|  |  |  |
| --- | --- | --- |
| **АДМИНИСТРАЦИЯ ЕВСТРАТОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ РОССОШАНСКОГО МУНИЦИПАЛЬНОГО** **РАЙОНА ВОРОНЕЖСКОЙ ОБЛАСТИ****РАСПОРЯЖЕНИЕ**

|  |
| --- |
| от 23.12.2019 г. № 93 |
| с.Евстратовка |

 |

Об утверждении документов,

регламентирующих обработку и обеспечение безопасности

персональных данных

В соответствии с Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 21.03.2012г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», руководящими документами ФСТЭК Российской Федерации и другими нормативными правовыми документами по вопросам использования и защиты информационных ресурсов, содержащих персональные данные,

1. Утвердить прилагаемые:

1.1. Правила обработки персональных данных в администрации Евстратовского сельского поселения, приложение №1.

1.2. Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации Евстратовского сельского поселения, приложение №2.

1.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Евстратовского сельского поселения, приложение №3.

1.4. Правила работы с обезличенными данными в администрации Евстратовского сельского поселения, приложение №4.

1.5. Перечень информационных систем персональных данных обрабатываемых в администрации Евстратовского сельского поселения, приложение №5.

1.6. Перечни персональных данных, обрабатываемых в администрации Евстратовского сельского поселения, в связи с реализацией трудовых отношений, а также в связи с оказанием государственных (муниципальных) услуг и осуществлением государственных (муниципальных) функций, приложение №6.

1.7. Перечень должностейслужащих администрации Евстратовского сельского поселения и её структурных подразделений, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным, а также перечень должностей служащих, ответственным за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приложение№7.

1.8. Должностную инструкцию ответственного за организацию обработки персональных данных в администрации Евстратовского сельского поселения, приложение№8.

1.9. Инструкцию ответственного за обеспечение безопасности персональных данных в информационной системе (администратора безопасности) в администрации Евстратовского сельского поселения, приложение №9.

1.10. Инструкцию пользователя информационных систем персональных данных в администрации Евстратовского сельского поселения, приложение №10.

1.11. Типовое обязательство сотрудника администрации Евстратовского сельского поселения, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора, прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, приложение №11.

1.12. Типовую форму согласия на обработку персональных данных сотрудников администрации Евстратовского сельского поселения, или иных субъектов персональных данных, приложение №12.

1.13. Типовую формуразъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные, приложение №13.

1.14. Порядок доступа сотрудников администрации Евстратовского сельского поселения в помещения, в которых ведется обработка персональных данных, приложение №14.

1.15. Схемы контролируемых зон помещений, приложение №15.

1.16. Инструкцию ответственного пользователя средств криптографической защиты информации, приложение №16.

1.17. Инструкцию 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, приложение №17.

1.18. Регламент по учету, хранению и уничтожению носителей персональных данных администрации Евстратовского сельского поселения, приложение №18.

 1.19. Инструкция по организации антивирусной защиты в ИСПДн в администрации Евстратовского сельского поселения, приложение №20.

2.0. Инструкция при возникновении чрезвычайных ситуаций в ИСПДн в администрации Евстратовского сельского поселения, приложение №21.

 2.1. Инструкция о порядке технического обслуживания и ремонта технических средств ИСПДн в ИСПДн в администрации Евстратовского сельского поселения, приложение №22.

 2.2. Инструкция по маркировке съемных носителей информации, содержащих персональные данные в администрации Евстратовского сельского поселения, приложение №23.

 2.3. Инструкция по порядку учета и хранению съемных носителей персональных данных в администрации Евстратовского сельского поселения, приложение №24.

 2.4. Инструкция пользователям локальной вычислительной сети по порядку пользования в сети международного информационного обмена

(ИНТЕРНЕТ) в администрации Евстратовского сельского поселения, приложение №25

 2.5. Инструкция по организации парольной защиты в ИСПДн в администрации Евстратовского сельского поселения, приложение №26

 2.6. Инструкция администратору безопасности ИСПДн в администрации Евстратовского сельского поселения, приложение №27

1. Установить что, настоящий муниципальный правовой акт распространяется на все структурные подразделения администрации, в которых осуществляется автоматизированная и неавтоматизированная обработка персональных данных, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение функционирования информационных систем персональных данных. Настоящий документ обязаны знать и использовать в работе все сотрудники администрации, а также другие лица, допущенные к работе в ИСПДН.
2. Назначить:

4.1. Ответственного пользователя средств криптографической защиты информации – Грек О.Л., Головуз А.С., Злобина Л.И, Токмаев З.Ф, Радинская О.Н.

4.2. Пользователей средств криптографической защиты информации согласно приложению №19.

1. Ознакомить с настоящим распоряжением работников администрации Евстратовского сельского поселения в части их касающейся.
2. Признать утратившим силу распоряжение администрации Евстратовского сельского поселения от 14.03.2017года № 16 « Об утверждении документов, регламентирующих обработку и обеспечение безопасности персональных данных».
3. Контроль за исполнением настоящего распоряжения возложить на главу Евстратовского сельского поселения.

Приложения:

№ 1 на 21-ом л.в 1 экз;

№ 2 на 8-ми л.в 1 экз;

№ 3 на 3-х л.в 1 экз;

№ 4 на 2-х л.в 1 экз;

№ 5 на 3-х л.в 1 экз;

№ 6 на 15-ти л.в 1 экз;

№ 7 на 19-ти л.в 1 экз;

№ 8 на 2-х л.в 1 экз;

№ 9 на 3-х л.в 1 экз;

№ 10 на 3-х л.в 1 экз;

№ 11 на 1-ом л.в 1 экз;

№ 12 на 3-х л.в 1 экз;

№ 13 на 2-х л.в 1 экз;

№ 14 на 2-х л.в 1 экз;

№ 15 на 2-х л.в 1 экз;

№ 16 на 3-х л.в 1 экз;

№ 17 на 3-х л.в 1 экз;

№ 18 на 7- ми л.в 1 экз;

№ 19 на 1-ом л.в 1 экз.

№ 20 на 2 л. в 1 экз.;

№ 21 на 2 л. в 1 экз.;

№ 22 на 2 л. в 1 экз.;

№ 23 на 1 л. в 1 экз.;

№ 24 на 4 л. в 1 экз.;

№ 25 на 7 л. в 1 экз.;

№ 26 на 2 л. в 1 экз.;

№ 27 на 5 л. в 1 экз..

Глава Евстратовского сельского поселения Г.Д.Лобова

Ознакомлены: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_О.Л.Грек

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Л.И.Злобина

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.С.Головуз

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_З.Ф.Токмаев

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_О.Н.Радинская

Приложение №1

**Правила**

**обработки персональных данных в администрации Евстратовского сельского поселения**

**1. Общие положения**

1.1. Настоящие правила устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных в администрации Россошанского муниципального района Воронежской области (далее - администрация), а также определяют для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1.2. Правовым основанием обработки персональных данных муниципальных служащих и других лиц являются требования:

- Конституции Российской Федерации;

- Трудового кодекса Российской Федерации;

- Гражданского кодекса Российской Федерации;

- Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных»;

- Федерального закона от 02.03.2007г. № 25-ФЗ «О муниципальной службе в Российской Федерации»;

- Федерального закона от 06.10.2003г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации»;

- Федерального закона от 26.12.2008г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»;

- Федерального закона от 02.05.2006г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

- постановления Правительства Российской Федерации от 01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- постановления Правительства РФ от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- других нормативных и правовых актов Российской Федерации.

1.3. В настоящих Правилах используются следующие основные понятия:

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

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

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

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

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

**Вспомогательные технические средства и системы при обработке ПДн** - 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.

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

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

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

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

**Иные категории персональных данных** - персональные данные не относящиеся к категории специальных, биометрических и общедоступных персональных данных.

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

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

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

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

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

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

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

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

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

**Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

 **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**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.

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

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

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

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

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

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

 **Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

 **Система защиты персональных данных** - включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

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

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

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

**Субъект персональных данных** - человек, к которому относятся определенные персональные данные либо которое может быть определено на основании определенных персональных данных.

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

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

**Типовые информационные системы** – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

**Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**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.

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

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

**Целостность информации** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

**Частная модель угроз** – модель угроз применительно к конкретным условиям функционирования ИСПДн.

Иные понятия в настоящих Правилах используются в значениях, определенных действующим законодательством Российской Федерации либо их значение дается по тексту.

1.4. Обозначения и сокращения

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

АС – автоматизированная система

ВП – вредоносная программа

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

ИБ – информационная безопасность

КЗ – контролируемая зона

ЛС – локальная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СВТ – средства вычислительной техники

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СКЗИ – средство криптографической защиты информации

ТКУИ – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

**2. Принципы и цели обработки персональных данных**

2.1. Обработка персональных данных осуществляется на основе следующих принципов:

- обработка персональных данных должна осуществляться на законной и справедливой основе;

- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;

- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- обработке подлежат только персональные данные, которые отвечают целям их обработки;

- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;

- обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;

- оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Цели обработки персональных данных.

Администрация, являясь оператором персональных данных, определяет цели обработки персональных данных в своих информационных системах персональных данных.

Цели обработки персональных данных в информационных системах персональных данных должны быть четко определены и соответствовать:

- закрепленным в Уставе Евстратовского сельского поселения основным полномочиям и правам главы администрации Евстратовского сельского поселения;

- задачам и функциям структурных подразделений администрации, указанным в положениях о таких структурных подразделениях.

Цели обработки персональных данных должны быть:

- конкретны;

- заранее определены;

- законны;

- заявлены.

Цели обработки персональных данных определяют:

- содержание и объем обрабатываемых персональных данных;

- категории субъектов, персональные данные которых обрабатываются;

- сроки их обработки и хранения;

- порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

2.3. Настоящие Правила распространяются на все структурные подразделения администрации, в которых осуществляется автоматизированная и неавтоматизированная обработка персональных данных, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение функционирования информационных систем персональных данных. Настоящий документ обязаны знать и использовать в работе все сотрудники администрации, а также другие лица, допущенные к работе в ИСПДН.

**3. Состав персональных данных**

3.1. Персональные данные включают в себя:

* фамилия, имя, отчество;
* сведения о смене фамилии, имени, отчества;
* число, месяц, год рождения;
* место рождения;
* адрес регистрации;
* адрес местожительства (фактического проживания);
* контактный телефон;
* адрес электронной почты;
* табельный номер сотрудника;
* сведения документа удостоверяющего личность;
* номер страхового свидетельства государственного пенсионного страхования;
* серия, номер полиса обязательного медицинского страхования;
* идентификационный номер налогоплательщика;
* гражданство;
* характеристика сотрудника;
* сведения о воинском учете;
* данные, содержащиеся в военном билете;
* сведения об образовании, повышении квалификации и профессиональной переподготовке, наличии специальных знаний;
* сведения о профессиональной пригодности;
* сведения об инвалидности;
* сведения о фактах прохождения профессиональных медицинских осмотров;
* сведения о наградах, поощрениях, почетных званиях;
* сведения о месте работы (должность, структурное подразделение, категория квалификации, период работы, стаж, сведения об аттестации);
* информация о трудовой деятельности (трудовой стаж, информация о приеме на работу, перемещении по должности, увольнении, основание прекращения трудового договора);
* фотоизображение субъекта персональных данных;
* информация о знании иностранных языков;
* форма допуска;
* сведения о доходах;
* 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 и дополнительного отпусков, 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);
* данные об аттестации сотрудников;
* информация о государственном и негосударственном пенсионном обеспечении;
* семейное положение;
* сведения о близких родственниках (фамилия, имя, отчество, степень родства, год рождения, место работы, должность, сведения о доходах, номер контактного телефона);
* сведения о командировках;
* сведения о временной нетрудоспособности;
* сведения об удержаниях из заработной платы;
* сведения о выданных подотчетных суммах;
* сведения о выданных банковских картах;
* сведения о выплачиваемых алиментах;
* сведения об исправительных работах;
* сведения, содержащиеся в выписке из ЕГРИП;
* сведения, содержащиеся в выписке из ЕГРЮЛ;
* сведения о банковских счетах;
* сведения о земельных участках и ином имуществе, находящемся на определенном праве;
* информация о наличии судимости;
* сведения о привлечении к административной ответственности;
* сведения о совершенном правонарушении;
* сведения о признании гражданина недееспособным или ограниченно дееспособным;
* данные участников ГИА (ЕГЭ);
* свидетельство о рождении ребенка;
* документы, подтверждающие отсутствие родителей (свидетельство о смерти, решение суда, справка об отбывании наказания, иные);
* сведения о занятости несовершеннолетнего;
* справка о прекращении выплаты государственного пособия;
* сведения, подтверждающие отношение гражданина к льготной категории;
* сведения из удостоверения о вынужденных переселенцах;
* данные государственного материнского (семейного) капитала.

3.2. Информация о персональных данных может содержаться:

- на бумажных носителях;

- на электронных носителях;

- в информационных системах персональных данных;

- в информационно-телекоммуникационных сетях и иных информационных системах.

3.3. Перечень документов (копий документов) содержащих персональные данные сотрудников администрации и других лиц:

- распоряжения;

- постановления;

- приказы;

- служебные записки;

- заявления, обращения;

- доверенности;

- авансовые отчеты;

- расчетные листки;

- расходные кассовые ордера;

- справки (о работе, о сумме заработной платы, иных выплатах и вознаграждениях, о выплаченных алиментах и т.д.);

- реестры на получение заработной платы;

- описи документов в кредитном досье по банковским картам в рамках зарплатных проектов;

- графики отпусков;

- табели учета рабочего времени;

- расчетные ведомости заработной платы;

- лицевые счета;

- листки нетрудоспособности;

- справки о доходах, на которые были начислены страховые взносы на обязательное социальное страхование на случай временной нетрудоспособности и в связи с материнством, за два календарных года, предшествующих году прекращения работы (службы, иной деятельности) или году обращения за справкой, и текущий календарный год;

- справки о доходах физических лиц;

- реестры сведений о начисленных и уплаченных страховых взносах на обязательное пенсионное страхование застрахованных лиц;

- трудовые договоры сотрудников;

- личные карточки сотрудников;

- фотографические изображения;

- копии дипломов, сертификатов, удостоверений, аттестатов;

- документы об аттестации (переаттестации) сотрудников;

- копии свидетельств о повышении квалификации;

- копии свидетельств о постановке на учет физического лица в налоговом органе на территории Российской Федерации;

- копии страховых свидетельств государственного пенсионного страхования;

- копии паспортов сотрудников;

- копии свидетельств о заключении/расторжении брака;

- копии свидетельств о рождении детей;

- личный листок по учету кадров;

- направление для участия во временном трудоустройстве;

- трудовые книжки;

- журнал выдачи трудовых книжек;

- согласие на обработку персональных данных;

- лист ознакомления;

- обязательство о неразглашении;

- справки о прохождении медосмотра;

- исполнительные листы (копии), выданные судами общей юрисдикции;

- судебные приказы (копии);

- сведения о гражданине, подлежащем воинскому учету, и принятии его на работу (увольнении его с работы);

- акты (копии) органов, осуществляющих контрольные функции по взысканию денежных средств;

- судебные акты (копии), акты других органов и должностных лиц по делам о правонарушениях;

- постановления (копии) судебного пристава-исполнителя;

- копии приговоров (определений, постановлений) суда;

- грамоты, благодарности;

- документы о конкурсах на должности;

- документы о награждении;

- журналы учета входящих/ исходящих документов;

- журналы регистрации распоряжений, постановлений, приказов;

- другие документы, содержащие персональные данные.

