

**Советский район**

**Ханты-Мансийский автономный округ – Югра**

**Администрация сельского поселения Алябьевский**

|  |
| --- |
| **ПОСТАНОВЛЕНИЕ** |

 « 29» мая 2020 г. № 82

Об утверждении пакета организационно-

распорядительной документации,

регламентирующей вопросы обработки

и защиты персональных данных в

Администрации сельского поселения Алябьевский

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации сельского поселения Алябьевский:

1. Утвердить пакет организационно-распорядительной документации, регламентирующей вопросы обработки и защиты персональных данных в следующем составе:
	1. Положение по обработке и защите персональных данных в Администрации сельского поселения Алябьевский (приложение 1);
	2. Положение об организации и проведении работ в Администрации сельского поселения Алябьевский по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных (приложение 2);
	3. Положение о режиме безопасности в помещениях, предназначенных для обработки и хранения персональных данных в Администрации сельского поселения Алябьевский (приложение 3);
	4. Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных Администрации сельского поселения Алябьевский (приложение 4);
	5. Перечень должностей в Администрации сельского поселения Алябьевский, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (приложение 5);
	6. Инструкция по организации работы с электронными носителями конфиденциальной информации в Администрации сельского поселения Алябьевский (приложение 6);
	7. Инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в Администрации сельского поселения Алябьевский (приложение 7);
	8. Инструкция по организации резервного копирования в информационных системах персональных данных Администрации сельского поселения Алябьевский (приложение 8);
	9. Инструкция по организации парольной защиты Администрации сельского поселения Алябьевский (приложение 9);
	10. Инструкция по организации антивирусной защиты информационных систем персональных данных Администрации сельского поселения Алябьевский (приложение 10);
	11. Инструкция по обработке персональных данных без использования средств автоматизации в Администрации сельского поселения Алябьевский (приложение 11);
	12. Инструкция по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в Администрации сельского поселения Алябьевский (приложение 12);
	13. Руководство администратора информационной безопасности ИСПДн Администрации сельского поселения Алябьевский (приложение 13);
	14. Руководство пользователя по обеспечению безопасности ИСПДн
	в Администрации сельского поселения Алябьевский (приложение 14);
	15. Инструкция ответственного за организацию обработки персональных данных в Администрации сельского поселения Алябьевский (приложение 15);
	16. Инструкция ответственного за обеспечение безопасности персональных данных в информационной системы персональных данных Администрации сельского поселения Алябьевский (приложение 16);
	17. Инструкция ответственного за эксплуатацию информационных систем персональных данных (приложение 17);
	18. Положение о порядке выявления и реагирования на инциденты информационной безопасности в Администрации сельского поселения Алябьевский (приложение 18);
	19. Журнал учёта съемных носителей конфиденциальной информации (персональных данных) в Администрации сельского поселения Алябьевский (приложение 19);
	20. Журнал учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в информационной системе персональных данных Администрации сельского поселения Алябьевский (приложение 20);
	21. Журнал учета инцидентов информационной безопасности в Администрации сельского поселения Алябьевский (приложение 21);
	22. Положение об уничтожении персональных данных, обрабатываемых
	в Администрации сельского поселения Алябьевский (приложение 22);
	23. Правила работы с обезличенными персональными данными Администрации сельского поселения Алябьевский (приложение 23);
	24. Журнал ознакомления служащих, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локально-нормативными актами по защите персональных данных в Администрации сельского поселения Алябьевский (приложение 24).
2. Контроль за исполнением настоящего постановления оставляю за собой.

Глава сельского

поселения Алябьевский Ю.А. Кочурова

Приложение 1

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Положение**

**по обработке и защите персональных данных**

**в Администрации сельского поселения Алябьевский**

* 1. **Общие положения**

1.1. Положение об обработке и защите персональных данных в Администрации сельского поселения Алябьевский (далее Положение) определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в Администрации сельского поселения Алябьевский (далее администрация).

1.2. Настоящее Положение определяет политику администрации как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.3. Настоящее Положение разработано в соответствии с Трудовым кодексом Российской Федерации (далее Трудовой кодекс Российской Федерации), Кодексом Российской Федерации об административных правонарушениях, Федеральным законом
от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее Федеральный закон
«О персональных данных»), Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации»
(далее Федеральный закон «О муниципальной службе в Российской Федерации»), Федеральным законом от 25 декабря 2008 года № 273-ФЗ «О противодействии коррупции» (далее Федеральный закон «О противодействии коррупции»), Федеральным законом
от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее Федеральный закон «Об организации предоставления государственных и муниципальных услуг»), Федеральным законом от 2 мая 2006 года
№ 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (далее Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации»), Федеральным законом от 07 июля 2003 года № 126-ФЗ «О связи», Законом Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» (далее Закон Российской Федерации «О средствах массовой информации»), Указом Президента Российской Федерации от 30 мая 2005 года № 609 «Об утверждении Положения
о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», постановлением Правительства Российской Федерации
от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 06 июля 2008 года № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012 года № 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», распоряжением Правительства Российской Федерации от 26 мая 2005 года
№ 667-р об утверждении формы анкеты, подлежащей представлению в государственный орган гражданином Российской Федерации, изъявившим желание участвовать в конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации.

1.4. Обработка персональных данных в администрации осуществляется с соблюдением принципов и условий, предусмотренных настоящим Положением и законодательством Российской Федерации в области персональных данных.

1. **Принципы и условия обработки персональных данных**

2.1. Обработка персональных данных в Администрации сельского поселения Алябьевский осуществляется на основе следующих принципов:

2.1.1. законности и справедливой основы;

2.1.2. ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;

2.1.3. недопущения обработки персональных данных, несовместимой с целями сбора персональных данных;

2.1.4. недопущения объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

2.1.5. обработки только тех персональных данных, которые отвечают целям их обработки;

2.1.6. соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;

2.1.7. недопущения обработки избыточных персональных данных по отношению
к заявленным целям их обработки;

2.1.8. обеспечения точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;

2.1.9. уничтожения либо обезличивания персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения допущенных нарушений обработки персональных данных, если иное не предусмотрено федеральным законом.

2.2. Обработка оператором персональных данных производится только при наличии хотя бы одного из следующих условий:

2.2.1. обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных либо на основании федерального закона;

2.2.2. обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

2.2.3. обработка персональных данных необходима для исполнения полномочий органов местного самоуправления, участвующих в предоставлении государственных и муниципальных услуг;

2.2.4. обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных;

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

2.2.6. 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;

2.2.7. обработка персональных данных осуществляется в статистических целях, при условии обязательного обезличивания персональных данных;

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

2.2.9. осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законодательством.

