «на защелку», в зависимости от технического исполнения запорного устройства) и опечатывают их печатью;
не покидают последними Помещение, если в нем находятся лица, не внесенные в Список;
при обнаружении фактов нарушения режима доступа ставят в известность Администратора ИБ ИСПДн;
при посещении Помещения посторонними лицами с целями проведения контрольных, проверочных мероприятий, а также работ по обслуживанию помещений и их инженерно-технических средств ставят в известность об этом Администратор ИБ ИСПДн и руководителя подразделения.

1.28. При обнаружении нарушений режима доступа в Помещения выполняется порядок действий предусмотренный «Инструкцией по действиям персонала в нештатных ситуациях».

6. Режим при обслуживании и ремонте в Помещении

1.29. Обслуживание Помещения (уборка или различный ремонт Помещения, инженерно-технического оборудования) проводится обслуживающим персоналом только в присутствии и под присмотром хотя бы одного из сотрудников, имеющего право самостоятельно находиться в Помещении.

1.30. Механические или электронные ключи от замков дверей Помещений обслуживающему персоналу и/или другим лицам, не допущенных самостоятельно находиться в Помещении, без согласования с ответственным лицом за защиту ПДн, не выдаются.

1.31. Сотрудники подразделения, обеспечивающие контроль действий обслуживающего персонала в Помещении, обязаны не допускать несанкционированных действий в отношении компонентов ИСПДн, бумажных и магнитных носителей информации, компонентов инженерных систем и т.п.

1.32. Капитальный и/или иной ремонт, продолжительный по времени и требующий высвобождения рабочей площади Помещения, может проводиться и без присмотра, однако при этом в обязательном порядке:

компоненты ИСПДн, носители информации должны быть вынесены из ремонтируемого Помещения в другое контролируемое Помещение;
по окончанию ремонта должны быть сменены ключи и коды доступа в Помещение (организовывает и контролирует исполнение Администратор ИБ ИСПДн).

7. Смена кодов и ключей

1.33. При утере основного или запасного комплекта ключей доступа руководитель подразделения инициирует служебное расследование, по результатам которого принимается решение или об изготовлении дополнительного комплекта, или о смене секрета замка и, соответственно, замене всех комплектов ключей на новые.

1.34. Смена кодов доступа и секретов замков в Помещениях организуется руководителем подразделения (как правило, силами Администратора ИБ ИСПДн) в следующих случаях:

увольнения или перемещения из состава подразделения сотрудника, знавшего код доступа в Помещение или имеющего доступ к ключам доступа;
преднамеренного или непреднамеренного разглашения кода доступа в Помещения тем лицам, у которых нет производственной необходимости его знать;
установленного факта бесконтрольного нахождения в Помещении лиц, у которых нет производственной необходимости знать код доступа или иметь ключи доступа;
истечения одного календарного года с момента первичного ввода или последней смены значения кода доступа.

1.35. Смена секретов механических замков и/или кодов доступа электромеханических производится с оформлением акта, который доводится под роспись до всех сотрудников, имеющих право самостоятельно находиться в данном Помещении. Коды доступа доводятся до сотрудников администратором информационной безопасности, как правило, устно, с практической демонстрацией правильности работы устройств разграничения и/или контроля доступа. При необходимости записать код доступа на бумаге, последняя оформляется как парольная карта.

8. Порядок пересмотра Регламента

5.1. Регламент подлежит полному пересмотру в случае приобретения новых технических средств разграничения и контроля доступа. В остальных случаях осуществляется частичный пересмотр настоящего Регламента.

5.2. Полный пересмотр настоящего Регламента проводится с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в Администрации.

5.3. Частичный пересмотр настоящего Регламента проводится ответственным лицом за защиту ПДн.

5.4. Внесение изменений в обязательном порядке фиксируется в «Листе регистрации изменений в Регламенте». Лист регистрации изменений в Регламенте представлен в Приложении № 2.

5.5. Вносимые изменения не должны противоречить другим положениям Регламента.

9. Ответственные за выполнение Регламента

5.6. Ответственность за организацию контрольных и проверочных мероприятий по вопросам доступа в Помещения возлагается на ответственного за защиту ПДн.

5.7. Ответственность за своевременное доведение Регламента до сотрудников в части их компетенции и обеспечение условий для выполнения требований данного Регламента возлагается на руководителей подразделений.

5.8. Ответственность за организацию (полноту и своевременность) материально-технического обеспечения Помещений и сотрудников подразделения несет руководитель этого подразделения.

5.9. Ответственность за соблюдение требований настоящего Регламента возлагается на Администратора ИБ ИСПДн и сотрудников подразделений.

5.10. Администратор ИБ ИСПДн проводит текущий контроль выполнения сотрудниками подразделений требований Регламента.

ПРИЛОЖЕНИЕ № 1 ФОРМА СПИСКА СОТРУДНИКОВ

Подразделение Утверждаю

СПИСОК
сотрудников, имеющих право самостоятельно находиться в помещении №_____

№ п/п	Ф.И.О.	должность	№ личной металлической печати

Администратор
информационной безопасности дата, роспись Ф.И.О.

Ознакомлены сотрудники

_____
_____
_____

ПРИЛОЖЕНИЕ № 2 ФОРМА РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РЕГЛАМЕНТЕ

ЛИСТ № _____ регистрации изменений в Регламенте

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Приложение № 17
к приказу главы Администрации
Октябрьского района города Ставрополя
от «18» 08 2017 г. № 177

Журнал регистрации письменных запросов граждан на доступ к своим персональным данным

№ п/п	Вх. № письма	Дата получения запроса	Ф.И.О.гражданина	Сведения о документе, удостоверяющем личность			Отметка о предоставлении доступа к ПДн (отказе в доступе)	исх. номер и дата письма с ответом на запрос	Ф.И.О., должность, роспись сотрудника, выдавшего ответ	Примечание
				Номер, серия	Дата выдачи	Кем выдан				
1	2	3	4	5	6	7	8	9	10	11