**4. Порядок обработки персональных данных**

4.1. В процессе обработки персональных данных администрация совершает следующие действия (операции) или совокупность действий (операций) с персональными данными субъектов персональных данных: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

4.2. Способы обработки персональных данных.

4.2.1. Администрация самостоятельно устанавливает способы обработки персональных данных в зависимости от целей такой обработки и материально-технических возможностей.

4.2.2. Администрация использует следующие способы обработки персональных данных:

- без использования средств вычислительной техники (неавтоматизированная обработка);

- с использованием средств вычислительной техники (автоматизированная обработка).

4.2.3. Неавтоматизированная обработка персональных данных осуществляется в администрации с учетом требований постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4.2.4. При обработке персональных данных с использованием средств вычислительной техники сотрудники администрации, осуществляющие такую обработку (пользователи объектов вычислительной техники), должны быть ознакомлены под роспись с распоряжениями администрации, устанавливающими порядок использования объектов вычислительной техники.

Обработка персональных данных с использованием средств вычислительной техники в администрации допускается в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

- обработка персональных данных необходима для осуществления и выполнения возложенных на администрацию полномочий и обязанностей;

- 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;

- обработка персональных данных необходима для предоставления или обеспечения предоставления государственных или муниципальных услуг;

- 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;

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

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

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии их обязательного обезличивания;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

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

4.3. Создание персональных данных.

4.3.1. Документы, в том числе в электронном виде, содержащие персональные данные, создаются путем:

- получения оригиналов или надлежаще заверенных копий необходимых документов;

- копирования оригиналов документов;

- внесения сведений в учетные формы (на бумажных и электронных носителях).

4.3.2. Администрация получает персональные данные субъектов персональных данных следующими способами:

- непосредственно от самих субъектов персональных данных, их законных представителей;

- от третьих лиц (например, федеральных органов исполнительной власти, муниципальных органов, судов общей юрисдикции, органов, осуществляющих контрольные функции по взысканию денежных средств, органов уголовно-исполнительной системы).

4.3.3. При сборе персональных данных администрация предоставляет субъекту персональных данных по его просьбе следующую информацию:

- подтверждение факта обработки персональных данных;

- правовые основания и цели обработки персональных данных;

- цели и применяемые способы обработки персональных данных;

- наименование и место нахождения администрации, сведения о лицах (за исключением сотрудников администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с администрацией или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством;

- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных действующим законодательством о персональных данных;

- информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению администрации, если обработка поручена или будет поручена такому лицу;

- иные сведения, предусмотренные действующим законодательством Российской Федерации.

4.3.4. Администрация вправе ограничить право субъекта персональных данных на доступ к его персональным данным в соответствии с федеральным законом, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

4.3.5. Если персональные данные получены не от субъекта персональных данных, администрация, до начала обработки таких персональных данных, предоставляет субъекту персональных данных следующую информацию:

- наименование и адрес администрации или ее представителя;

- цель обработки персональных данных и ее правовое основание;

- предполагаемые пользователи персональных данных;

- права субъекта персональных данных;

- источник получения персональных данных.

Администрация освобождается от обязанности предоставить субъекту персональных данных указанные сведения в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных администрацией;

- персональные данные получены администрацией на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

- персональные данные получены из общедоступного источника;

- администрация осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

- предоставление субъекту персональных данных сведений нарушает права и законные интересы третьих лиц.

4.4. Администрация предоставляет персональные данные субъектов персональных данных непосредственно самим субъектам персональных данных.

4.5. Трансграничная передача персональных данных.

4.5.1. Трансграничная передача обрабатываемых персональных данных сотрудников администрации не осуществляется.

4.5.2. В случае принятия администрацией решения о трансграничной передаче персональных данных, такие данные могут обрабатываться только в случаях:

- наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

- предусмотренных международными договорами Российской Федерации;

- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

- 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 субъекта персональных данных.

Администрация до начала осуществления трансграничной передачи персональных данных обязана убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

4.6. Сроки обработки персональных данных.

4.6.1. Общий срок обработки персональных данных определяется периодом времени, в течение которого администрация осуществляет действия (операции) в отношении персональных данных, обусловленные заявленными целями их обработки, в том числе хранение персональных данных.

4.6.2. Обработка персональных данных начинается с момента их получения администрацией и заканчивается:

- по достижении конкретных, заранее определенных и законных целей;

- по факту утраты необходимости в достижении заранее заявленных целей обработки.

4.6.3. Администрация осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

4.6.4. Сроки хранения персональных данных определяются в соответствии с Приказом Минкультуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», сроком исковой давности, требованиями действующих нормативных правовых актов Российской Федерации, Воронежской области, Россошанского муниципального района.

4.7. Согласие субъекта персональных данных на обработку его персональных данных.

4.7.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие администрации на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным.

4.7.2. Одним из условий обработки персональных данных является ее осуществление с согласия субъекта персональных данных, за исключением случаев, когда:

* 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;
* 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);
* обработка персональных данных необходима для предоставления муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010г. N 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;
* 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;
* обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
* 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;
* 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;
* обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона от 27.07.2006г. N 152-ФЗ «О персональных данных», при условии обязательного обезличивания персональных данных;
* осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);
* осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Во всех других случаях администрацией проводится комплекс мероприятий по получению согласия на обработку персональных данных.

4.7.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных администрация вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии соответствующих оснований, предусмотренных действующим законодательством в области персональных данных.

4.7.4.  Представитель субъекта персональных данных предоставляет согласие на обработку его персональных данных с предъявлением документа, подтверждающего его полномочия.

4.7.5. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, предусмотренных действующим законодательством в области персональных данных, возлагается на администрацию.

4.7.6. В случаях, предусмотренных федеральным законодательством, обработка специальных категорий персональных данных и биометрических персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

4.7.7. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

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

- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

- наименование и адрес администрации, получающей согласие субъекта персональных данных;

- цель обработки персональных данных;

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

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению администрации, если обработка будет поручена такому лицу;

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

- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва;

- подпись субъекта персональных данных.

4.7.8. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

4.7.9. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

4.7.10. Персональные данные могут быть получены администрацией от лица, не являющегося субъектом персональных данных, при условии предоставления администрации подтверждения наличия соответствующих оснований, предусмотренных действующим законодательством в области персональных данных.

4.8. Доступ к персональным данным.

4.8.1. Доступ к персональным данным сотрудников администрации имеют сотрудники администрации, непосредственно использующие эти данные в рамках выполнения своих должностных обязанностей.

4.8.2. Доступ к персональным данным других лиц имеют сотрудники администрации, непосредственно использующие их в рамках выполнения своих должностных обязанностей.

4.8.3. Доступ к персональным данным других лиц и третьих лиц разрешается только при наличии официального заявления запросившего их лица с указанием перечня необходимой информации, целей для которых она будет использована, с согласия субъекта персональных данных, персональные данные которого затребованы, за исключением случаев предусмотренных законодательством.

4.8.4. Сообщение сведений о персональных данных субъекта персональных данных его родственникам, членам семьи, иным близким ему людям также производится администрацией только при наличии письменного согласия субъекта персональных данных.

4.8.5. При передаче персональных данных другим лицам, третьим лицам, в том числе представителям субъектов персональных данных, в порядке, установленном нормативными правовыми актами РФ и настоящими Правилами, передаваемая информация ограничивается только теми персональными данными, которые необходимы для выполнения другими лицами и третьими лицами их функций.

4.8.6. Запрещается передача персональных данных, в том числе их распространение, предоставление и доступ к ним в коммерческих целях без согласия субъекта персональных данных, а также иное использование персональных данных в неслужебных целях.

4.9. Устранение администрацией нарушений законодательства, допущенных при обработке персональных данных. Уточнение, блокирование и уничтожение персональных данных.

4.9.1. Субъект персональных данных вправе требовать от администрации 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.

4.9.2. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных администрация осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации) с момента такого обращения или получения указанного запроса на период проверки.

4.9.3. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных администрация осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

4.9.4. В случае выявления неправомерной обработки персональных данных, осуществляемой администрацией или лицом, действующим по поручению администрации, в срок, не превышающий трех рабочих дней с даты этого выявления, администрация прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению администрации. В случае если обеспечить правомерность обработки персональных данных невозможно, в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, администрация уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных администрация уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя, либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4.9.5. В случае достижения цели обработки персональных данных администрация прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению администрации) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между администрацией и субъектом персональных данных, либо, если администрация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных действующим законодательством в области персональных данных.

4.10. Условия обеспечения конфиденциальности информации.

4.10.1. Сотрудники администрации, имеющие в силу исполнения ими своих должностных обязанностей доступ к персональным данным, при их обработке должны обеспечивать конфиденциальность этих данных.

4.10.2. Обеспечение конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных;

- для общедоступных персональных данных, то есть данных включенных в целях информационного обеспечения в общедоступные источники персональных данных (в том числе справочники, адресные книги и т.п.). В общедоступные источники персональных данных могут включаться фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

4.11. Лица, виновные в нарушении требований действующего законодательства в области персональных данных, несут предусмотренную законодательством Российской Федерации ответственность.

**5. Уведомление об обработке персональных данных**

5.1. Администрация в установленном порядке уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, о внесении изменений в сведения, указанные в уведомлении об обработке персональных данных, а также в случае прекращения обработки персональных данных.

5.2. Администрация вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

- относящихся к субъектам персональных данных, которых связывают с администрацией трудовые отношения;

- полученных администрацией 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 исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

- относящихся к членам (участникам) общественного объединения и обрабатываемых соответствующими общественным объединением, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам 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 или в иных 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 или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

5.3. Уведомление готовится лицом, ответственным за организацию обработки персональных данных в администрации, подписывается главой администрации и направляется в виде документа на бумажном носителе или в форме электронного документа по форме, установленной уполномоченным органом по защите прав субъектов персональных данных.

5.4. В случае изменения сведений, содержащихся в уведомлении об обработке персональных данных, структурное подразделение администрации, являющееся инициатором таких изменений в обработке персональных данных, готовит изменения в уведомление и передает такие изменения лицу, ответственному за организацию обработки персональных данных в администрации. Дальнейшие действия по подготовке изменений в уведомление для передачи в уполномоченный орган по защите прав субъектов персональных данных осуществляются аналогично действиям при первоначальной подаче уведомления.

Приложение №2

**Правила**

 **рассмотрения запросов субъектов персональных данных или их представителей в администрации Евстратовского сельского поселения**

1. Настоящие правила устанавливают процедуры рассмотрения и учета (регистрации) в администрации Евстратовского сельского поселения (далее - администрация) запросов субъектов персональных данных или их представителей (далее - запросы), а также определяют права субъектов персональных данных на доступ к их персональным данным и ограничения таких прав.

2. Настоящие правила разработаны в соответствии с требованиями Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных».

3. При обращении субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных администрация обязана:

3.1. Сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также о возможности ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение 30 дней с даты регистрации запроса субъекта персональных данных или его представителя.

3.2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных дать в письменной форме мотивированный ответ, содержащий ссылку на норму Федерального закона № 152-ФЗ, являющуюся основанием для такого отказа в срок, не превышающий 30 дней со дня обращения субъекта персональных данных или его представителя, либо с даты получения запроса субъекта персональных данных или его представителя.

3.3. Предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

3.4. Уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах, а также принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.5. В случае получения запроса уполномоченного органа по защите прав субъектов персональных данных администрация обязана направить необходимую информацию в течение 30 дней с даты регистрации такого запроса.

4. Право субъекта персональных данных на доступ к его персональным данным.

4.1. Субъект персональных данных имеет право на получение следующих сведений (заявление и уведомление согласно приложению № 1 к настоящим Правилам):

- подтверждение факта обработки персональных данных администрацией;

- правовые основания и цели обработки персональных данных;

- цели и применяемые способы обработки персональных данных;

- наименование и место нахождения, сведения о лицах (за исключением сотрудников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных действующим законодательством о персональных данных;

- информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению администрации, если обработка поручена или будет поручена такому лицу.

4.2. Субъект персональных данных вправе требовать от администрации уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4.3. Сведения, указанные в пункте 4.1 настоящих Правил, должны быть предоставлены субъекту персональных данных в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4.4. Сведения, указанные в пункте 4.1 настоящих Правил, предоставляются субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4.5. В случае если сведения, указанные в пункте 4.1 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

4.6. Субъект персональных данных вправе обратиться повторно к оператору или направить повторный запрос в целях получения сведений, указанных в пункте 4.1 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 4.5 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4.4 настоящих Правил, должен содержать обоснование направления повторного запроса.

4.7. Администрация вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 4.5 и 4.6 настоящих Правил. Такой отказ должен быть мотивированным.

5. Ограничения на право субъекта персональных данных на доступ к его персональным данным.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

- обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

6. Рассмотрение запросов осуществляется структурными подразделениями оператора, обрабатывающими персональные данные.

7. Лицо, ответственное за обработку персональных данных, обеспечивает:

- объективное, всестороннее и своевременное рассмотрение запроса;

- принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

- направление письменного ответа по существу запроса.

8. Все поступившие запросы регистрируются в день их поступления в журнале регистрации запросов.

9. Запрос проверяется на его повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской.