2.3. Персональные данные лиц, замещающих должности муниципальной службы, лиц, замещающих должности, не отнесенные к должностям муниципальной службы, и осуществляющих техническое обеспечение деятельности Администрации сельского поселения Алябьевский (далее сотрудники администрации), лиц, замещающих должности руководителей муниципальных учреждений, граждан, претендующих на замещение должностей муниципальной службы и должностей не отнесенных к должностям муниципальной службы, и осуществляющих техническое обеспечение деятельности Администрации сельского поселения Алябьевский и иных граждан, обрабатываются для реализации трудовых отношений в Администрации сельского поселения Алябьевский, в связи с проведением конкурсов на замещение должности муниципальной службы, по формированию кадрового резерва Администрации сельского поселения Алябьевский, резерва управленческих кадров, в целях реализации мер по противодействию коррупции.

2.4. В целях, указанных в пункте 2.2. настоящего Положения, обрабатываются следующие категории персональных данных сотрудников администрации и граждан, претендующих на замещение должностей в администрации:

2.4.1. фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

2.4.2. число, месяц, год рождения;

2.4.3. место рождения;

2.4.4. информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

2.4.5. вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

2.4.6. адрес места жительства (адрес регистрации, фактического проживания) и дата регистрации;

2.4.7. номер контактного телефона или сведения о других способах связи;

2.4.8. реквизиты страхового индивидуального лицевого счета в Пенсионном фонде Российской Федерации (далее СНИЛС);

2.4.9. реквизиты идентификационного номера налогоплательщика (далее ИНН);

2.4.10. реквизиты полиса обязательного медицинского страхования;

2.4.11. реквизиты свидетельства государственной регистрации актов гражданского состояния;

2.4.12. семейное положение, состав семьи; сведения о наличии детей, близких родственниках (в том числе бывших), их возрасте, месте учебы (работы), месте жительства;

2.4.13. сведения о трудовой деятельности (данные о трудовой деятельности с полным указанием должности, структурного подразделения, организации и ее наименования, адреса и телефонов);

2.4.14. сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записей в ней сведений о трудовой (служебной) деятельности;

2.4.15. содержание и реквизиты трудового договора, дополнительных соглашений
к трудовому договору;

2.4.16. отношение к воинской обязанности, воинское звание, состав рода войск, военный билет, приписное свидетельство, сведения о постановке на воинский учет
и прохождении службы в Вооруженных Силах;

2.4.17. сведения о получении профессионального и дополнительного профессионального образования (наименование и год окончания образовательной организации, специальность, направление подготовки и квалификация по документу
об образовании, наименование реквизиты документа об образовании, дата выдачи);

2.4.18. сведения о подготовке кадров высшей квалификации (наименование образовательной организации, год окончания), ученая степень, ученое звание (дата присвоения, номер документа об образовании);

2.4.19. сведения об уровне специальных знаний (работа на компьютере, информация о владении иностранными языками и языками народов Российской Федерации, степень владения);

2.4.20. медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или её прохождению; результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований);

2.4.21. фотография;

2.4.22. сведения о прохождении муниципальной службы, в том числе: дата, основания поступления на муниципальную службу и назначения на должность муниципальной службы, дата, основания назначения, перевода, перемещения на иную должность муниципальной службы, наименование замещаемых должностей муниципальной службы
с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности муниципальной службы, а также сведения о прежнем месте работы;

2.4.23. сведения о пребывании за границей (когда, где, с какой целью);

2.4.24. информация о классном чине муниципальной службы (в том числе дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации), квалификационном разряде государственной гражданской службы (квалификационном разряде или классном чине муниципальной службы);

2.4.25. информация о наличии или отсутствии судимости;

2.4.26. информация об оформленных допусках к государственной тайне;

2.4.27. сведения о государственных наградах, иных наградах и знаках отличия;

2.4.28. сведения о прохождении аттестации и сдаче квалификационного экзамена;

2.4.29. сведения о награждении (поощрении), сведения о взысканиях;

2.4.30. сведения о заработной плате, пенсии, выслуге лет на муниципальной службе;

2.4.31. сведения о дополнительном профессиональном образовании;

2.4.32. информация об отпусках, командировках;

2.4.33. сведения о доходах, расходах, об имуществе и обязательствах имущественного характера лиц, замещающих должность муниципальной службы и членов их семей, сведения о социальных льготах, информация о доходах, выплатах и удержаниях; номера банковских счетов;

2.4.34. сведения об адресах сайтов и (или) страниц сайтов в информационно-коммуникационной сети «Интернет», на которых муниципальный служащий размещал общедоступную информацию, а также данные, позволяющие его идентифицировать

2.4.35. номер расчетного счета;

2.4.36. номер банковской карты;

2.4.37. иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 2.2. настоящего Положения.

2.5. Обработка биометрических персональных данных и специальных категорий персональных данных муниципальных служащих администрации, а также граждан, претендующих на замещение должностей муниципальной службы в администрации, осуществляется без согласия указанных лиц в рамках целей, определенных пунктом
2.1. настоящего Положения, в соответствии с пунктом 2 части 1 статьи 6, частью 2 статьи 11 и в соответствии с подпунктом 2.3. пункта 2 части 2 статьи 10 Федерального закона
«О персональных данных», а также положениями Федерального закона «О муниципальной службе Российской Федерации», Федерального закона «О противодействии коррупции», Трудовым кодексом Российской Федерации.

2.6. Обработка персональных данных сотрудников администрации и граждан, претендующих на замещение должностей в администрации, осуществляется при условии получения согласия указанных лиц в следующих случаях:

2.6.1. при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации;

2.6.2. при трансграничной передаче персональных данных;

2.6.3. при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

2.7. В случаях, предусмотренных пунктом 2.5. настоящего Положения, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

2.8. Обработка персональных данных сотрудников администрации и граждан, претендующих на замещение должностей в администрации, осуществляется отделом (работником) органа местного самоуправления, в обязанности которого входит ведение кадровой работы, (далее - кадровое подразделение) и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных сотрудников администрации и граждан, претендующих на замещение должностей в администрации, осуществляется путем:

2.9.1. получения оригиналов необходимых документов (заявление, трудовая книжка, анкета, иные документы, предоставляемые в кадровое подразделение);

2.9.2. копирования оригиналов документов;

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

2.9.4. формирования персональных данных в ходе кадровой работы;

2.9.5. внесения персональных данных в информационные системы органов местного самоуправления, используемые кадровым подразделением.

2.10. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от сотрудников администрации и граждан, претендующих на замещение должностей в администрации.

2.11. В случае возникновения необходимости получения персональных данных сотрудника администрации у третьей стороны, следует известить об этом сотрудника Администрации заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных.

2.12. Запрещается получать, обрабатывать и приобщать к личному делу сотрудника администрации персональные данные, не предусмотренные пунктом 2.3. настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.13. При сборе персональных данных сотрудник кадрового подразделения, осуществляющий сбор (получение) персональных данных непосредственно от сотрудников администрации, а также граждан, претендующих на замещение должностей
в администрации, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

2.14. Передача (распространение, предоставление) и использование персональных данных сотрудников администрации, а также граждан, претендующих на замещение должностей в администрации, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

1. **Условия и порядок обработки персональных данных субъектов в связи с предоставлением государственных и муниципальных услуг и исполнением государственных и муниципальных функций**

3.1. В администрации обработка персональных данных физических лиц осуществляется в целях предоставления муниципальных услуг и исполнения государственных и муниципальных функций в соответствии с Перечнем муниципальных услуг, оказываемых Администрацией сельского поселения Алябьевский, на основании утвержденных административных регламентов.

3.2. Персональные данные граждан, обратившихся в администрацию лично, а также направивших индивидуальные или коллективные письменные обращения или обращения
в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением заявителей о результатах рассмотрения.

В соответствии с законодательством Российской Федерации в администрации подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан и лиц без гражданства.

3.3. В рамках рассмотрения обращений граждан подлежат обработке следующие персональные данные заявителей:

3.3.1. фамилия, имя, отчество (последнее при наличии);

3.3.2. дата, месяц, год рождения;

3.3.3. место рождения;

3.3.4. адрес регистрации и проживания;

3.3.5. адрес электронной почты;

3.3.6. указанный в обращении контактный телефон;

3.3.7. серия, номер, дата выдачи основного документа, удостоверяющего личность,

и выдавший его орган;

3.3.8. ИНН;

3.3.9. СНИЛС;

3.3.10. иные персональные данные, указанные заявителем в обращении (жалобе),
а также ставшие известными в ходе личного приема или в процессе рассмотрения поступившего обращения.

3.4. Обработка персональных данных, необходимых в связи с предоставлением государственных и муниципальных услуг и исполнением государственных функций, указанных в пункте 3.1. настоящего Положения, осуществляется без согласия субъектов персональных данных в соответствии с пунктом 4 части 1 статьи 6 Федерального закона
«О персональных данных», Федеральными законами «Об организации предоставления государственных и муниципальных услуг», «О порядке рассмотрения обращений граждан Российской Федерации» и иными нормативными правовыми актами и административными регламентами, определяющими предоставление государственных и муниципальных услуг
и исполнение государственных и муниципальных функций в установленной сфере ведения администрации.

3.5. Обработка персональных данных, необходимых в связи с предоставлением государственных и муниципальных услуг и исполнением государственных
и муниципальных функций, указанных в пункте 3.1 настоящего Положения, осуществляется структурными подразделениями администрации, предоставляющими соответствующие государственные и муниципальные услуги и (или) исполняющими государственные и муниципальные функции, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.6. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, обратившихся в администрацию для получения государственной (муниципальной) услуги или в целях исполнения государственной и муниципальной функции, осуществляется путем:

3.6.1. получения оригиналов необходимых документов (заявление);

3.6.2. заверения копий документов;

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

3.6.4. внесения персональных данных в прикладные программные подсистемы администрации.

3.7. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (заявителей).

3.8. При предоставлении государственной (муниципальной) услуги или исполнении государственной и муниципальной функции администрации запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

3.9. При сборе персональных данных уполномоченное должностное лицо Администрации сельского поселения Алябьевский, осуществляющее получение персональных данных непосредственно от субъектов персональных данных, обратившихся за предоставлением государственной (муниципальной) услуги или в связи с исполнением государственной (муниципальной) функции, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

3.10. Передача (распространение, предоставление) и использование персональных данных заявителей (субъектов персональных данных) администрации осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

1. **Порядок обработки персональных данных субъектов персональных данных в информационных системах**

4.1. Сотрудникам Администрации сельского поселения Алябьевский, имеющим право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными инструкциями сотрудников администрации.

Информация может вноситься как в автоматическом режиме, при получении персональных данных с Единого портала государственных услуг или официального сайта Администрации сельского поселения Алябьевский, так и в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

4.2. Обеспечение безопасности персональных данных, обрабатываемых
в информационных системах, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

4.2.1. определение угроз безопасности персональных данных при их обработке
в информационных системах персональных данных;

4.2.2. применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

4.4.3. применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

4.2.4. оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

4.2.5. учет машинных носителей персональных данных;

4.2.6. обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

4.2.7. восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;

4.2.8. установление правил доступа к персональным данным, обрабатываемым
в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;

4.2.9. контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

4.3. Должностное лицо, ответственное за обеспечение информационной безопасности, организует и контролирует ведение учета материальных носителей персональных данных.

4.4. Должностное лицо, ответственное за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных, должно обеспечить:

4.4.1. своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в Администрации сельского поселения Алябьевский;

4.4.2. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

4.4.3. возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

4.4.4. постоянный контроль за обеспечением уровня защищенности персональных данных;

4.4.5. знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

4.4.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

4.4.7. при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;

4.4.8. разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

4.5. Должностное лицо, ответственное за обеспечение функционирования информационных систем персональных данных, принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

4.6. Обмен персональными данными при их обработке в информационных системах персональных данных осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

4.7. Доступ служащих к персональным данным, находящимся в информационных системах персональных данных, предусматривает обязательное прохождение процедуры идентификации и аутентификации.

4.8. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

1. **Обработка персональных данных в рамках межведомственного информационного взаимодействия с применением единой системы межведомственного электронного взаимодействия**

5.1. Администрация сельского поселения Алябьевский в соответствии с законодательством Российской Федерации осуществляет обработку персональных данных в рамках межведомственного электронного информационного взаимодействия в электронном виде с федеральными органами государственной власти с применением единой системы межведомственного электронного взаимодействия (далее СМЭВ).

5.2. Администрация в рамках СМЭВ на основании поступивших межведомственных запросов направляет информацию, включающую персональные данные субъектов, обрабатываемые в администрации в федеральные органы исполнительной власти и региональные органы исполнительной власти Ханты-Мансийского автономного
округа – Югры в соответствии с административными регламентами.

1. **Сроки обработки и хранения персональных данных**

6.1. Сроки обработки и хранения персональных данных сотрудников и граждан, претендующих на замещение должностей в администрации, определяются в соответствии
с Федеральным законом от 22 октября 2004 года № 125-ФЗ «Об архивном деле в Российской Федерации», Приказом Министерства культуры Российской Федерации от 25 августа 2010 года № 558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения» и Сводной номенклатурой дел Администрации сельского поселения Алябьевский.

6.2. Сроки обработки и хранения персональных данных, предоставляемых субъектами персональных данных в администрации в связи с получением государственных (муниципальных) услуг и исполнением государственных (муниципальных) функций, указанных в пункте 3.1. настоящего Положения, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

6.3. Персональные данные граждан, обратившихся в администрации лично, а также направивших индивидуальные или коллективные письменные обращения или обращения
в форме электронного документа, хранятся в течение пяти лет.

6.4. Персональные данные, предоставляемые субъектами на бумажном носителе
в связи с предоставлением государственных (муниципальных) услуг и исполнением государственных (муниципальных) функций, хранятся на бумажных носителях
в структурных подразделениях, к полномочиям которых относится обработка персональных данных в связи с предоставлением государственной услуги или исполнением государственной функции, в соответствии с утвержденными положениями
о соответствующих структурных подразделениях.

6.5. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

6.6. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.