10. Лицо, ответственное за обработку персональных данных, при рассмотрении и разрешении запроса обязано:

- внимательно разобраться по существу запроса, в случае необходимости истребовать дополнительные материалы или направить сотрудников на места для проверки фактов, изложенных в запросе, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;

- принять законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;

- сообщить в письменной форме заявителю о решениях, принятых по его запросу, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

11. В случае выявления неправомерной обработки персональных данных при обращении или по запросу субъекта персональных данных (его представителя) или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица администрации обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки.

12. В случае выявления неточных персональных данных при обращении или по запросу субъекта персональных данных (его представителя) или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица администрации обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

13. В случае подтверждения факта неточности персональных данных уполномоченные должностные лица администрации на основании сведений, представленных субъектом персональных данных или его представителем или иных необходимых документов, обязаны уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

14. В случае выявления неправомерной обработки персональных данных уполномоченные должностные лица администрации в срок, не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченные должностные лица администрации в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных администрация обязана уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

15. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения муниципальными служащими администрации действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается незамедлительно в правоохранительные органы. Результаты служебной проверки докладываются главе администрации Евстратовского сельского поселения.

16. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

17. Непосредственный контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов осуществляет ответственный за организацию обработки персональных данных.

18. Ответственный за организацию обработки персональных данных осуществляет контроль за работой с запросами и организацией их приема как лично, так и через специалистов оператора, в чьи обязанности входит полномочия по осуществлению контроля. На контроль берутся все запросы.

19. При осуществлении контроля обращается внимание на сроки исполнения поручений по запросам и полноту рассмотрения поставленных вопросов, объективность проверки фактов, изложенных в запросах, законность и обоснованность принятых по ним решений, своевременность их исполнения и направления ответов заявителям.

20. Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение № 1

**Форма уведомления об обработке персональных данных**

**субъекта персональных данных**

В администрацию Евстратовского сельского поселения

(Оператор)

от\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (Ф.И.О. заявителя)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование и реквизиты документа, удостоверяющего личность заявителя)

**Заявление**

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, указать цели, способы и сроки ее обработки; предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ); сведения о том, какие юридические последствия для меня может повлечь её обработка. В случае отсутствия такой информации, прошу Вас уведомить меня об этом.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись)«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Ф.И.О.) |  |  |  |

|  |  |
| --- | --- |
|  |    |
| **АДМИНИСТРАЦИЯ ЕВСТРАТОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ РОССОШАНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ВОРОНЕЖСКОЙ ОБЛАСТИ**Ул.Пролетарская, 2 с.Евстратовка, Россошанский район, Воронежская область, 396630. Тел.: 8 (47396) 72-5-31  |
|  |   |  г. | № |   |  |
|  |

**Уведомление**

Уважаемый(ая) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

 (Ф.И.О.)

производится обработка сведений, составляющих Ваши персональные данные:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(указать сведения)

Цели обработки:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Способы обработки:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Перечень лиц, которые имеют доступ к информации, содержащей Ваши персональные данные, или могут получить такой доступ:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Должность** | **Ф.И.О.** | **Вид доступа** | **Примечания** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

По результатам обработки указанной информации нами планируется принятие следующих решений, которые будут доведены до Вашего сведения \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

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

Приложение №3

**Правила**

**осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Евстратовского сельского поселения**

**1. Общие положения**

1.1. В соответствии с настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в администрации Евстратовского сельского поселения (далее - администрация) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006г. N 152-ФЗ "О персональных данных", Постановлениями Правительства Российской Федерации от 15.09.2008г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации", от 21.03.2012г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и другими нормативными правовыми актами.

Для целей настоящих Правил используются понятия, определенные Федеральным законом от 27.07.2006г. N 152-ФЗ "О персональных данных".

**2. Способы и порядок осуществления внутреннего контроля**

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в администрации организуется проведение периодических проверок условий обработки персональных данных.

2.2. Проверки осуществляются уполномоченными должностными лицами, ответственными за организацию обработки персональных данных в администрации, либо комиссией, образуемой распоряжением администрации.

В проведении проверки не может участвовать муниципальный служащий, прямо или косвенно заинтересованный в ее результатах.

2.3. Проверки соответствия обработки персональных данных установленным требованиям в администрации проводятся на основании утвержденного правовым актом администрации ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в администрацию письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

2.4. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

2.5. Должностные лица, ответственные за организацию обработки персональных данных в администрации, имеют право:

- запрашивать у сотрудников администрации информацию, необходимую для реализации полномочий;

- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить главе администрации предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить главе администрации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.6. В отношении персональных данных, ставших известными должностному лицу, ответственному за организацию обработки персональных данных, в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

2.7. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о ее проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывает должностное лицо, ответственное за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

2.8. Контроль за своевременностью и правильностью проведения внеплановой проверки осуществляет должностное лицо, определенное распоряжением администрации о назначении внеплановой проверки.

Приложение № 4

**Правила**

**работы с обезличенными данными в администрации Евстратовского сельского поселения**

**1. Общие положения**

1.1. Настоящие Правила работы с обезличенными персональными данными администрации Евстратовского сельского поселения (далее - администрация) разработаны с учетом Федерального закона от 27.07.2006г. N 152-ФЗ "О персональных данных" и Постановления Правительства РФ от 21.03.2012г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

1.2. Для целей настоящих Правил используются понятия, определенные Федеральным законом "О персональных данных".

**2. Условия и способы обезличивания персональных данных**

2.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных администрации и по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом от 27.07.2006г. N 152-ФЗ "О персональных данных".

2.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;

- замена части сведений идентификаторами;

- обобщение - понижение точности некоторых сведений;

- понижение точности некоторых сведений (например, "Место жительства" может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

- деление сведений на части и обработка в разных информационных системах;

- другие способы.

2.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

2.4. Решение о необходимости обезличивания персональных данных принимается руководителем аппарата администрации.

2.5. Начальники отделов, непосредственно осуществляющих обработку персональных данных, готовят предложения по обезличиванию персональных данных, способу обезличивания, а также обоснование такой необходимости.

2.6. Сотрудники подразделений, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных осуществляют непосредственное обезличивание выбранным способом.

**3. Порядок работы с обезличенными персональными данными**

3.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

3.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

3.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;

- антивирусной политики;

- правил работы со съемными носителями (если они используются);

- правил резервного копирования;

- правил доступа в помещения, где расположены элементы информационных систем.

3.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение правил хранения бумажных носителей, а также правил доступа к ним и в помещения, где они хранятся.

Приложение № 5

**Перечень информационных систем**

**персональных данных, обрабатываемых в администрации Евстратовского сельского поселения.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование ИСПДн, в которой обрабатываются персональные данные | Режим обработки | Вид обработки | Срок хранения |
| 1 | 2 | 3 | 4 | 5 |
| 1. 1
 |  | Многопользова-тельский | Электронный и бумажный |  |
| 1. 2
 |  | Многопользова-тельский | Электронный и бумажный |  |
| 1. 3
 |  | Многопользова-тельский | Электронный и бумажный |  |

Приложение № 6

**Перечни**

**персональных данных, обрабатываемых в администрации Евстратовского сельского поселения, в связи с реализацией трудовых отношений, а также в связи с оказанием государственных (муниципальных) услуг и осуществлением государственных (муниципальных) функций.**

1. Информационная система персональных данных «Кадры» администрации Евстратовского сельского поселения.

Цель: ведение кадровой работы.

Состав обрабатываемых персональных данных:

|  |  |
| --- | --- |
| Состав персональных данных | Категория персональных данных |
| Специальные | Биометриические | Общедоступные | Иные |
| Фамилия, имя, отчество | - | - | - |  |
| Число, месяц, год рождения | - | - | - |  |
| Место рождения | - | - | - |  |
| Адрес (адрес регистрации, фактического проживания) | - | - | - |  |
| Семейное положение |  |  |  |  |
| Социальное положение |  |  |  |  |
| Имущественное положение |  |  |  |  |
| Гражданство | - | - | - |  |
| Образование | - | - | - |  |
| Профессия | - | - | - |  |
| Владение иностранными языками | - | - | - |  |
| Судимость | - | - | - |  |
| Допуск к государственной тайне | - | - | - |  |
| Выполняемая работа с начала трудовой деятельности | - | - | - |  |
| Награды и знаки отличия | - | - | - |  |
| Близкие родственники (степень родства, фамилия, имя, отчество, год, число, месяц и место рождения, место работы, домашний адрес) | - | - | - |  |
| Пребывание за границей | - | - | - |  |
| Отношение к воинской обязанности, воинское звание (военный билет) | - | - | - |  |
| Номер телефона | - | - | - |  |
| Документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан) | - | - | - |  |
| Наличие заграничного паспорта (серия, номер, кем и когда выдан) | - | - | - |  |
| Номер страхового свидетельства обязательного пенсионного страхования | - | - | - |  |
| Идентификационный номер налогоплательщика (ИНН) | - | - | - |  |
| Сведения о доходах, об имуществе и обязательствах имущественного характера |  |  |  |  |
| Фотоизображение | - |  | - |  |

1. Информационная система персональных данных «Бухгалтерский учет» администрации Евстратовского сельского поселения.

Цель: ведение бухгалтерского учета, отчетности, начисления заработной платы, предоставление сведений в ФНС, ПФР, ФСС и т.д.

Состав обрабатываемых персональных данных:

|  |  |
| --- | --- |
| Состав персональных данных | Категория персональных данных |
| Специальные | Биометриические | Общедоступные | Иные |
| Фамилия, имя, отчество | - | - | - |  |
| Число, месяц, год рождения | - | - | - |  |
| Место рождения | - | - | - |  |
| Адрес (адрес регистрации, фактического проживания) | - | - | - |  |
| Семейное положение |  |  |  |  |
| Гражданство | - | - | - |  |
| Профессия |  |  |  |  |
| Документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан) | - | - | - |  |
| Номер страхового свидетельства обязательного пенсионного страхования | - | - | - |  |
| Идентификационный номер налогоплательщика (ИНН) | - | - | - |  |
| Сведения о доходах, об имуществе и обязательствах имущественного характера | - | - | - |  |

1. Информационная система персональных данных «Обращение граждан» администрации Евстратовского сельского поселения.

Цель: обеспечение исполнения полномочий.

Состав обрабатываемых персональных данных:

|  |  |
| --- | --- |
| Состав персональных данных | Категория персональных данных |
| Специальные | Биометриические | Общедоступные | Иные |
| Фамилия, имя, отчество | - | - | - |  |
| Адрес (адрес регистрации, фактического проживания) |  |  |  |  |
| Документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан) |  |  |  |  |
| Номер телефона | - | - | - |  |
| Профессия | - | - | - |  |

1. Информационная система персональных данных «Межведомственное электронное взаимодействие» администрации Евстратовского сельского поселения.

Цель: обеспечение исполнения полномочий.

Состав обрабатываемых персональных данных:

|  |  |
| --- | --- |
| Состав персональных данных | Категория персональных данных |
| Специальные | Биометриические | Общедоступные | Иные |
| Фамилия, имя, отчество | - | - | - |  |
| Адрес (адрес регистрации, фактического проживания) | - | - | - |  |
| Номер телефона | - | - | - |  |
| Документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан) | - | - | - |  |
| Номер страхового свидетельства обязательного пенсионного страхования | - | - | - |  |
| Свидетельство о рождении | - | - | - |  |

1. Информационная система персональных данных «Архив» администрации Евстратовского сельского поселения.

Цель: обеспечение исполнения полномочий.

Состав обрабатываемых персональных данных:

|  |  |
| --- | --- |
| Состав персональных данных | Категория персональных данных |
| Специальные | Биометриические | Общедоступные | Иные |
| Фамилия, имя, отчество | - | - | **-** |  |
| Число, месяц, год рождения | - | - | **-** |  |
| Место рождения | - | - | **-** |  |
| Адрес (адрес регистрации, фактического проживания) | - | - | **-** |  |
| Семейное положение | - | - | **-** |  |
| Социальное положение | - | - | **-** |  |
| Гражданство | - | - | **-** |  |
| Образование | - | - | **-** |  |
| Профессия | - | - | **-** |  |
| Близкие родственники (степень родства, фамилия, имя, отчество, год, число, месяц и место рождения, место работы, домашний адрес) | - | - | **-** |  |
| Документ, удостоверяющий личность (вид документа, серия, номер, кем и когда выдан) | - | - | **-** |  |
| Адрес (адрес регистрации, фактического проживания) | - | - | **-** |  |
| Номер телефона | - | - | **-** |  |
| Номер страхового свидетельства обязательного пенсионного страхования | - | - | **-** |  |
| Идентификационный номер налогоплательщика (ИНН) | - | - | **-** |  |
| Сведения о доходах, об имуществе и обязательствах имущественного характера | - | - | **-** |  |
| Страховой номер в ПФР | - | - | **-** |  |
| Трудовая деятельность | - | - | **-** |  |
| Воинский учет | - | - | **-** |  |
| Ученая степень | - | - | **-** |  |
| Классный чин | - | - | **-** |  |
| Воинское или специальное звание | - | - | **-** |  |
| Дипломатический ранг | - | - | **-** |  |
| Квалификационный разряд | - | - | **-** |  |
| Фотоизображение | - |  | **-** |  |
| Наличие судимости | - | - | **-** |  |
| Доступ к гос. Тайне | - | - | **-** |  |
| Награды или знаки отличия | - | - | **-** |  |
| Сведения об отпусках | - | - | **-** |  |
| Выслуга лет | - | - | **-** |  |
| Наименование организации | - | - | **-** |  |
| № расчетного счета, карты и иные ПДн | - | - | **-** |  |

Приложение № 7

**Перечень**

**должностей служащих администрации Евстратовского сельского поселения и ее структурных подразделений, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным, а также перечень должностей служащих, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных**

1. Главный бухгалтер
2. Старший инспектор
3. Ведущий специалист/ инспектор ВУР
4. Инспектор - бухгалтер
5. Директор КДЦ

Приложение № 8

**Должностная инструкция**

**ответственного за организацию обработки персональных данных**

**в администрации Евстратовского сельского поселения**

**1. Общие положения**

1.1. Настоящая должностная инструкция определяет основные права и обязанности ответственного за организацию обработки персональных данных в администрации Евстратовского сельского поселения (далее - ответственный за организацию обработки персональных данных).

1.2. Ответственный за организацию обработки персональных данных назначается распоряжением администрации (приказом отдела).

1.3. Ответственный за организацию обработки персональных данных в своей деятельности руководствуется Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных», нормативными правовыми актами Российской Федерации, действующими в области обработки персональных данных.