6.7. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители структурных подразделений.

6.8. Срок хранения персональных данных, внесенных в информационные системы персональных данных, указанные в пункте 5.1. настоящего Положения, должен соответствовать сроку хранения бумажных оригиналов.

1. **Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований**

7.1. Органами Администрации сельского поселения Алябьевский осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

7.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании комиссии, состав которой утверждается распоряжением Администрации сельского поселения Алябьевский.

По итогам заседания составляются протокол и Акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами комиссии и утверждается главой сельского поселения Алябьевский.

7.3. Уничтожение документов содержащих персональные данные осуществляется путем сожжения или измельчения, после утверждения Акта. Должностное лицо, ответственное за архивную деятельность, сопровождает документы, содержащие персональные данные, присутствует при процедуре уничтожения документов (сжигание или химическое уничтожение).

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

1. **Рассмотрение запросов субъектов персональных данных или их представителей**

8.1. Сотрудники администрации, граждане, претендующие на замещение должностей, и лица, состоящие с ними в родстве (свойстве), а также граждане, персональные данные которых обрабатываются в Администрации в связи с предоставлением государственных (муниципальных) услуг и осуществлением государственных (муниципальных) функций, имеют право на получение информации, касающейся обработки их персональных данных,
в том числе содержащей:

8.1.1. подтверждение факта обработки персональных данных;

8.1.2. правовые основания и цели обработки персональных данных;

8.1.3. применяемые способы обработки персональных данных;

8.1.4. наименование и место нахождения Администрации, сведения о лицах (за исключением муниципальных служащих), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора или на основании Федерального закона;

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

8.1.6. сроки обработки персональных данных, в том числе сроки их хранения;

8.1.7. порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;

8.1.8. информацию об осуществленной или предполагаемой трансграничной передаче данных;

8.1.9. наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению администрации, если обработка поручена или будет поручена такой организации или лицу;

8.1.10. иные сведения, предусмотренные законодательством Российской Федерации
в области персональных данных.

8.2. Лица, указанные в пункте 8.1. настоящего Положения (далее субъекты персональных данных), вправе требовать уточнения их 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.

8.3. Сведения, указанные в подпунктах 8.1.1.-8.1.10. пункта 8.1. настоящего Положения, должны быть предоставлены субъекту персональных данных оператором
в доступной форме, и 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.

8.4. Сведения, указанные в подпунктах 8.1.1.-8.1.10. пункта 8.1. настоящего Положения, сообщаются субъекту персональных данных или его представителю, а также предоставляется возможность ознакомления с его персональными данными при обращении либо в течение 30 дней с даты получения запроса субъекта персональных данных или его представителя. Запрос должен содержать:

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

8.4.2. сведения, подтверждающие участие субъекта персональных данных
в правоотношениях с администрацией (документ, подтверждающий прием документов на участие в конкурсе на замещение вакантных должностей муниципальной службы, оказание государственной (муниципальной) услуги или осуществление государственной (муниципальной) функции), либо сведения, иным образом подтверждающие факт обработки персональных данных, 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.

8.5. В случае, если сведения, указанные в подпунктах 8.1.1.-8.1.10. пункта 8.1. настоящего Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно 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.

8.6. Субъект персональных данных вправе обратиться повторно или направить повторный запрос в целях получения сведений, указанных в подпунктах 8.1.1.-8.1.10. пункта 8.1 настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 8.5. настоящего Положения, 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 8.4. настоящего Положения, должен содержать обоснование направления повторного запроса.

8.7. Администрация вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 8.5. и 8.6. настоящего Положения. Такой отказ должен быть мотивированным.

8.8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

1. **Лицо, ответственное за организацию обработки персональных данных**

**в администрации**

9.1. Ответственный за организацию обработки персональных данных в Администрации сельского поселения Алябьевский (далее Ответственный за обработку персональных данных) назначается распоряжением Администрации сельского поселения Алябьевский из числа штатных сотрудников в соответствии с распределением обязанностей.

9.2. Ответственный за обработку персональных данных в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящим Положением.

9.3. Ответственный за обработку персональных данных обязан:

9.3.1. организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в администрации
от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

9.3.2. осуществлять внутренний контроль за соблюдением муниципальными служащими требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

9.3.3. доводить до сведения муниципальных служащих положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

9.3.4. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом
и обработкой таких обращений и запросов;

9.3.5. в случае нарушения требований к защите персональных данных, принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

9.4. Ответственный за обработку персональных данных вправе:

9.4.1. иметь доступ к информации, касающейся обработки персональных данных
и включающей:

9.4.1.1. цели обработки персональных данных;

9.4.1.2. категории обрабатываемых персональных данных;

9.4.1.3. категории субъектов, персональные данные которых обрабатываются;

9.4.1.4. правовые основания обработки персональных данных;

9.4.1.5. перечень действий с персональными данными, общее описание используемых способов обработки персональных данных;

9.4.1.6. описание мер, предусмотренных статьями 18.1. и 19 Федерального закона
«О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

9.4.1.7. дату начала обработки персональных данных;

9.4.1.8. срок или условия прекращения обработки персональных данных;

9.4.1.9. сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

9.4.1.10. сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

9.4.2. привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в администрации, иных муниципальных служащих с возложением на них соответствующих обязанностей и закреплением ответственности.

9.5. Ответственный за обработку персональных данных несет ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных в соответствии с положениями законодательства Российской Федерации в области персональных данных.

Приложение 1

к Положению по обработке и защите

персональных данных

в Администрации сельского

поселения Алябьевский

**Типовая форма согласия
на обработку персональных данных субъектов персональных данных**

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

|  |
| --- |
| (фамилия, имя, отчество) |

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

|  |
| --- |
| (вид документа, удостоверяющего личность, серия, номер, когда и кем выдан) |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

проживающий (-ая) по адресу:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

настоящим даю свое согласие на обработку Администрации сельского поселения Алябьевский моих персональных данных и подтверждаю, что, давая такое согласие, я действую своей волей и в своих интересах.

Согласие дается мною для целей:

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

|  |
| --- |
| (цель обработки персональных данных) |

Настоящее согласие предоставляется на осуществление любых действий по обработке моих персональных данных для достижения указанных выше целей, в соответствии
с требованиями, установленными Федеральным законом от 27.07.2006 № 152-ФЗ
«О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами и действует со дня его подписания и до достижения целей обработки персональных данных, указанных в данном согласии, либо до дня отзыва согласия на обработку персональных данных в письменной форме.

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(фамилия, инициалы лица, давшего согласие) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись, дата) |

Приложение 2

к Положению по обработке и защите

персональных данных

в Администрации сельского

поселения Алябьевский

**Типовая форма разъяснения
субъекту персональных данных юридических последствий отказа
представить свои персональные данные**

Мне, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

|  |
| --- |
| (фамилия, имя, отчество) |

разъяснены юридические последствия отказа в предоставлении своих персональных данных Администрации сельского поселения Алябьевский.

В соответствии со статьями 16, 29, 30 Федерального закона от 02.03.2007 № 25-ФЗ
«О муниципальной службе в Российской Федерации», статьями 65, 86 Трудового кодекса Российской Федерации, определен перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с поступлением или прохождением муниципальной службы (работы).

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

На основании статьи 19 Федерального закона от 02.03.2007 № 25-ФЗ
«О муниципальной службе в Российской Федерации», 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 службы (работы).

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(дата) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Ф.И.О. полностью, подпись) |

Приложение 3

к Положению по обработке и защите

персональных данных

в Администрации сельского

 поселения Алябьевский

**Типовое обязательство
служащего, 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, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

|  |
| --- |
| (фамилия, имя, отчество) |

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

|  |
| --- |
|  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(указать должность и наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными мне
в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ
«О персональных данных», я уведомлен (-а) о том, что персональные данные являются конфиденциальной информацией, и я обязан (-а) не раскрывать третьим лицам
и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден (-а) о том, что в случае нарушения данного обязательства буду привлечен (-а) к ответственности в соответствии с законодательством Российской Федерации.

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(фамилия, инициалы лица, давшего согласие) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись, дата) |

Приложение 2

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Положение**

**об организации и проведении работ в Администрации сельского поселения Алябьевский по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных**

* 1. **Общие положения**

1.1. Данное «Положение об организации и проведению работ в Администрации сельского поселения Алябьевский по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных» (далее Положение) разработано в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом Российской Федерации от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями Федеральной службы по техническому и экспортному контролю (далее ФСТЭК России) и Федеральная служба безопасности Российской Федерации (далее ФСБ России) в целях обеспечения безопасности персональных данных (далее ПДн) при их обработке в информационных системах персональных данных (далее ИСПДн).

1.2. Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений
по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн
в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

1.3. При обеспечении безопасности персональных данных в ИСПДн с использованием криптографических средств защиты информации все сотрудники Администрации сельского поселения Алябьевский обязаны выполнять требования, изложенные в документе «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ России 21 февраля 2008 № 149/6/6-622)».

* 1. **Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн**

Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании распоряжения Администрации сельского поселения Алябьевский, и в соответствии со списком лиц допущенных к работе в ИСПДн. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн распоряжением Администрации сельского поселения Алябьевский назначается администратор безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности ответственный за защиту информации;

2.2. Пользователь имеет право в отведенное ему время решать поставленные задачи
в соответствии с полномочиями доступа к ресурсам ИСПДн. Полномочия пользователей
к информационным ресурсам определяются в матрице доступа, утверждаемой распоряжением Администрации сельского поселения Алябьевский. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации.

2.3. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (далее СВТ), входа в систему и все действия при работе
в ИСПДн.

2.4. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

2.5. Запись информации, содержащей ПДн, может, осуществляется пользователем на съемные машинные носители информации, соответствующим образом учтенные в Журнале учета съемных носителей конфиденциальной информации (персональных данных) (приложение 19 к распоряжению).

2.6. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов
с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

2.7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей
в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

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

знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;

хранить в тайне свой пароль (пароли). В соответствии с п.п. 8.5., 8.6. данного Положения и с установленной периодичностью менять свой пароль (пароли);

хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

выполнять правила антивирусной защиты в полном объеме.

Немедленно известить ответственного за защиту информации и (или) администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данным защищаемым СВТ;

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев
в системе электроснабжения;

некорректного функционирования установленных на компьютеры технических средств защиты;

непредусмотренных отводов кабелей и подключенных устройств.

Пользователю категорически запрещается:

использовать компоненты программного и аппаратного обеспечения ПЭВМ
в неслужебных целях;

самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.

2.8. Администратор безопасности (а при его отсутствии - ответственный за защиту информации) обязан:

знать состав основных и вспомогательных технических систем и средств (далее ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее ПО) в ИСПДн;

контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

производить необходимые настройки подсистемы управления доступом установленных в ИСПДн средств защиты информации (далее СЗИ) от НСД и сопровождать их в процессе эксплуатации, при этом:

реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;

своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;

проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;

контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;

обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;

вводить в базу данных СЗИ от НСД описания событий, подлежащих регистрации в системном журнале;

проводить анализ системного журнала для выявления попыток НСД к защищаемым ресурсам не реже одного раза в 10 дней;

организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации. Сопровождать подсистемы обеспечения целостности информации в ИСПДн;

периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;

восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;

контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;

периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования:

проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований
по размещению и использованию технических средств ИСПДн;

контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;

обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях
с составлением соответствующего акта);

присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

вести «Журнал учёта съемных носителей конфиденциальной информации (персональных данных) Администрации сельского поселения Алябьевский» (приложение 19
к распоряжению);

вести «Журнал учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в информационной системе персональных данных Администрации сельского поселения Алябьевский» (приложение 20
к распоряжению);

вести «Журнал учета инцидентов информационной безопасности Администрации сельского поселения Алябьевский» (приложение 21 к распоряжению);

вести «Журнал ознакомления служащих, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локально-нормативными актами по защите персональных данных в Администрации сельского поселения Алябьевский» (приложение 24 к распоряжению);

поддерживать установленный порядок проведения антивирусного контроля согласно требований настоящего Положений в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

докладывать ответственному за защиту информации, ответственному за эксплуатацию ИСПДн о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

2.9. Администратор безопасности и ответственный за защиту информации имеют право:

требовать от сотрудников - пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;

требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

* 1. **Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации**

3.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

3.2. К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в журнале учета носители.

3.3. Администратор безопасности обязан осуществлять периодическое резервное копирование конфиденциальной информации.

3.4. Еженедельно, по окончанию работы с конфиденциальными документами (содержащими персональные данные) на компьютере, пользователь, при отсутствии администратора, обязан создавать резервную копию конфиденциальных документов на зарегистрированный носитель (жёсткий магнитный диск (далее ЖМД), гибкий магнитный диск (далее ГМД), CD, DVD - диски, USB накопитель, другие), создавая тем самым резервный электронный архив конфиденциальных документов.

3.5. Носители информации (ЖМД, ГМД, CD-ROM, USB накопитель, другие), предназначенные для создания резервной копии и хранения конфиденциальной информации выдаются установленным порядком руководителем, ответственным за защиту информации и (или) администратором. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности, или руководителю, или ответственному за защиту информации.

3.6. Перед резервным копированием пользователь или администратор безопасности обязан проверить электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель) на отсутствие вирусов.

3.7. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль в соответствии с п. 7 настоящего Положения.

3.8. Запрещается запись посторонней информации на электронные носители (ЖМД, ГМД, CD-ROM, USB накопитель и другие) резервной копии.

3.9. Порядок создания резервной копии:

вставить в компьютер зарегистрированный электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель, другие) для резервного копирования;

выбрать необходимый каталог (файл) для создания резервного архива;

при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;

выполнить процедуру создания резервной копии;

произвести копирование на отчуждаемый носитель;

произвести отключение отчуждаемого носителя и, создав необходимые записи в Журнале учета процедур резервного копирования (приложение 28 к распоряжению) и Журнале учёта съемных носителей конфиденциальной информации (персональных данных) (приложение 19 к распоряжению) убрать носитель в хранилище.