**2. Должностные обязанности**

Ответственный за организацию обработки персональных данных:

- обеспечивает общую организацию работ по защите ПДн;

- подготавливает руководящие документы по вопросам организации СЗПДн для их утверждения;

- утверждает список лиц, допущенных к обработке ПДн в информационных системах персональных данных (разрешительная система доступа);

- заслушивает должностных лиц о состоянии работ по защите ПДн;

- осуществляет внутренний контроль, проводит плановые проверки соблюдения требований безопасности при обработке ПДн;

- организует ознакомление сотрудников с руководящими документами в сфере защиты персональных данных;

- определяет необходимость обучения сотрудников по вопросам обеспечения безопасности ПДн, а также определяет формы и программы обучения сотрудников в области защиты ПДн;

- организует и контролирует регистрацию и рассмотрение запросов субъектов персональных данных.

**3. Права**

Для выполнения возложенных обязанностей ответственный за организацию обработки персональных данных наделяется следующими правами:

* требовать от лиц, осуществляющих обработку персональных данных, и лиц, имеющих доступ к персональным данным, в том числе от пользователей информационных систем персональных данных выполнения установленной технологии обработки персональных данных, инструкций и других правовых документов по обеспечению безопасности персональных данных.
* участвовать в разработке мероприятий по совершенствованию безопасности персональных данных.
* инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемых персональных данных и технических средств из состава информационных систем.
* обращаться с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.
* давать свои предложения по совершенствованию организационных, технологических и технических мер защиты персональных данных в администрацию Евстратовского сельского поселения.

**4. Ответственность**

Ответственный за организацию обработки персональных данных, виновный в нарушении требований Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных», нормативных правовых актов Российской Федерации, действующих в области обработки персональных данных, правовых актов оператора, несет ответственность, предусмотренную законодательством Российской Федерации.

Приложение № 9

**Инструкция**

**ответственного за обеспечение безопасности**

**персональных данных в информационной системе (администратора безопасности)**

**администрации Евстратовского сельского поселения**

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
	1. Ответственный за обеспечение безопасности персональных данных в информационной системе - лицо, выполняющее функции по настройке и сопровождению всех программных и технических средств защиты информации информационной системы персональных данных, предназначенных для обработки информации, содержащей персональные данные (далее ИСПДн).
	2. Ответственный за обеспечение безопасности персональных данных в информационной системе в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой, передаваемой и хранимой в ИСПДн.
	3. Ответственный за обеспечение безопасности персональных данных назначается распоряжением администрации (приказом отдела).
	4. Ответственный за обеспечение безопасности персональных данных в своей работе руководствуется положениями нормативно - правовых актов РФ, руководящими документами по безопасности информации, положениями, приказами и нормативными актами министерств и ведомств Российской Федерации и положениями настоящей Инструкции.

### 2. ОБЯЗАННОСТИ

Основными обязанностями ответственного за обеспечение безопасности персональных данных являются:

* + управление средствами и системами защиты информации (СЗИ) ИСПДн и поддержание их функционирования;
	+ восстановление функций программных и технических СЗИ от НСД к информации;
	+ генерация ключей, личных идентификаторов, а так же паролей для пользователей АС;
	+ формирование и управление списком необходимых реквизитов и значением атрибутов объектов и субъектов доступа;
	+ назначение прав доступа, полномочий и привилегий пользователей к объектам доступа (программам, файлам, каталогам, портам и устройствам ввода-вывода (УВВ);
	+ обеспечение правильной эксплуатации технических и программных СЗИ в ИСПДн;
	+ контроль целостности эксплуатируемого в ИСПДн программного обеспечения, в том числе самих СЗИ, с целью недопущения и выявления несанкционированных модификаций;
	+ текущий, после сбоев и периодический (не реже 1 раза в год) контроль работоспособности средств и систем защиты информации от НСД;
	+ контроль соблюдения пользователями ИСПДн требований инструкций и порядка работы при обработке информации в ИСПДн, по вопросам защиты информации от НСД;
	+ контроль выполнения утвержденной технологии обработки информации в ИСПДн;
	+ выявление подозрительных действий пользователей и попыток НСД к информации, обрабатываемой в ИСПДн, путем анализа системных журналов информационной безопасности при работе в ИСПДн. В случае обнаружения или выявления таких попыток, немедленно докладывать ответственному за соблюдение режима конфиденциальности и руководителю организации;
	+ выполнение резервного копирования машинных документов содержащих персональные данные;
	+ обучение и консультации персонала и пользователей ИСПДн правилам работы с СЗИ от НСД;
	+ организация антивирусной защиты информации и программных средств в ИСПДн;
	+ корректировка содержания с целью соответствия реальным условиям следующих документов:
* инструкция системному администратору;
* инструкция пользователю.
* разрешительная система доступа к информационным ресурсам, программным и техническим средствам.
* взаимодействие с системным администратором, ответственным за организацию обработки персональных данных, по вопросам обеспечения защиты информации и предоставления пользователям прав доступа к ней.

**3. ПРАВА**

Ответственный за обеспечение безопасности персональных данных имеет право:

* Требовать от пользователей ИСПДн выполнения установленной технологии обработки информации, инструкций по обеспечению информационной безопасности ИСПДн.
* Останавливать обработку информации в ИСПДн в случаях подтвержденных нарушений установленной технологии обработки данных, приводящих к нарушению функционирования СЗИ.

**4. ОТВЕТСТВЕННОСТЬ**

* 1. На ответственного за обеспечение безопасности персональных данных возлагается персональная ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с его функциональными обязанностями.
	2. Ответственный за обеспечение безопасности персональных данных несет ответственность по законодательству РФ за нарушение требований нормативно - методических документов по защите информации и настоящей инструкции.

Приложение № 10

**Инструкция**

**пользователя информационных систем персональных данных**

**администрации Евстратовского сельского поселения**

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность пользователя информационных систем персональных данных (далее - пользователь) администрации Евстратовского сельского поселения (далее - администрация).

1.2. Пользователем является каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации (далее - СЗИ) информационных систем персональных данных (далее - ИСПДн).

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией и Положением по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации Россошанского муниципального района.

1.5. Ознакомление сотрудников с требованиями настоящей Инструкции проводит ответственный за обеспечение безопасности персональных данных (далее - ПДн) под роспись.

1.6. Методическое руководство работой пользователя осуществляется ответственным за обеспечение безопасности ПДн.

**2. ФУНКЦИИ И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ**

2.1. Каждый пользователь обязан:

2.1.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по обеспечению безопасности ПДн.

2.1.2. Выполнять свои функциональные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам, техническим средствам, полученным согласно Разрешительной системы доступа к информационным ресурсам, программным и техническим средствам ИСПДн.

2.1.3. Знать и соблюдать установленные требования по режиму обработки ПДн, организации парольной защиты, по проведению антивирусного контроля, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн.

2.1.4. Знать и строго выполнять правила работы с СЗИ.

2.1.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена.

2.1.6. Во время работы с защищаемой информацией экран монитора в помещении располагать так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами, шторы (жалюзи) на оконных проемах должны быть завешаны.

2.1.7. Обо всех выявленных нарушениях, связанных с обработкой ПДн, сообщать ответственному за обеспечение безопасности ПДн.

2.1.8. Заблокировать доступ при отсутствии визуального контроля за рабочей станцией. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.2. Пользователю запрещается:

2.2.1. Разглашать защищаемую информацию по Перечню ПДн, подлежащих защите, третьим лицам.

2.2.2. Копировать защищаемую информацию на неучтенные носители информации.

2.2.3. Использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях.

2.2.4. Самостоятельно устанавливать, тиражировать, или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств ИСПДн.

2.2.5. Подключать личные внешние носители и мобильные устройства к техническим средствам ИСПДн.

2.2.6. Отключать (блокировать) СЗИ ИСПДн.

2.2.7. Обрабатывать информацию и выполнять работы, не предусмотренные Разрешительной системой доступа к информационным ресурсам, программным и техническим средствам ИСПДн.

2.2.8. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

2.2.9. Привлекать посторонних лиц для производства ремонта или настройки средств ИСПДн.

**3. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ**

3.1. Личные пароли доступа к средствам ИСПДн выдаются пользователям администратором безопасности, ответственным за обеспечение безопасности ПДн или другим уполномоченным лицом.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила ввода пароля:

- ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

3.4. Правила хранение пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

- запрещается сообщать другим пользователям личный пароль.

3.5. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования организации парольной защиты;

- своевременно сообщать администратору безопасности или ответственному за обеспечение безопасности ПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

**4. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ**

4.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, другими организационно-распорядительными документами, в соответствии с действующим трудовым законодательством Российской Федерации.

4.2. За правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.3. За разглашение сведений конфиденциального характера и другой защищаемой информации в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

 Приложение № 11

**Типовое обязательство**

**сотрудника администрации Евстратовского сельского поселения, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, паспорт серии \_\_\_\_, номер \_\_\_\_\_\_\_\_\_\_, выданный \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_"\_\_\_" \_\_\_\_\_\_\_\_\_\_ 20\_\_\_ года,

 в период трудовых отношений с администрацией Евстратовского сельского поселения и в течение \_\_\_\_ лет после их прекращения в соответствии с распоряжением администрации от "\_\_"\_\_\_\_\_\_\_\_\_ 20 \_\_ г. N \_\_\_\_\_\_ обязуюсь:

1) не разглашать и не передавать третьим лицам сведения, содержащие персональные данные, которые мне будут доверены или станут известны по работе, кроме случаев, предусмотренных законодательством Российской Федерации и с разрешения ответственного за обработку данных в администрации;

2) выполнять требования приказов, распоряжения и инструкций по обработке персональных данных в части, меня касающейся;

3) в случае попытки посторонних лиц получить от меня сведения, содержащие персональные данные, а также в случае утери носителей информации, содержащих такие сведения, немедленно сообщить об этом лицу, ответственному за обработку персональных данных;

4) не производить преднамеренных действий, нарушающих достоверность, целостность или конфиденциальность персональных данных, хранимых и обрабатываемых в администрации Евстратовского сельского поселения

До моего сведения также доведены: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 (указываются муниципальные правовые акты)

Мне известно, что нарушение этого обязательства может повлечь ответственность, предусмотренную трудовым, административным и уголовным законодательством Российской Федерации.

"\_\_\_" \_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись)

Приложение №12

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (наименование должности руководителя)

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (наименование организации)

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (Фамилия И.О. руководителя)

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (Ф.И.О. гражданина)

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (место регистрации)

**Типовая форма**

 **согласия на обработку персональных данных сотрудников администрации Евстратовского сельского поселения, или иных субъектов персональных данных**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

паспорт серии \_\_\_, номер \_\_\_\_\_\_, выданный\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_"\_\_\_" \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ года, даю согласие администрации на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных п. 3 ч. 1 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, представление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных) и содержащихся в настоящем заявлении, в целях обеспечения соблюдения трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, формирования муниципального резерва кадров, управленческого резерва для замещения вакантных должностей муниципальной службы, а именно:

Фамилия, имя, отчество; сведения о смене фамилии, имени, отчества; число, месяц, год рождения; место рождения; адрес регистрации; адрес местожительства (фактического проживания); контактный телефон; адрес электронной почты; табельный номер сотрудника; сведения из документа удостоверяющего личность; номер страхового свидетельства государственного пенсионного страхования; серия, номер полиса обязательного медицинского страхования; идентификационный номер налогоплательщика; гражданство; характеристика сотрудника; сведения о воинском учете; данные, содержащиеся в военном билете; сведения об образовании, повышении квалификации и профессиональной переподготовке, наличии специальных знаний; сведения о профессиональной пригодности; сведения об инвалидности; сведения о фактах прохождения профессиональных медицинских осмотров; сведения о наградах, поощрениях, почетных званиях; сведения о месте работы (должность, структурное подразделение, категория квалификации, период работы, стаж, сведения об аттестации); информация о трудовой деятельности (трудовой стаж, информация о приеме на работу, перемещении по должности, увольнении, основание прекращения трудового договора); фотоизображение субъекта персональных данных; информация о знании иностранных языков; форма допуска; сведения о доходах; 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 и дополнительного отпусков, 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); данные об аттестации сотрудников; информация о государственном и негосударственном пенсионном обеспечении; семейное положение; сведения о близких родственниках (фамилия, имя, отчество, степень родства, год рождения, место работы, должность, сведения о доходах, номер контактного телефона); сведения о командировках; сведения о временной нетрудоспособности; сведения об удержаниях из заработной платы; сведения о выданных подотчетных суммах; сведения о выданных банковских картах; сведения о выплачиваемых алиментах; сведения об исправительных работах; сведения, содержащиеся в выписке из ЕГРИП; сведения, содержащиеся в выписке из ЕГРЮЛ; сведения о банковских счетах; сведения о земельных участках и ином имуществе, находящемся на определенном праве; информация о наличии судимости; сведения о привлечении к административной ответственности; сведения о совершенном правонарушении; сведения о признании гражданина недееспособным или ограниченно дееспособным; данные участников ГИА (ЕГЭ); свидетельство о рождении ребенка; документы, подтверждающие отсутствие родителей (свидетельство о смерти, решение суда, справка об отбывании наказания, иные); сведения о занятости несовершеннолетнего; справка о прекращении выплаты государственного пособия; сведения, подтверждающие отношение гражданина к льготной категории; сведения из удостоверения о вынужденных переселенцах; данные государственного материнского (семейного) капитала.

Для обработки в целях \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 (указать цели обработки)

Я утверждаю, что ознакомлен с документами администрации Евстратовского сельского поселения, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

"\_\_\_" \_\_\_\_\_\_\_\_\_ 20 \_\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (подпись) (Ф.И.О.)

 Приложение №13

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (адрес местонахождения)

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (фамилия, имя, отчество, адрес места регистрации,

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 серия, номер паспорта,

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 сведения о дате выдачи паспорта, сведения об органе,

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 выдавшем паспорт субъекта персональных данных)

**Типовая форма**

**разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные**

 Уважаемый(ая) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (фамилия, имя, отчество)

В соответствии с требованиями Федерального закона Российской Федерации N 152-ФЗ от 27.07.2006 "О персональных данных" уведомляем Вас, что обязанность представления Вами персональных данных установлена пунктом 2 части 1 статьи 6 Федерального закона "О персональных данных" (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), а также следующими нормативными актами: Федеральным законом "О муниципальной службе в Российской Федерации", Федеральным законом "О противодействии коррупции", Трудовым кодексом Российской Федерации.