3.10. Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище совместно с ключевой и аутентифицирующей информацией.

3.11. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

3.12. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

3.13. При необходимости ремонта технических средств, с них удаляются опечатывающие пломбы, изымаются носители конфиденциальной информации и по согласованию с администратором безопасности, ответственным за защиту информации и представителем организации, проводившей аттестацию, оборудование передается
в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа
с использованием неисправных технических средств запрещается.

3.14. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

3.15. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных. Оценку эффективности данных средств защиты должен выполнять сотрудник организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

3.16. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

3.17. Ответственность за проведение резервного копирования в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора безопасности.

3.18. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора безопасности.

3.19. Ответственность за проведение мероприятий по восстановлению средств защиты информации возлагается администратора безопасности.

* 1. **Порядок контроля защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий**

4.1. Контроль защиты информации в ИСПДн - комплекс организационных
и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

4.2. Основными задачами контроля являются:

проверка организации выполнения мероприятий по защите информации в подразделениях Администрации сельского поселения Алябьевский, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

выявление демаскирующих признаков объектов ИСПДн;

уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

4.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн Администрации сельского поселения Алябьевский и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

4.4. В ходе контроля проверяются:

соответствие принятых мер по обеспечению безопасности персональных данных (далее ОБ ПДн);

своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;

полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

эффективность применения организационных и технических мероприятий по защите информации;

устранение ранее выявленных недостатков.

Кроме того, могут проводиться необходимые измерения и расчеты, приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии ФСТЭК России.

4.5. Основными видами технического контроля являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

4.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор безопасности докладывает руководителю для принятия ими решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

4.7. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя или ответственного за защиту информации проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора безопасности. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования Глава принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

4.8. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов Администрации проводятся, как правило, силами администратора безопасности и (или) ответственного за защиту информации, в соответствии с утвержденным планом или по согласованию с руководителем.

4.9. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора безопасности, ответственного за защиту информации, ответственного за эксплуатацию объекта. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

4.10. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в «Аттестате соответствия» требованиям по безопасности персональных данных.

4.11. В ходе обследования проверяется:

соответствие текущих условий функционирования обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;

соблюдение организационно-технических требований помещений, в которых располагается ИСПДн;

сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;

соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в настоящем положении;

выполнение требований по защите информационных систем от несанкционированного доступа;

выполнение требований по антивирусной защите.

4.12. Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в выделенных и защищаемых помещениях, а также других нарушений и способов возникновения каналов утечки информации необходимо:

тщательно осмотреть мебель, сувениры (особенно иностранного производства), оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы и т.д.;

вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;

проверить качество установки стеклопакетов оконных проемов;

провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры), при необходимости для проведения данных видов работ могут привлекаться организации, имеющие соответствующие лицензии ФСБ России.

4.13. Государственный контроль состояния защиты информации осуществляется Федеральной службы по техническому и экспортному контролю России и Федеральной службой безопасности России в рамках их полномочий в соответствии с действующим законодательством Российской Федерации. Доступ представителей указанных федеральных органов исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, а также документа установленной формы на право проведения проверки.

* 1. **Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных**

5.1. Перед началом работы в ИСПДн пользователи должны ознакомиться
с положениями законодательства Российской Федерации и локально-нормативными актами по защите персональных данных в Администрации сельского поселения Алябьевский под роспись в «Журнале ознакомления служащих, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локально-нормативными актами по защите персональных данных в Администрации сельского поселения Алябьевский» (приложение 24 к распоряжению).

5.2. Пользователи должны продемонстрировать администратору безопасности и (или) ответственному за защиту информации наличие необходимых знаний и умений для выполнения требований настоящего Положения.

5.3. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего положения, к работе в ИСПДн не допускаются.

5.4. Ответственным за организацию обучения и оказание методической помощи
в Администрации сельского поселения Алябьевский является администратор безопасности.

Администратор должен организовывать совещательные мероприятия и инструктажи, направленные на:

разъяснение сотрудникам требований организационно-распорядительной документации и правил работы в ИСПДн;

повышение уровня их квалификации в области информационной безопасности и применения штатных средств защиты информации;

разъяснение порядка использования съёмных носителей информации.

Инструктажи должны проводиться периодически (не реже одного раза в три месяца),
а также при возникновении нештатных ситуаций.

5.5. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИСПДн, организаций-лицензиатов ФСТЭК России и ФСБ России.

5.6. К работе в ИСПДн допускаются только сотрудники прошедшие первичный инструктаж ОБ в ИСПДн и показавшие твердые теоретические знания и практические навыки, о чём делается соответствующая запись в Журнале учёта допуска к работе
в ИСПДн.

5.7. Администратор безопасности должен иметь профильное образование (либо дипломы о повышении квалификации) в области защиты информации. Рекомендуется прохождение администратором специализированных курсов по администрированию средств защиты информации, используемых в ИСПДн.

* 1. **Правила антивирусной защиты**

6.1. Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения (ПО), компьютерных вирусов и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение. Настоящие правила распространяются на все объекты ИСПДн Администрации сельского поселения Алябьевский.

6.2. К использованию на компьютерах допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

6.3. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности.

6.4. Администратор безопасности осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

6.5. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

6.6. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Настройки средств антивирусной защиты должны быть выполнены в соответствии
с требованиями безопасности персональных данных определенного для данной ИСПДн класса. Настройку средств антивирусной защиты выполняет администратор безопасности.

6.7. Файлы, помещаемые в электронный архив на магнитных носителях, должны
в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

6.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности должна быть выполнена антивирусная проверка ИСПДн.

6.9. На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

6.10. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

приостановить обработку данных в ИСПДн;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные подразделения, использующие эти файлы в работе;

совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;

провести лечение или уничтожение зараженных файлов.

6.11. Ответственность за организацию антивирусного контроля в ИСПДн
в соответствии с требованиями настоящего Положения возлагается на ответственного
за защиту информации.

6.12. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

* 1. **Правила парольной защиты**

7.1. Данные правила регламентируют организационно-технические мероприятия
по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн,
а также контроль действий пользователей при работе с паролями.

7.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора безопасности.

7.3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ОВТ самостоятельно с учетом следующих требований:

пароль должен быть не менее 6 символов;

в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, \*, % и т.п.);

символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

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 предыдущих;

пользователь не имеет права сообщать личный пароль другим лицам.

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

7.4. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение руководителю структурного подразделения. Запечатанные конверты (пеналы) с паролями исполнителей должны храниться в недоступном месте у руководителя структурного подразделения.

7.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.

7.6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри администрации и т.п.) должна производиться администратором безопасности (либо новым постоянным пользователем) немедленно после окончания последнего сеанса работы данного пользователя с системой на основании указания руководителя структурного подразделения.

7.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри администрации и другие обстоятельства) администратора безопасности.

7.8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.

7.9. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности.

**8. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн**

8.1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновлении, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций
в работе ИСПДн.

8.2. Все изменения конфигураций технических и программных средств ИСПДн должны производиться только на основании заявок ответственного за эксплуатацию конкретного ИСПДн.

Перед проведением работ по внесению изменений в состав технических и программных средств ИСПДн необходимо согласовать возможность данных изменений с органом, производившим работы по аттестации. При возможности осуществления подобных изменений представители органа по аттестации осуществляют надзор за всеми проводимыми работами. Проведение работ по изменению состава технических и программных средств ИСПДн без согласования с органом по аттестации автоматически прекращает действие выданного Аттестата.

8.3. Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ИСПДн предоставляется:

в отношении системных и прикладных программных средств - администратору безопасности по согласованию с органом по аттестации, проводившим аттестацию данной ИСПДн;

в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты - администратору безопасности по согласованию с органом по аттестации, проводившим аттестацию данной ИСПДн.

8.4. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных сотрудников и подразделений, запрещено.

8.5. Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн инициируется заявкой ответственного за эксплуатацию ИСПДн.

8.6. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

установка (развертывание) на компьютер (-ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн;

обновление (замена) на компьютере (-ах) программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);

удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

8.7. Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

8.8. Заявку ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает Глава, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

После чего заявка передается администратору безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера указанного в заявке ИСПДн.

8.9. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором безопасности по согласованию
с органом по аттестации, проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

8.10. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

8.11. Установка и обновление ПО (системного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, прикладного ПО -
с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

8.12. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

8.13. После установки (обновления) ПО, администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в «Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн», делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте».

8.14. Формат записей «Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» устанавливается распоряжением администрации.

8.15. При возникновении ситуаций, требующих передачи технических средств
в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за защиту информации, который в свою очередь связывается
с сотрудниками органа по аттестации и в дальнейшем действует согласно их инструкций.
В данном случае администратор безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИСПДн и «Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» у ответственного за защиту информации.

8.16. Копии заявок могут храниться у администратора безопасности:

для восстановления конфигурации ИСПДн после аварий;

для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;

для проверки правильности установки и настройки средств защиты ИСПДн.

8.17. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора безопасности и сотрудника ответственного за эксплуатацию данной ИСПДн.

8.18. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном компьютере.

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

8.20. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн. Форма заявки приведена ниже.

В заявке указывается:

содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);

должность (с полным наименованием структурного подразделения), фамилия, имя и отчество сотрудника;

имя пользователя (учетной записи) данного сотрудника;

полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

8.21. Заявку рассматривает Глава, визируя её, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем подписывает задание администратору безопасности на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

8.22. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 360 дней.

8.23. После внесения изменений в списки пользователей администратор безопасности должен обеспечить настройки средств защиты соответствующие требованиям безопасности указанной ИСПДн. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя - администратор безопасности.

8.24. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное (-ые) значение (-ия) пароля (-ей), которое (-ые) он обязан сменить при первом же входе в систему.

8.25. Исполненные заявка и задание (за подписью администратора безопасности) передаются руководителю на хранение.

Они могут впоследствии использоваться:

для восстановления полномочий пользователей после аварий ИСПДн;

для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;

для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

1. **Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических**

9.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации.

9.2. Технические средства защиты информации являются важным компонентом ОБ ПДн.

9.3. Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ, обязательных для исполнения, как сотрудниками обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

9.4. Право проверки соблюдения условий использования средств защиты информации имеют:

глава (заместитель);

ответственный за защиту информации;

администратор безопасности.

9.5. Пользователю ИСПДн категорически запрещается:

обрабатывать конфиденциальную информацию с отключенными СЗИ;

менять настройки СЗИ.

9.6. Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

9.7. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлено нарушение требования п. 10.5. то вступает в силу п.п. 3.7., 3.8. данного Положения.

9.8. Криптографические средства защиты информации (далее – КСЗИ) должны использоваться в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими. Поэкземплярный учет СКЗИ ведет администратор безопасности в «Журнале учета средств криптографической защиты информации» (приложение 20 к распоряжению) и «Журнале учета ключевых носителей» (приложение 21 к распоряжению).

1. **Порядок охраны и допуска посторонних лиц в защищаемые помещения**

10.1. Настоящее Положение устанавливает порядок охраны (сдачи под охрану) защищаемых помещений ИСПДн.

10.2. Должны быть предусмотрены: контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации, особенно
в нерабочее время.

Ответственный за обеспечение безопасности информации должен:

поддерживать в актуальном состоянии списки сотрудников допущенных к вскрытию помещений, списки допущенных в помещения и списки пользователей ИСПДн;

периодически контролировать отсутствие в помещениях ИСПДн лиц, не имеющих права находиться в данном помещении;

периодически контролировать корректность организации доступа в помещения и хранилища носителей информации (надёжность замков, порядок выдачи ключей сотрудникам и т.п.).

10.3. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

10.4. При отсутствии сотрудников, ответственных за вскрытие (сдачу под охрану) помещений, данные помещения могут быть вскрыты комиссией, созданной на основании распоряжения, о чем составляется акт.

10.5. При закрытии помещений и сдачей их под охрану сотрудники, ответственные за помещения, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержится конфиденциальная информация, убираются для хранения в опечатываемый сейф (металлический шкаф).

10.6. Помещение сдается под охрану следующим образом:

закрывает помещение;

сдается помещение под подпись с указанием даты и времени сдачи под охрану.

10.7. Сотрудник, имеющий право на вскрытие помещений:

получает на посту охраны ключи от помещения под подпись в Журнале с указанием даты и времени;

производит запись в Журнале о вскрытии помещения с указанием фамилии и времени;

производит проверку исправность запоров;

вскрывает помещение.

10.8. При обнаружении нарушений целостности оттисков печатей, повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и(или) ответственному за защиту информации.

Одновременно принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается.

10.9. Ответственный за обеспечение безопасности информации и администратор безопасности организуют проверку ИСПДн на предмет несанкционированного доступа
к конфиденциальной информации и наличие документов и машинных носителей информации.

1. **Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации**

11.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые
из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускается стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим порядком.

11.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные
в сертифицированные средства защиты информации).

11.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

11.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

11.5. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

11.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию ИСПДн, ответственный за защиту информации, администратор безопасности.

1. **Порядок передачи и хранения персональных данных**

12.1. При передаче персональных данных граждан Оператор должен соблюдать следующие требования:

12.1.1. Не сообщать персональные данные третьей стороне без письменного согласия гражданина, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом.

12.1.2. Предупредить лиц, получивших персональные данные гражданина, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные, обязаны соблюдать режим конфиденциальности. С данными лицами Оператор подписывает Соглашение о конфиденциальности.

Данное Положение не распространяется на обмен персональными данными граждан
в порядке, установленном федеральными законами.