В случае отказа Вами представить свои персональные данные администрация Россошанского муниципального района Воронежской области не сможет на законных основаниях осуществить такую обработку, что приведет к следующим для Вас юридическим последствиям:

В соответствии со статьями 57, 65, 69 Трудового кодекса Российской Федерации субъект персональных данных, поступающий на работу или работающий в администрации Евстратовского сельского поселения, обязан представить определенный перечень информации о себе.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений трудовой договор не может быть заключен.

На основании пункта 11 части 1 статьи 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

"\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (дата) (подпись) (расшифровка подписи)

Приложение №14

**Порядок**

**доступа работников администрации Евстратовского в помещения, в которых ведется обработка персональных данных**

**1. Общие положения**

1.1. Настоящий Порядок доступа работников администрации в помещения, в которых ведется обработка персональных данных (далее - Порядок), устанавливает единые требования к доступу работников администрации Евстратовского сельского поселения (далее - администрация) в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в администрации, и обеспечения соблюдения требований законодательства о персональных данных.

1.2. Настоящий Порядок обязателен для применения и исполнения всеми работниками администрации.

1.3. Перечень служебных помещений, в которых ведется обработка персональных данных, утверждается распоряжением администрации.

**2. Требования к служебным помещениям**

2.1. В целях обеспечения соблюдения требований к ограничению доступа в служебные помещения администрации обеспечиваются:

- использование служебных помещений строго по назначению;

- наличие на входах в служебные помещения дверей, оборудованных запорными устройствами, уплотняющими прокладками;

- содержание дверей служебных помещений в нерабочее время в закрытом на запорное устройство состоянии;

- остекление окон в здании администрации, содержание их в нерабочее время в закрытом состоянии;

- доступ в служебные помещения только работников администрации.

2.2. Доступ в служебные помещения работников допускается только для выполнения поручений и получения информации, необходимой для исполнения служебных обязанностей в соответствии с должностной инструкцией, иных лиц - в случаях, установленных законодательством.

2.3. В каждом служебном помещении назначается лицо, ответственное за соблюдение требований к ограничению доступа в служебное помещение.

2.4. Работникам запрещается передавать ключи от служебных помещений третьим лицам.

**3. Контроль за соблюдением требований**

**к доступу работников в служебные помещения**

3.1. Текущий контроль за содержанием служебных помещений осуществляет должностное лицо, ответственное за защиту персональных данных в администрации.

3.2. Работники, обнаружившие попытку проникновения посторонних лиц в служебное помещение, немедленно сообщают об этом должностному лицу, ответственному за защиту персональных данных в администрации.

Приложение 2. Схема электропитания рабочего места и прокладки в помещении линий коммуникаций



Шкаф





Сейф

 Линия слаботочной сети

 Линия электропитания

 Приложение № 16

**Инструкция**

**ответственного пользователя средств криптографической защиты информации**

1. **Общая часть**
	1. Настоящая инструкция разработана в соответствии приказом Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) от 13.06.2001 №152 «Об утверждении инструкции 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» и приказом ФСБ России от 10.07.2014 N 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".
	2. Ответственный пользователь средств криптозащиты информации (далее – СКЗИ) назначается из числа сотрудников администрации Евстратовского сельского поселения (далее – администрация) и освобождается от этих обязанностей распоряжением главы администрации.
2. **Квалификационные требования**

Профессиональные знания и навыки:

* 1. Ответственный пользователь СКЗИ в своей работе руководствуется следующими нормативными документами Российской Федерации и организационно-распорядительной документацией администрации:

– «Инструкцией 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», утвержденной приказом ФАПСИ от 13.06.2001 №152;

– «Типовыми требованиями 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 ФСБ России от 21.02.2008 № 149/6/6-622;

- приказом ФСБ России от 10.07.2014 N 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";

– распоряжениями, инструкциями и иными организационно-распорядительные документами администрации.

1. **Функциональные обязанности**

В обязанности ответственного пользователя СКЗИ входит:

* 1. Своевременное и качественное исполнение поручений руководства администрации, данные в пределах его полномочий, установленных законодательством Российской Федерации.
	2. Оказание консультационной помощи по вопросам соблюдения защиты информации при обращении со средствами криптографической защиты информации.
	3. Постоянное повышение профессиональных навыков и умений, необходимых для надлежащего исполнения функциональных обязанностей.
	4. Знание порядка эксплуатации используемых администрацией СКЗИ.
	5. Ведение установленного нормативными документами учета СКЗИ, ключевых документов, сертификатов электронных цифровых подписей.
	6. Соблюдение режима конфиденциальности при обращении со сведениями, полученными при исполнении функциональных обязанностей, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним.
	7. Надежное хранение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.
	8. Выявление попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним и своевременное оповещение об этом руководителя органа криптографической защиты информации.
	9. Немедленное принятие мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

Ответственный пользователь СКЗИ осуществляет следующие функции:

* 1. Осуществляет профилактическую деятельность по соблюдению требований руководящих документов, технической, эксплуатационной документации с сотрудниками администрации, назначенными пользователями СКЗИ.
	2. Участвует в проведении служебных расследований по фактам нарушения требований по обращению с СКЗИ.
	3. Принимает меры к предотвращению разглашения и утечки информации ограниченного доступа при эксплуатации и хранении специальных технических средств, предназначенных для передачи, приема и обработки конфиденциальной информации, а также при использовании незащищенных каналов связи.

3.13. Участвует в разработке методических и нормативных материалов и оказании необходимой методической помощи в проведении работ по защите информации при обращении с СКЗИ.

1. **Права**

Ответственный пользователь СКЗИ:

* 1. Осуществлять плановые и внеплановые проверки функционирования СКЗИ, наличия ключевых документов и технической документации с СКЗИ.
	2. Осуществлять, в рамках своей компетенции, взаимодействие с организациями-производителями СКЗИ.
	3. При изменении состава СКЗИ получить профессиональную переподготовку, повышение квалификации и стажировку в порядке, установленном законодательством Российской Федерации.
	4. Ходатайствовать о проведении служебной проверки.
1. **Ответственность**

Ответственный пользователь СКЗИ несет персональную ответственность в соответствии с законодательством Российской Федерации за:

* 1. Выполнение возложенных на него обязанностей и правильное использование предоставленных ему прав в соответствии с данными функциональными обязанностями.
	2. Несвоевременное или некачественное выполнение распоряжений администрации.
	3. Разглашение сведений, отнесенных к сведениям ограниченного доступа, ставших известными в ходе выполнения функциональных обязанностей или иным путем, утрату их носителей, передачу третьим лицам, публикацию без разрешения руководства, а также использование для занятия любой деятельностью, которая может нанести ущерб администрации.

 Приложение № 17

**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**

**(инструкция пользователя СКЗИ)**

1. Средства криптографической защиты информации (далее – СКЗИ) предназначены для обеспечения безопасности хранения, обработки и передачи по каналам связи информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну.
2. Обладатели конфиденциальной информации обязаны выполнять указания ответственного пользователя СКЗИ по всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

Для работы с СКЗИ допускаются только уполномоченные должностные лица, имеющие необходимый уровень знаний работы с СКЗИ и назначенные распоряжением главы администрации Евстратовского сельского поселения.

1. Пользователи СКЗИ ОБЯЗАНЫ**:**
* не разглашать конфиденциальную информацию, к которой они допущены, рубежи её защиты, в том числе сведения о криптоключах;
* соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
* сообщать ответственному пользователю СКЗИ о ставших им известных попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документов к ним;
* при отстранении, увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы;
* немедленной уведомлять ответственного пользователя СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.
1. Пользователям ЗАПРЕЩАЕТСЯ**:**
* осуществлять несанкционированное копирование ключевых документов;
* осуществлять несанкционированный вынос ключевых носителей за пределы контролируемой зоны;
* хранить ключевые документы и ключевые носители вне специально выделенных хранилищ и помещений;
* вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя;
* вносить какие-либо изменения в программное обеспечение СКЗИ;
* изменять настройки, установленные программой установки СКЗИ или администратором информационной безопасности;
* осуществлять несанкционированное вскрытие системных блоков ПЭВМ, подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные в комплектации.
1. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения и ознакомления с настоящей инструкцией. Обучение пользователей правилам работы с СКЗИ осуществляет ответственный пользователь СКЗИ.
2. Изготовление ключевых документов осуществляется ответственным пользователем СКЗИ с применением штатных СКЗИ (если такая возможность предусмотрена эксплуатационной и технической документацией СКЗИ).
3. Ключевые документы, СКЗИ с введёнными криптографическими ключами относятся к материальным носителям, содержащие конфиденциальную информацию. При этом должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения с конфиденциальной информацией в организации.
4. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учёту в «Журнале поэкземплярного учета криптографических средств, эксплуатационной и технической документации к ним, ключевых документов».
5. Все экземпляры СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы должны быть выданы под расписку в соответствующем журнале учета пользователей СКЗИ, несущих персональную ответственность за их сохранность.
6. Передача экземпляров СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под расписку в соответствующем журнале.
7. Пользователи СКЗИ хранят установочные пакеты СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в шкафах (ящиках, сейфах) индивидуального пользования, в условиях, исключающих бесконтрольный доступ к ним, а также и непреднамеренное уничтожение.
8. Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется создать их резервные копии. Копии должны быть соответствующим образом маркированы и могут использоваться и храниться так же, как и оригиналы.
9. Криптографические ключи, в отношении которых возникло подозрение в компрометации, необходимо немедленно изъять и при доказательстве компрометации надлежащим образом уничтожить.
10. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, должны обеспечивать сохранность конфиденциальной информации, СКЗИ, ключевых документов и ключевых носителей.
11. Средства вычислительной техники, на которых осуществляется штатное функционирование СКЗИ, должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

Приложение №18

**Регламент по**

**учету, хранению и уничтожению носителей персональных данных**

 **в администрации Евстратовского сельского поселения**

1. Настоящий регламент устанавливает организацию учета, хранения, выдачи и уничтожению машинных носителей персональных данных информационных систем персональных данных (ИСПДн)в администрации Евстратовского сельского поселения*.*

 2. Учет, хранение и выдачу машинных носителей персональных данных осуществляют сотрудники структурных подразделений, на которых возложены функции учета, хранения и выдачи носителей персональных данных, данные сотрудники несут персональную ответственность за сохранность персональных данных. При увольнении сотрудника, ответственного за учет, хранение и выдачу машинных носителей персональных данных, составляется акт приема-сдачи этих документов.

 3. Организация учета машинных носителей персональных данных.

 Все находящиеся на хранении и в обращении машинные носители персональных данных (далее - носители) подлежат учёту. Учет всех видов и типов носителей производится в Журнале учета носителей персональных данных (приложение №1).

 Каждый носитель должен иметь этикетку, на которой указывается его уникальный учетный номер. На несъемную часть носителя ПДн наносятся:

* учетный номер;
* отметка «Персональные данные»;
* дата регистрации (день, месяц, год);

4. Организация выдачи машинных носителей персональных данных.

 Пользователи ИСПДн получают учтенный съемный носитель от уполномоченного сотрудника, для выполнения работ на конкретный срок. При получении делаются соответствующие записи в Журнале учета выдачи машинных носителей персональных данных (приложение №2). По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в Журнале учета выдачи машинных носителей персональных данных.

 5. Организация хранения машинных носителей персональных данных.

Хранение носителей осуществляется в условиях, исключающих несанкционированное копирование, изменение или уничтожение конфиденциальной информации, а также хищение носителей**.** Носители должны храниться в служебных помещениях, в сейфе – установленным порядком. Запрещается хранить машинные носители персональных данных вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

 **6.** Действия при утрате или уничтожении съемных носителей персональных данных – в случае утраты носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность ответственный за обеспечение безопасности персональных данных. Соответствующие отметки вносятся в Журналы учета машинных носителей персональных данных.

7. Носители, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение носителей осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется Акт уничтожения машинных носителей персональных данных.

 8. При передаче средств вычислительной техники администрации Россошанского муниципального района сторонним организациям для проведения ремонтно-восстановительных или иных работ, несъемные машинные носители изымаются из состава средства вычислительной техники.

 9. Ответственность за выполнение правил эксплуатации машинных носителей персональных данных при выполнении непосредственных работ с носителями несет пользователь ИСПДн.

 10. Контроль выполнения пользователями установленных правил эксплуатации машинных носителей персональных данных, осуществляет ответственный за эксплуатацию объекта информатизации, ответственный за обеспечение безопасности персональных данных и администратор безопасности информации в рамках своих должностных обязанностей.

Приложение №1

к регламенту по

учету, хранению и уничтожению

 носителей персональных данных администрации Евстратовского сельского поселения

**Журнал учета носителей персональных данных**

Журнал начат «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ г.

Должность\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица /

Журнал завершен «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ г.

Должность\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица /

На \_\_\_\_\_ листах

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Регистрационный номер | Дата учета | Тип / емкость носителя | Серийный номер | Отметка о постановке на учет (ФИО, подпись, дата) | Отметка о снятии с учета (ФИО, подпись, дата) | Местоположение носителя | Сведения об уничтожении носителя / стирании информации |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

Приложение №2

к регламенту по

учету, хранению и уничтожению

носителей персональных данных администрации Евстратовского сельского поселения

**Журнал учета выдачи носителей персональных данных**

Журнал начат «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ г.

Должность\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица /

Журнал завершен «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ г.

Должность\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО должностного лица /

На \_\_\_\_\_ листах

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Учетный номер | Датавыдачи НПДн | Кому выдан(фамилия) | Расписка в получении, дата | Расписка в обратном приеме, дата |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Приложение №19

**Список пользователей**

**средств криптографической защиты информации**

|  |  |  |
| --- | --- | --- |
| №п/п | Должность | ФИО |
|  | Главный бухгалтер | Злобина Л.И |
|  | Ведущий специалист/ инспектор ВУР | Грек О.Л. |
|  | Старший инспектор | Токмаев З.Ф. |
|  |  Инспектор -бухгалтер | Головуз А.С. |
|  | Директор КДЦ | Радинская О.Н.  |

|  |  |  |
| --- | --- | --- |
|

|  |  |
| --- | --- |
|  |  Приложение №20  |

 |

Инструкция

по организации антивирусной защиты в ИСПДн администрации Евстратовского сельского поселения

1. Общие положения

Компьютерный вирус является разрушающей программной закладкой и характеризуется значительным деструктивным потенциалом для программ, данных и любой информации, храня­щейся на компьютерах и магнитных носителях. Особую опасность представляет то обстоятельст­во, что компьютерные вирусы могут скрытно и постепенно уничтожать, либо мгновенно разру­шать хранящуюся в компьютере и на носителях информацию, при этом также могут пострадать аппаратные средства.

Основными путями вирусного вторжения являются неквалифицированное обращение поль­зователей с компьютерной техникой при использовании ими зараженных носителей и программ, либо целенаправленное спланированное воздействие извне с использованием компьютерных ви­русов. При любых обстоятельствах это затрагивает вопросы защиты информации и интересы ад­министрации Россошанского муниципального района Воронежской области.

2.**Порядок обеспечивающий безопасную работу на компьютере с носителями информации**

1. Вновь поступающее программное обеспечение должно быть подвергнуто входному кон­тролю - проверке на отсутствие вирусов и проверке соответствия длины и контрольных сумм, ес­ли таковые указаны в сопроводительных документах, полученным длинам и контрольным сум­мам.
2. Допуск сотрудников к самостоятельной работе на компьютерах и с внешними носителями осуществляется только после овладения ими навыками работы с компьютером, антивирусными пакетами программ.
3. На компьютерах может использоваться программное и аппаратное обеспечение, необхо­димое только для выполнения служебной деятельности. Запрещается использовать на компьюте­рах программные и аппаратные средства, не согласованные с целями обработки информации ог­раниченного доступа.
4. В обязательном порядке должен быть установлен и активирован пакет антивирусных про­грамм. Ответственность за это несет администратор безопасности ИСПДн. Установка средств ан­тивирусного

контроля (в том числе настройка параметров средств антивирусного контроля) осу­ществляется в соответствии с руководствами по применению конкретных антивирусных средств. Антивирусные средства устанавливаются при вводе в эксплуатацию ИСПДн или при их плановой замене.

1. Периодически пользователь проверяет его дисковое пространство с использованием анти-
2. Пользователь (в случае необходимости совместно с администратором безопасности) обя­зан проводить антивирусный контроль любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивируемые/разархивируемые файлы и т.д.), получаемой на съемных носителях (магнитных дисках, оптических носителях, Flash - память и т.п.).
3. В случае обнаружения при проведении антивирусной проверки зараженных компьютер­ными вирусами файлов пользователь обязан:
* приостановить работу;
* немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ад­министратора безопасности ИСПДн, владельца зараженных файлов, а также смежные подразделе­ния, использующие эти файлы в работе;
* совместно с администратором безопасности провести анализ необходимости дальнейшего использования зараженных вирусом файлов;
* провести лечение или уничтожение зараженных файлов (при необходимости для выполне­ния требований данного пункта привлечь администратора безопасности).

Все факты обнаружения зараженных вирусом файлов администратор безопасности заносит в «Журнал регистрации работ по антивирусной защите и выявления вирусного заражения в ИСПДн» (приложение 1), где отображается тип зараженного файла, характер содержащейся в файле информации, название вируса, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность

Ответственность за поддержание установленного порядка проведения антивирусного кон­троля возлагается на администратора безопасности ИСПДн.

Пользователь и администратор безопасности несут ответственность за качество и своевре­менность выполнения задач и функций, возложенных на них в соответствии с настоящей Инст­рукцией.

|  |
| --- |
|   |

Приложение №21

Инструкция

при возникновении чрезвычайных ситуаций в ИСПДн администрации Евстратовского сельского поселения.

1. Общие положения

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн, меры и средства поддержания непрерывности работы и вос­становления работоспособности ИСПДн после возникновений аварийных ситуаций.

Задачей данной Инструкции является:

* определение мер защиты от прерывания работоспособности;
* определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

* системы жизнеобеспечения;
* системы обеспечения отказоустойчивости;
* системы резервного копирования и хранения данных;
* системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости.

В настоящем документе под аварийной ситуацией понимается некоторое происшест­вие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользо­вателям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных ниже:

* технологические угрозы (пожар в здании, повреждение водой, взрыв, химический вы­брос в атмосферу);
* внешние угрозы (массовые беспорядки, сбои общественного транспорта, эпидемия, массовое отравление персонала);
* стихийные бедствия (удар молнии, сильный снегопад, сильные морозы, просадка грунта с частичным обрушением здания, затопление водой в период паводка, навод­нение, вызванное проливным дождем, торнадо);
* телекоммуникационные и информационно-технические угрозы (сбой системы конди­ционирования, сбой ИТ - систем);
* угроза, связанная с человеческим фактором (ошибка персонала, имеющего доступ к серверной, нарушение конфиденциальности, целостности и доступности конфиденци­альной информации);
* угрозы, связанные с внешними поставщиками (отключение электроэнергии, сбой в работе интернет-провайдера, физический разрыв внешних каналов связи).
* Все действия в процессе реагирования на аварийные ситуации, возникающие в ИСПДн, должны документироваться администратором безопасности.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реаги­рование сотрудники (Администратор и пользователи ИСПДн) предпринимают меры по вос­становлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2. Уровни реагирования на инцидент.

При реагировании на инцидент, важно, чтобы пользователь правильно классифициро­вал критичность инцидента. Критичность оценивается на основе следующей классификации:

1. Незначительный инцидент. Незначительный инцидент определяется как локаль­ное событие с ограниченным разрушением, которое не влияет на общую доступность эле­ментов ИСПДн и средств защиты. Эти инциденты решаются пользователями и администра­тором безопасности ИСПДн.

Сбой программного обеспечения. Администратор безопасности выясняет причину сбоя программного обеспечения (далее - ПО). Если исправить ошибку своими силами (в том числе после консультации с разработчиками ПО) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику ПО.

Отключение электричества. Администратор безопасности проводит анализ на наличие потерь и (или) разрушения данных и ПО, а так же проверяет работоспособность оборудова­ния. В случае необходимости, производится восстановление ПО и данных из последней ре­зервной копии с составлением акта.

Потеря данных. При обнаружении потери данных администратор безопасности про­водит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий с составлением акта.

Обнаружена утечка информации (уязвимость в системе защиты). При обнаружении утечки информации ставится в известность администратор безопасности и начальник под­разделения. Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищённости системы и, если необходимо, при­нимаются меры по устранению уязвимостей и предотвращению их возникновения.

Физическое повреждение ПЭВМ. Ставится в известность администратор безопасно­сти. Проводится анализ на утечку или повреждение информации. Определяется причина по­вреждения ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное рас­следование. Проводится проверка ПО на наличие вредоносных программ-закладок, целост­ность ПО и данных. Проводится анализ электронных журналов. При необходимости прово­дятся меры по восстановлению ПО и данных из резервных копий с составлением акта.

1. Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты реша­ются администратором безопасности совместно с руководством. К авариям относятся сле­дующие инциденты:
* отказ элементов ИСПДн и средств защиты из-за повреждения водой, сбоя системы

кондиционирования;

* отсутствие администратора безопасности более чем на сутки из-за химического вы­броса в атмосферу, сбоев общественного транспорта, эпидемии, массового отравления

персонала, сильного снегопада, торнадо, сильных морозов.

1. Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособ­ности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

* пожар в здании;
* взрыв;
* просадка грунта с частичным обрушением здания;
* массовые беспорядки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций.

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвра­щения возникновения аварийных ситуаций, такие как:

* системы жизнеобеспечения;
* системы обеспечения отказоустойчивости;
* системы резервного копирования и хранения данных;
* системы контроля физического доступа.
* Системы жизнеобеспечения ИСПДн включают:
* пожарные сигнализации и системы пожаротушения;
* системы вентиляции и кондиционирования;
* системы резервного питания.

Помещения, в которых размещаются элементы ИСПДн и средства защиты должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Администратор безопасности ознакомляет всех пользователей, находящихся в его зо­не ответственности, с данной инструкцией в срок, не превышающий 3-х рабочих дней с мо­мента выхода нового сотрудника на работу.

Должно быть проведено обучение сотрудников Управления, имеющих доступ к ре­сурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

* оказание первой медицинской помощи;
* пожаротушение;
* эвакуация людей;
* защита материальных и информационных ресурсов;
* методы оперативной связи со службами спасения и лицами, ответственными за реа­гирование сотрудниками на аварийную ситуацию;
* выключение оборудования, электричества, водоснабжения, газоснабжения.

Администратор безопасности ИСПДн должен быть дополнительно обучен методам

частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации. Сроки и поря­док их обучения согласуется с Администратором безопасности

|  |
| --- |
|   |

Приложение №22

ИНСТРУКЦИЯ

о порядке технического обслуживания и ремонта технических средств ИСПДн администрации Евстратовского сельского поселения

Общие положения

Настоящая инструкция определяет правила работ по техническому обслуживанию, ремонту, модернизации технических средств, входящих в состав ИСПДн, защищенных от несанкционированного доступа (НСД) и предназначенных для обработки и хранения персональных данных.

Данные работы проводятся только с разрешения руководителя администрации Евстратовского сельского поселения, после согласования с администратором безопасности ИСПДн.

Порядок проведения работ по техническому обслуживанию, ремонту,

модернизации

В случае, когда необходимо провести работы по техническому обслуживанию (ремонту, модернизации) технических средств, входящих в состав ИСПДн, администратор безопасности ИСПДн представляет служебную записку, в которой:

* указывает название (ПЭВМ, технического средства, системы), техническое обслуживание (ремонт, модернизацию) которой необходимо провести и с какой целью;
* обосновывает необходимость технического обслуживания (модернизации);
* указывает планируемые место и сроки работ, режим их проведения;
* перечисляет меры безопасности, которые будут реализованы при техническом обслуживании (ремонте, модернизации) с целью недопущения доступа к персональным данным посторонних лиц.

В случае если для проведения работ необходимо привлекать лиц, не имеющих постоянного допуска к работе на ПЭВМ или в помещение, составляется список сотрудников, который согласовывается с руководителем администрации.

Запрещается выносить технические средства и системы (ТСС), входящие в состав ИСПДн, с территории здания без согласования с администратором безопасности ИСПДн и разрешения руководителя администрации.

При вскрытии печатей и пломб на технических средствах (системах), последующее опечатывание производится комиссионно в присутствии администратора безопасности информации, о чём составляется акт.

В акте указывается:

* номер (название) помещения, в котором проводились работы.
* дата и время начала и окончания работ,
* лица, присутствовавшие при вскрытии и обслуживании (ремонте, модернизации),
* наличие, целостность и места размещения печатей (пломб, специальных защитных знаков) до вскрытия ПЭВМ (технического средства, системы),
* установленные неисправности,
* виды и результаты проведенных работ,
* замененные или отремонтированные узлы (детали), наличие на этих узлах специальных защитных знаков,
* какими печатями (пломбами и т.д.) и в каких местах ПЭВМ (устройство) опечатано по окончании работ,
* необходимость проведения дополнительной специальной проверки и специальных исследований (сертификации) ПЭВМ (технического средства, системы) или её отдельных узлов,
* иная необходимая для дальнейшей работы и обеспечения безопасности информация.

Если для ремонта (модернизации) ИСПДн (другого технического средства, системы, узла ПЭВМ в составе ИСПДн) необходимо направить в специализированную организацию, то комиссией составляется заключение.

Перед отправкой ПЭВМ (другого технического средства, системы, узла ПЭВМ) администратор безопасности информации обязан гарантированно удалить персональные данные с жесткого диска и иных устройств памяти ПЭВМ (другого технического средства, системы) сертифицированными средствами, о чем он составляет акт. По запросу из специализированной организации копия акта передаётся и ей.

В случае если не имеется возможности гарантировано удалить персональные данные с жесткого диска и иных устройств памяти ПЭВМ (другого технического средства, системы) сертифицированными средствами, эти устройства опечатываются и хранятся в ИСПДн с соблюдением требований, предъявляемым к хранению персональных данных.

Ремонт и замена жесткого диска производится в присутствии администратора безопасности информации. При диагностике и ремонте жесткого диска должны быть реализованы меры безопасности, исключающие несанкционированный доступ к хранящимся на нём данным.

|  |
| --- |
|  |

Приложение №23

ИНСТРУКЦИЯ

 по маркировке съемных носителей информации, содержащих персональные данные

Носители информации (съемные магнитные диски, CD и DVD диски, дискеты и USB флеш-накопители), предназначенные для хранения на них конфиденциальной информации, берутся на учет до записи на них персональных данных.

Для записи информации, содержащей персональные данные, должны использоваться специально выделенные диски, дискеты и USB флеш-накопители.

При постановке на учет съемного диска его маркировка производится на металлической пластине, прикрывающей нерабочую поверхность нижнего диска, посредством нанесения записей механическим путем или красящим веществом, имеющим хорошую механическую стойкость. На дискеты и USB флеш-накопители с двух сторон наносится красящее стойкое вещество. На CD и DVD дисках наносится на нерабочую поверхность красящее стойкое вещество.

К работе с персональными данными должны допускаться только те лица, которые указаны в разрешении на автоматизированную обработку информации, и только в те интервалы рабочего времени, которые отведены для решения указанной задачи в графике рабочего времени.

Инвентарный номер персональному компьютеру, съемному диску, CD и DVD дискам, USB флеш-накопители или дискете присваивается один раз при их первичном учете и может быть изменен только при проведении инвентаризации и заведении нового учета, о чем делается отметка в соответствующих учетных формах.

Персональные компьютеры, используемые для хранения информации на длительное время, подлежат инвентарному учету с отражением содержащейся информации. В этих случаях указанные компьютеры на период, пока они не используются в работе, опечатываются администратором безопасности. Включение этих компьютеров в работу в соответствии с заказом (заданием, запросом) производится исполнителем (пользователем) в присутствии администратора безопасности.

Жесткие магнитные диски при обработке на них персональных данных используются, как правило, в качестве рабочих магнитных носителей информации, которая должна обязательно стираться по окончании выполнения каждого конкретного расчета.

Приложение №24

ИНСТРУКЦИЯ

по порядку учета и хранению съемных носителей персональных данных в администрации Евстратовского сельского поселения

* 1. Общие положение
1. Настоящая Инструкция разработана в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования носителей информации.
2. Действие настоящей Инструкции распространяется на сотрудников администрации, подрядчиков и третью сторону.

2. Основные термины, сокращения и определения

* Администратор ИС - технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.
* АРМ - автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.
* ИБ - информационная безопасность - комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

ИС- информационная система - система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

* Носитель информации - любой материальный объект, используемый для хранения и передачи электронной информации.
* Паспорт ПК - документ, содержащий полный перечень оборудования и программного обеспечения АРМ.
* ПК - персональный компьютер.
* ПО - Программное обеспечение вычислительной техники.
* ПО вредоносное - ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.
* ПО коммерческое - ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.
* Пользователь - работник Организации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования носителей информации

Под использованием носителей информации в ИС Государственной инспекции труда в Воронежской области понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации, администрации Евстратовского сельского поселения.

В ИС допускается использование только учтенных носителей информации, которые являются собственностью администрации и подвергаются регулярной ревизии и контролю.

К предоставленным носителям персональных данных предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется ответственным за защиту персональных данных).

Носители персональных данных предоставляются сотрудникам администрации по инициативе Руководителей структурных подразделений в случаях:

* необходимости выполнения вновь принятым работником своих должностных обязанностей;
* возникновения у сотрудника администрации производственной необходимости.

Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизация:

* Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.
* Учет и выдачу съемных носителей персональных данных осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Факт выдачи съемного носителя фиксируется в «журнале учета съемных носителей с персональными данными».
* Сотрудники администрации получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.
* При использовании сотрудниками носителей с персональными данными **необходимо:**
* Соблюдать требования настоящей Инструкции.
* Использовать носители информации исключительно для выполнения своих служебных обязанностей.
* Ставить в известность ответственного за защиту персональных данных о любых фактах нарушения требований настоящей Инструкции.
* Бережно относится к носителям персональных данных.
* Обеспечивать физическую безопасность носителей информации всеми разумными способами.
* Извещать ответственного за защиту персональных данных о фактах утраты (кражи) носителей персональных данных.

При использовании носителей персональных данных запрещено:

* Использовать носители персональных данных в личных целях.
* Передавать носители персональных данных лицам, не имеющим доступ к обработке персональных данных в данной информационной системе персональных данных.
* Хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
* Выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником администрации Россошанского муниципального района Воронежской области между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с ответственным за защиту персональных данных заранее). Ответственный за защиту персональных данных оставляет за собой право блокировать или ограничивать использование носителей информации.

Информация об использовании сотрудником администрации носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена Руководителю администрации Евстратовского сельского поселения.

В случае выявления фактов несанкционированного и/или нецелевого использовании носителей персональных данных инициализируется служебная проверка, проводимая комиссией, состав которой определяется Руководителем администрации.

По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю администрации для принятия мер согласно локальным актам администрации и действующему законодательству.

Информация, хранящаяся на носителях персональных данных, подлежит обязательной проверке на отсутствие вредоносного ПО.

При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

В случае утраты или уничтожения съемных носителей персональных данных либо разглашении содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей персональных данных.

Съемные носители персональных данных, пришедшие в негодность, или отслуживших установленный срок, подлежат уничтожению. Уничтожение съемных носителей с персональными данными осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт по прилагаемой форме

В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители персональных данных изымаются.

**4.Ответственность**

Работники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством и локальными актами администрации Россошанского муниципального района Воронежской области.

Приложение №25

Инструкция

пользователям локальной вычислительной сети по порядку пользования в сети международного информационного обмена

(ИНТЕРНЕТ)

1. Общие положения

Инструкция разработана на основании федерального закона «Об информации информатизации и защите информации» от 27 июля 2006 года №149-ФЗ, «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 9 сентября 2000 года№ Пр-1895, «Специальных требований и рекомендаций по защите конфиденциальной информации» (СТР-К) утвержденных приказом Гостехкомиссии России 30 августа 2002 года № 282, указа Президента «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 года № 35 1 и других нормативно ­правовых документов в области защиты информации.

Настоящая Инструкция определяет основные требования по организации работы в области защиты информации, общий порядок обращения с документами и другими материальными носителями информации при подключении и использовании международных информационных сетей (МИС) общего пользования, в том числе сети Интернет.

Интернет - всемирная компьютерная сеть, которая использует для взаимодействия стек протоколов TCP/IP (протокол управления передачи сообщений / Интернет протокол). Работа в Интернет осуществляется в режиме реального времени (on-line). Существует ряд протоколов и служб, связанных с TCP/IP и Интернетом. Наиболее распространенными из них являются:

SMTP - протокол приема - передачи электронной почты.

TELNET - протокол для подключения к удаленным системам, присоединенным к МИС общего пользования в режиме удаленного терминала.

FTP - протокол предназначенный для передачи файлов с одного компьютера на другой в вычислительной сети.

DNS - служба сетевых имен используемых для протоколов TELNET, FTP и т.д.

WWW - служба (всемирная паутина), использующая гипертекстовый формат HTML (язык разметки гипертекста), предназначенная для передачи тестовой, графической, аудио и видео информации, а также ссылок на другие документы (гипертекстовые ссылки - выделенные области документа, позволяющие переходить к другому документу, содержащему связанную информацию).

Помимо перечисленных, существует ряд служб и протоколов для удаленной печати, предоставления удаленного доступа к файлам и дискам, работы с распределенными базами данных и т.д.

Основная цель обеспечения информационной безопасности - предотвращение несанкционированного уничтожения, искажения. копирования, блокирования информации в компьютерных и телекоммуникационных системах

* 1. Источники угроз информационной безопасности

Подключение средств вычислительной техники к МИС общего пользования представляет реальную угрозу создания разветвленных систем регулярного несанкционированного контроля информационных процессов и ресурсов, несанкционированного доступа (НСД) в автоматизированные системы (АС).

Информационные вычислительные сети общего пользования являются открытыми системами передачи информации, при работе в которых могут возникнуть следующие основные угрозы безопасности информации:

* проникновение в систему незаконных пользователей, которое происходит вследствие ошибок в конфигурации программных средств (ошибок администрирования), дефектов в средствах обеспечения защиты информации от НСД операционных систем;
* перенос вАС разрушающего программного обеспечения (внедрение программных закладок, вирусов);
* выбор и использование законным пользователем системы неудачных паролей;
* несанкционированная передача служебной информации ограниченного распространения пользователями в МИС общего пользования и т.д.

При непосредственном подключении локальной вычислительной сети к МИС общего пользования любой пользователь МИС имеет возможность:

* получить информацию об адресной структуре сети;
* установить типы и версии используемого сетевого программного обеспечения (сетевое оборудование, операционные системы, прикладные и служебные сервисы);
* получить информацию о пользователях сети;
* попытаться подключиться к информационным ресурсам сети;
* вызвать отказ в обслуживании легальных пользователей.

Кроме явных, то есть непосредственно направленных на сеть организации, внешних угроз информационной безопасности, существуют угрозы, связанные с неумышленным распространением зловредного программного кода самими сотрудниками организации. К зловредному программному коду относят вирусы, троянские программы, «опасные» компоненты прикладных протоколов.

По этим причинам самым опасным с точки зрения безопасности информации является несанкционированное использование модемов, подключенных к рабочим станциям пользователя. Причем подключение не обязательно может использоваться для доступа в Интернет (возможны соединения к серверам других организаций, и к отдельным компьютерам, например домашним).

* 1. Технические средства защиты информации

К техническим средствам защиты информации при работе с информационными сетями общего пользования, в том числе Интернет относятся: системы разграничения прав доступа, межсетевые экраны, системы построения защищенных виртуальных сетей (VirtualPrivateNetwork - VPN), системы обнаружения атак, системы анализа защищенности, системы антивирусной защиты и т.д.

4. Системы разграничения доступа

Система разграничения доступа запрещает посторонним лицам доступ к ресурсам автоматизированной системы и позволяет разграничить права пользователей при работе на компьютере, при этом контролируются права локальных, удаленных и терминальных пользователей.

4.1 Межсетевые экраны (МСЭ)

Межсетевой экран представляет собой локальное (однокомпонентное) или функционально-распределенное средство, реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или выходящей из АС, и

обеспечивает защиту АС посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Межсетевые экраны позволяют осуществить: контроль доступа на межсетевом уровне, протоколирование информационных потоков, сокрытие топологии защищаемой сети, реагирование на несанкционированные действия.

Средствами МСЭ могут быть выявлены следующие виды атак: сканирование сетевых портов, атаки на отказ в обслуживании, изучение топологии внутренней сети, использование слабостей протоколов прикладного уровня, распространение вирусов и спама.

К дополнительным службам МСЭ относятся: средства резервного копирования и восстановления, средства обеспечения высокой доступности, сетевая служба имен.

Основные показатели защищенности МСЭ: управление доступом, идентификация и аутентификация, регистрация событий и оповещение, контроль целостности, восстановление работоспособности.

Межсетевые экраны делятся на пять классов в соответствии с руководящим документом «Средства вычислительной техники. Межсетевые экраны. Защите от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» - М.: Гостехкомиссиия России, 1997.

 4.2.Системы построения защищенных виртуальных сетей

Системы построения защищенных виртуальных сетей позволяют организовать прозрачное для пользователей соединение локальных вычислительных сетей с помощью шифрования.

1. Системы обнаружения атак

К системам обнаружения атак можно отнести: системы обнаружения атак на уровне сети, системы обнаружения атак на уровне хоста. Системы обнаружения атак используют:

* системы обнаружения аномального поведения пользователя (большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора, использование периферийных устройств, которые обычно пользователем не используются и т.д.);
* системы обнаружения злоупотребления (обнаружение уже известной атаки по шаблону или «сигнатуре»).
1. Системы анализа защищенности

Средства анализа защищенности предназначены для поиска в вычислительной технике и ее компонентах различных уязвимостей, которые могут быть использованы злоумышленниками для реализации атак;

5. Организация работы с международными информационными сетями 5.1 Общие требования

АС МИС общего пользования должны быть автономны, не иметь логических и физических каналов (линий) связи с объектами вычислительной техники, на которых ведется обработка информации ограниченного распространения, а также для которых установлены особые правила доступа к информационным ресурсам.

На технических средствах абонентского пункта должно находиться только программное обеспечение, необходимое для его функционирования системы. Владельцам открытых и общедоступных государственных информационных ресурсов необходимо осуществлять их включение в состав объектов международного информационного обмена только при использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации.

Владельцам и пользователям указанных ресурсов необходимо осуществлять размещение технических средств, подключаемых к открытым информационным системам, сетям и сетям связи, используемым при международном информационном обмене, включая сеть "Интернет", вне помещений, предназначенных для ведения закрытых переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну.

 5.1Резервное копирование

При размещении информации в сетях общего пользования, необходимо иметь копию такой информации, для ее восстановления в случае разрушения, изменения или блокирования по причине несанкционированного доступа либо неисправности оборудования. Также необходимо иметь резервную копию системы для восстановления информации в случае ее разрушения.

1. Аппаратно - программная защита

Для фильтрации входящих и исходящих сообщений, а также обнаружения атак, рекомендуется использовать межсетевые экраны.

Для работы с открытыми информационными ресурсами в режиме реального времени (on-line) как правило, используют технологию VPN. Для передачи информации конфиденциального характера по открытым каналам связи необходимо использовать сертифицированные средства криптографической защиты.

Программное обеспечение, устанавливаемое наАС МИС общего пользования, должно быть сертифицировано и иметь все последние обновления.

1. Организационные меры

Приказом по предприятию, подразделению, учреждению, организации назначаются должностные лица, ответственные за эксплуатацию АС МИС, допущенные к работам в МИС общего пользования (в том числе администратор АС МИС, должностные лица, имеющие право подписи документов для отправки по МИС общего пользования, должностные лица, ответственные за прием/отправку электронных сообщений и т.д.).

Пользователь АС МИС обязан:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;

знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемых на персональных компьютерах;

хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему), а также информацию о системе защиты установленной на АС;

Администратор АС МИС обязан:

перед работой пользователей в МИС обеспечить обновление антивирусных баз;

после окончания работы проверить технические средства на наличие/отсутствие вредоносного кода и целостность АС (запрещается использование АС при отключенных или неисправных средствах защиты информации).

Администратор обеспечивает выдачу аутентификаторов (имя пользователя/электронный адрес) и идентификаторов (пароль) пользователя, а также регулярную смену идентификаторов. В случае прекращения полномочий пользователя по работе с МИС (перевод на другую должность, не предусматривающую работу с МИС или увольнение), администратор удаляет учетную запись пользователя из АС МИС.

Администратор обеспечивает ведение журнала приема-передачи информации средствами МИС на бумажных или электронных носителях, который должен содержать следующие обязательные поля: дата работы в сети, ФИО пользователя, время (продолжительность) работы в сети, подпись (в случае ведения журнала на бумажном носителе) или аутентификатор (при ведении электронного журнала). Данная информация используется для сверки времени работы в сети со счетом предъявленным организацией

предоставляющей услуги связи с МИС, и выявления злоупотреблений работы в сети, а также для обнаружения факта компрометации пароля пользователя сети.

Пользователи, работающие на АС МИС общего пользования, обязаны: знать порядок входа в МИС общего пользования и регистрации в сети; знать данную инструкцию;

знать правила работы со средствами защиты информации установленными на АС; передачу документированной информации, производить только по письменному разрешению должностного лица, имеющего право подписи документов для отправки по МИС общего пользования, и после учета в несекретном делопроизводстве;

материальные носители информации с записанной на них входящей документированной информации полученной в процессе работы с информационными ресурсами МИС общего пользования передавать для учета в несекретное делопроизводство;

при пользовании электронной почтой запрещается передача сведений, содержащих конфиденциальную информацию без применения специальных мер защиты (сертифицированных средств криптографической защиты информации);

запрещается копирование или распространение информации с нарушением авторских прав или условий программных лицензий;

запрещается распространение противозаконных материалов;

С целью предотвращения заполнения почты ненужной почтовой (рекламной и др.) информацией - спамом не рекомендуется размещать адрес своего электронного ящика на досках (доски объявлений или BBS) объявлений. Для фильтрации данных сообщений необходимо использование белого и черного списка для настройки почтовой службы, а также сообщить о наличии спама администратору сети, провайдеру.

Ежемесячно необходимо проверять фактически отработанное время работы в сети Интернет со счетом, представленным провайдером.

5.4 Антивирусная защита

АС МИС общего пользователя оснащаются, в обязательном порядке, антивирусным программным обеспечением, обновление антивирусной базы которого производится непосредственно перед каждым началом работы. Антивирусное программное обеспечение настраивается на проверку всех файлов без исключения. При использовании съемных накопителей информации для передачи информации, каждый из них должен быть проверен на отсутствие вредоносного программного обеспечения. АС МИС общего пользования регулярно, не реже одного раза в неделю, проверяются на отсутствие вредоносного программного кода.

При отправке электронных сообщений необходимо заполнять поле тема. Не рекомендуется открывать для чтения почтовые сообщения, адресат которых неизвестен или почтовое отправление носит подозрительный характер (реклама или запрос информации неизвестной фирмы, спам, и т.д.)

Если обнаружено, что почтовое отправление, пришедшее от адресата, заражено вредоносным кодом, администратору необходимо:

срочно принять все меры по предотвращению дальнейшего распространения заражения путем прекращения приема передачи сообщений данной АС МИС;

провести сканирование и лечение системы антивирусными средствами (при необходимости обновить базы данных антивирусного программного обеспечения);

отметить данный факт в журнале учета с указанием названия вредоносного программного обеспечения и адресата, от которого оно получено;

поставить в известность руководителя подразделения Правительства области, а также абонента с которыми осуществлялась связь в период заражения для проверки АС антивирусными средствами.

сообщить адресату о наличии у него заражения, для последующего принятия адресатом срочных мер.

 Запрещается хранение вредоносного кода, на каких либо носителях информации.

При обнаружении вредоносного кода необходимо произвести его удаление антивирусными средствами. Удаление зараженных файлов средствами операционной системы может привести к безвозвратному разрушению информации.

 6. Учет АС, подключенных к международным сетям общего пользования и контроль за обеспечением защиты от несанкционированного доступа

Ведение учета АС, подключенных к МИС общего пользования в Правительстве области, организуется администратором АС МИС.

Сведения о наличии и особенностях функционирования АС МИС общего пользования представляются в отдел защиты информации Правительства области в установленном порядке.

Отдел по защите информации имеет право вносить предложения по порядку и ограничениям использования АС МИС общего пользования, а также выдавать рекомендации и предъявлять дополнительные требования по защите информации от несанкционированного доступа.

Приложение №26

ИНСТРУКЦИЯ

 по организации парольной защиты в ИСПДн администрации Евстратовского сельского поселения

1. Общие положения

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в ИСПДн администрации Евстратовского сельского поселения, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Порядок парольной защиты

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн возлагается на администратора безопасности. Контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности.
2. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:
* длина пароля должна быть не менее 6 символов;
* пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
* при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
* личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

1. Формирование личных паролей пользователей осуществляется централизованно. Ответственность за правильность их формирования и распределения возлагается на администратора безопасности. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других пользователей.
2. Списки паролей пользователей хранятся в сейфе.
3. Полная плановая смена паролей пользователей должна проводиться регулярно.
4. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.
5. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с п.6 настоящей Инструкции.
6. Хранение сотрудником значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале (возможно вместе с персональным носителем информации и идентификатором).
7. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на администратора безопасности.

3. Ответственность

Пользователь и администратор безопасности несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

 Приложение 27

ИНСТРУКЦИЯ

 администратору безопасности ИСПДн Администрации Евстратовского сельского поселения

Общие положения.

Настоящая инструкция определяет основные функции и порядок работы администратора безопасности в технологическом процессе обработки конфиденциальной информации на объекте информатизации ИСПДн администрации с применением комплекса средств защиты информации (СЗИ) от несанкционированного доступа (НСД) Dallas Lock и VIP NET CUSTOM.

В процессе выполнения своих служебных обязанностей администратор безопасности должен выполнять требования нормативных документов по защите информации и требова­ния эксплуатационной документации на комплекс Dallas Lock и YIP NET CUSTOM.

1.**Функции администратора безопасности.**

1. Администратор безопасности обязан выполнять начальную установку и настройку ком­плекса СЗИ НСД на ПЭВМ объекта информатизации.
2. Администратор обязан вести учет электронных идентификаторов комплексов СЗИ НСД, выполнять действия по их регистрации на ПЭВМ, организовывать их выдачу пользователям и периодически контролировать их наличие.
3. Администратор безопасности обязан проводить работы по генерации и регулярной сме­не паролей пользователей.
4. Администратор безопасности обязан выполнять действия по настройке комплексов СЗИ НСД на ПЭВМ объекта информатизации в соответствии с утвержденными правилами раз­граничения доступа (матрицей доступа).
5. Администратор безопасности обязан осуществлять оперативный контроль над функцио­нированием комплекса СЗИ НСД на ПЭВМ объекта информатизации, проводить его перио­дическое тестирование и осуществлять контроль целостности резервных копий программно­го обеспечения комплекса на носителях.
6. Администратор безопасности обязан проводить проверки целостности программного обеспечения.
7. Администратор безопасности обязан осуществлять постоянный контроль над соблюде­нием операторами (пользователями) технологии обработки конфиденциальной информации, анализировать содержимое регистрационных журналов, формируемых комплексами СЗИ НСД и принимать конкретные меры по выявленным нарушениям.
8. Администратор безопасности обязан организовывать и контролировать проведение ра­бот по ремонту, наладке и сервисному обслуживанию ПЭВМ и вспомогательных техниче­ских средств объекта информатизации.

 Администратор безопасности обязан контролировать сохранность и целостность эта тон­ных копий программного обеспечения.

1. Администратор безопасности обязан оказывать методическую и консультационную помощь операторам (пользователям) объекта информатизации в процессе эксплуатации комплексов СЗИ НСД.

2.УСТАНОВКА И НАСТРОЙКА КОМПЛЕКСА СЗИ НСД

1. Установка (повторная установка) комплексов СЗИ НСД выполняется в следующих си­туациях:
* на этапе ввода в действие объекта информатизации;
* в случае выхода из строя накопителей с конфиденциальной информацией;
* в случае возникновения сбойных и аварийных ситуаций, повлекших нарушения в работе программного обеспечения (ПО) ПЭВМ;
* в случае ввода новых ПЭВМ в состав объекта информатизации.
1. Установка комплекса СЗИ НСД на ПЭВМ объекта информатизации должна выполнять­ся администратором безопасности в строгом соответствии с инструкциями, приведенными в эксплуатационной документации.
2. Установка ПО комплекса СЗИ НСД должна производиться с эталонных носителей (CD- дисков). Перед установкой комплекса ПО ПЭВМ должно быть проверено на отсутствие ви­русного заражения.
3. Регистрация электронных идентификаторов пользователей и установка правил разгра­ничения доступа производится в соответствии с утвержденными правилами разграничения доступа (матрицей доступа). Регистрация дополнительных (не указанных) в матрице доступа пользователей запрещена

3.СОПРОВОЖДЕНИЕ СЗИ НСД В ПРОЦЕССЕ ЭКСПЛУАТАЦИИ

* 1. **Ведение служебной информации** СЗИ НСД

3.1.1**Регистрация пользователей**

1. Действия по регистрации пользователей выполняются администратором безопасно­сти на основании оформленных установленным порядком приказов и распоряжений о до­пуске пользователей к обработке конфиденциальной информации.
2. В соответствии с установленными уровнями полномочий операторов (пользовате­лей) и эксплуатационной документацией на комплекс СЗИ НСД администратор безопасно­сти разрабатывает правила разграничения доступа (ПРД) и оформляет матрицу доступа.
3. На основании утвержденной матрицы доступа администратор безопасности, в соот­ветствии с эксплуатационной документацией выполняет действия по настройке системы за­щиты ПЭВМ от НСД.
4. В процессе регистрации пользователей и настройки системы защиты администратор безопасности должен соблюдать следующие правила:
* все информационные ресурсы, к которым разрешен доступ пользователя (логиче­ские диски, каталоги и файлы) должны быть явно указаны;
* каталогам, в которых планируется размещать конфиденциальную информацию должны быть заранее присвоены соответствующие метки конфиденциальности;
* все запускаемые программы и подгружаемые модули должны быть явно указаны и включены в список контроля при запуске;
* должна быть обеспечена регистрация в системном журнале операций чтения, записи и удаления;
* журнал регистрации должен вестись для всех пользователей;
* должен быть активизирован режим ограничения времени действия пароля по коли­честву попыток неправильного ввода;
* должен быть активизирован режим полного удаления файлов;
* должен быть активизирован режим очистки освобождаемой памяти;
1. доступ к портам ввода-вывода должен быть максимально ограничен.Регистрация электронных идентификаторов пользователей, установка правил разгра­ничения доступа выполняются средствами СЗИ НСД.
2. Контроль целостности файлов системы защиты обеспечивается средствами СЗИ НСД.
3. Контроль файловой системы, в том числе обнаружение изменения и создания новых файлов обеспечивается средствами программы контроля целостности файловой системы СЗИ НСД.
4. По окончании работ по регистрации пользователей администратор безопасности вы­полняет проверки функционирования общесистемной программной среды каждого зареги­стрированного пользователя, тестирует работоспособность комплекса СЗИ НСД. и коррект­ность реализации ПРД.
5. После выдачи идентификаторов каждому пользователю администратор (возможно совместно с пользователем) осуществляет генерацию пароля и контролирует установку па­роля пользователем.
	* 1. **Генерация и смена паролей**
6. Действия по генерации и смене паролей пользователей должны организовываться администратором безопасности.
7. Для организации работ по смене паролей администратор безопасности устанавливает ограничения на время действия пароля.
8. Процедура генерации паролей должна исключать задание в качестве паролей комби­наций критичных с точки зрения их подбора.
9. Смена паролей выполняется, в соответствии с эксплуатационной документацией на комплекс СЗИ НСД.
10. Установленные (новые) пароли администратор безопасности должен лично сообщать каждому конкретному пользователю. Администратор безопасности несет ответственность за разглашение личных паролей пользователей.

**3.1.3Сопровождение ПРД**

1. Администратор безопасности обеспечивает реализацию разрешительной системы доступа в виде наборов правил разграничения доступа к техническим, программным средст­вам и информационным ресурсам формируемых для каждого регистрируемого пользователя.
2. Распределение и изменение прав доступа пользователей к конкретным программам и информационным ресурсам должно осуществляться на основании Заявок.
3. Правила разграничения доступа разрабатываются в соответствии с требованиями разрешительной системы доступа на основании заявок на доступ пользователей и докумен­тально оформляются в виде матрицы доступа или в виде дополнений и изменений матрицы доступа и физически реализуются настройками подсистемы разграничения доступа к объек­там файловой системы.
4. Заявки на доступ пользователей к техническим средствам объекта должны содержать перечень (список) программ и информационных ресурсов, доступ к которым должен быть предоставлен каждому конкретному пользователю с указанием дисков и каталогов, на кото­рых размещены данные ресурсы.

3.2 Оперативный контроль над функционированием СЗИ НСД

1. Администратор безопасности несет ответственность за нормальное функционирова­ние комплекса СЗИ НСД на ПЭВМ объекта информатизации.
2. Администратор безопасности должен осуществлять периодическое тестирование ра­ботоспособности комплекса СЗИ НСД и корректности реализации ПРД.
3. В случае, когда средства комплекса СЗИ НСД отказывают в доступе легальным поль­зователям, администратор безопасности должен анализировать причины отказа в доступе и предпринимать оперативные действия по выявлению возможных нарушений.Администратор безопасности должен предпринимать оперативные действия в случае возникновения внештатных ситуаций при работе ПЭВМ, анализировать причины их возник­новения и предпринимать необходимые меры по восстановлению работоспособности ком­плекса СЗИ НСД и программного обеспечения.
4. Администратор безопасности должен постоянно контролировать уровень защищен­ности информации от НСД и, в случае выявления возможных каналов утечки информации за счет НСД, предпринимать оперативные меры по их устранению за счет изменения парамет­ров настройки подсистемы разграничения доступа комплекса СЗИ НСД.

3.3 Контроль соответствия программной среды эталону

1. Контроль соответствия общесистемной программной среды эталону осуществляется администратором безопасности с использованием средств комплекса. Для этого админист­ратор средствами администрирования формирует для каждого зарегистрированного пользо­вателя списки файлов, входящих в состав общесистемного программного обеспечения, це­лостность которых контролируется и включает режим проверки целостности «до запуска» ОС.
2. Все исполняемые модули (файлы, содержащие исполняемый или интерпретируемый программный код), входящие в состав общесистемной программной среды доступ к кото­рым разрешен конкретному пользователю, должны быть включены в список контроля цело­стности.
3. В случае выявления фактов нарушения целостности компонентов, входящих в состав общесистемного программного обеспечения, администратором безопасности должны пред­приниматься действия по анализу причин таких нарушений и действия по восстановлению данных компонент с эталонных копий.
4. Администратор безопасности должен обеспечивать контроль над сохранностью эта­лонных копий ПО и периодически проверять состояние учтенных носителей, на которых оно расположено.
	1. Приемка и ввод в эксплуатацию программных средств

3.4.1.Администратор безопасности организует и контролирует выполнение работ по уста­новке новых программных средств, включаемых в состав ИСПДн.

* + 1. Перед установкой дистрибутивные носители с новыми программными средствами, вводимыми в состав объекта информатизации, должны быть соответствующим образом про­верены.

3.4.3.Установка новых программных средств допускается только с проверенных носите­лей.

3.4.4.Перед установкой новых программных средств ПЭВМ должна быть физически от­ключена от ИСПДн. Если физическое отключение ПЭВМ не возможно (в силу специфики устанавливаемого ПО), выполнение работ по установке новых программных средств допус­кается только после полного прекращения обработки конфиденциальной информации в ИСПДн.

3.4.5.После выполнения работ по установке новых программных средств администратор безопасности проверяет их работоспособность и средствами администрирования комплекса СЗИ НСД выполняет необходимые действия по их настройке. По результатам выполненных работ оформляется акт приемки нового программного обеспечения и утверждаются допол­нения и изменения матрицы доступа.

3.4.6.Допуск пользователей к работе на ПЭВМ, на которых проводились работы по уста­новке нового программного обеспечения, разрешается только после утверждения акта при­емки и матрицы доступа.

Л

3.5 Контроль за ходом технологического процесса обработки информации

1. Контроль хода технологического процесса обработки информации администратор безопасности осуществляет путем регистрации и анализа действий операторов (пользовате­лей) по системному журналу.
2. Обработка и анализ системных журналов должны осуществляться регулярно, но не реже чем один раз в неделю.
3. В случае выявления нарушений администратор безопасности проводит мероприятия по выявлению виновников и причин нарушения. Результаты расследования доводятся до сведения руководства.
	1. Оказание методической и консультационной помощи пользователям
4. Администратор безопасности организует и проводит инструктаж пользователей пра­вилам применения и эксплуатации комплексов СЗИ НСД и периодически контролирует их знания.
5. Администратор безопасности должен оказывать методическую и консультационную помощь пользователям при применении и эксплуатации комплексов СЗИ НСД.