12.1.3. Осуществлять передачу персональных данных граждан в пределах администрации в соответствии с настоящим Положением.

12.1.4. Разрешать доступ к персональным данным граждан только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы им для выполнения конкретной функции.

12.1.5. Передавать персональные данные граждан их представителям в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции.

12.2. Хранение и использование персональных данных граждан:

12.2.1. Персональные данные граждан обрабатываются и хранятся в Администрации сельского поселения Алябьевский.

12.2.2. Персональные данные граждан могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде.

12.3. При получении персональных данных не от гражданина (за исключением случаев, если персональные данные были предоставлены на основании федерального закона или если персональные данные являются общедоступными) Оператор до начала обработки таких персональных данных обязан предоставить гражданину следующую информацию:

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

цель обработки персональных данных и ее правовое основание;

предполагаемые пользователи персональных данных;

установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» права субъекта персональных данных.

1. **Порядок взаимодействия с информационными сетями общего пользования**

13.1. Данный порядок определен, исходя из требований руководящего документа Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», настоящего документа, а также следующих основных угроз безопасности информации, возникающих при взаимодействии с информационными сетями общего пользования:

несанкционированного доступа к информации, хранящейся и обрабатываемой во внутренних локально-вычислительных сетях (далее ЛВС) (серверах, рабочих станциях) или на автономных ПЭВМ, как из международных сетей Интернет (далее Сети), так и из внутренних ЛВС;

несанкционированного доступа к коммуникационному оборудованию (маршрутизатору, концентратору, мосту, мультиплексору, серверу, Web/Proxy серверу), соединяющему внутренние ЛВС администрации с Сетями;

несанкционированного доступа к данным (сообщениям), передаваемым между внутренними ЛВС и Сетями, включая их модификацию, имитацию и уничтожение;

заражения программного обеспечения компьютерными "вирусами" из Сетей, как посредством приема «зараженных» файлов, так и посредством E-mail, апплетов языка JAVA и объектов ActiveX Control;

внедрения программных закладок с целью получения НСД к информации, а также дезорганизации работы внутренней ЛВС и ее взаимодействия с Сетями;

несанкционированной передачи защищаемой конфиденциальной информации ЛВС
в Сеть;

возможности перехвата информации внутренней ЛВС за счет побочных электромагнитных излучений и наводок от основных технических средств, обрабатывающих такую информацию.

13.2. Подключение к Сети абонентского пункта (далее АП) осуществляется по решению Главы на основании соответствующего обоснования.

13.3. Обоснование необходимости подключения АП к Сети должно содержать:

наименование Сети, к которой осуществляется подключение, и реквизиты организации-владельца Сети и провайдера Сети;

состав технических средств для оборудования АП;

предполагаемые виды работ и используемые прикладные сервисы Сети (E-Mail, FTP, Telnet, HTTP и т.п.) для АП в целом и для каждого абонента, в частности;

режим подключения АП и абонентов к Сети (постоянный, в т.ч. круглосуточный, временный);

состав общего и телекоммуникационного программного обеспечения АП и абонентов (ОС, клиентские прикладные программы для сети - Browsers и т.п.);

число и перечень предполагаемых абонентов (диапазон используемых IP - адресов);

меры и средства защиты информации от НСД, которые будут применяться на АП, организация-изготовитель, сведения о сертификации, установщик, конфигурация, правила работы с ними;

перечень сведений конфиденциального характера, обрабатываемых (хранимых) на АП, подлежащих передаче и получаемых из Сети.

13.4. Подключение к Сети АП, представляющих собой внутренние (локальные) вычислительные сети, на которых обрабатывается информация, не разрешенная
к открытому опубликованию, разрешается только после установки на АП средств защиты информации от НСД.

13.5. Подключение ЛВС предприятия (учреждения) к Сети должно осуществляться через средства разграничения доступа в виде межсетевого экрана (далее МЭ) (Firewall, Брандмауэр). Не допускается подключение ЛВС к Сети в обход МЭ. МЭ должны быть сертифицированы по требованиям безопасности информации.

13.6. Доступ к МЭ, к средствам его конфигурирования должен осуществляться только Администратором безопасности. Средства удаленного управления МЭ должны быть исключены из конфигурации.

13.7. На технических средствах АП должно находиться программное обеспечение только в той конфигурации, которая необходима для выполнения работ, заявленных в обосновании необходимости подключения АП к Сети (обоснование может корректироваться в установленном порядке).

13.8. Установку программного обеспечения, обеспечивающего функционирование АП, должен выполнять только Администратор безопасности.

13.9. Устанавливаемые межсетевые экраны должны соответствовать классу защищаемого АП и отвечать требованиям руководящего документа Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа
к информации».

13.10. СЗИ НСД, устанавливаемая на автономную ПЭВМ, рабочие станции и серверы внутренней ЛВС предприятия при обработке на них конфиденциальной информации, должна осуществлять:

идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;

контроль доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;

регистрацию доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС, включая попытки НСД;

регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов).

При этом СЗИ НСД должна запрещать запуск абонентом произвольных программ, не включенных в состав программного обеспечения АП.

Модификация конфигурации программного обеспечения АП должна быть доступна только со стороны Администратора безопасности.

Средства регистрации и регистрируемые данные должны быть недоступны для абонента.

СЗИ НСД должна быть целостной, т.е. защищенной от несанкционированной модификации и не содержащей путей обхода механизмов контроля.

Тестирование всех функций СЗИ НСД с помощью специальных программных средств должно проводится не реже одного раза в год.

13.11. В целях контроля за правомерностью использования АП и выявления нарушений требований по защите информации:

осуществлять анализ принимаемой из Сети и передаваемой в Сеть информации, в том числе на наличие «вирусов»;

проводить постоянный контроль информации, помещаемой на Web-серверы предприятия.

13.12. Абоненты Сети обязаны:

знать порядок регистрации и взаимодействия в Сети;

знать инструкцию по обеспечению безопасности информации на АП;

знать правила работы со средствами защиты информации от НСД, установленными на АП (серверах, рабочих станциях АП);

уметь пользоваться средствами антивирусной защиты;

после окончания работы в Сети проверить свое рабочее место на наличие «вирусов».

13.13. Входящие и исходящие сообщения (файлы, документы), а также используемые при работе в Сети носители информации учитываются в журналах делопроизводства.

13.14. При работе в Сети категорически запрещается:

подключать технические средства (серверы, рабочие станции), имеющие выход в Сеть, к другим техническим средствам (сетям), не определенным в обосновании подключения
к Сети;

изменять состав и конфигурацию программных и технических средств АП без санкции администратора и аттестационной комиссии;

производить отправку данных без соответствующего разрешения;

использовать зарегистрированные носители информации на рабочих местах других систем (в том числе и автономных ПЭВМ) без соответствующей санкции.

13.15. Контроль за выполнением мероприятий по обеспечению безопасности информации на АП возлагается на Администратора безопасности, руководителей соответствующих подразделений, определенных постановлением.

1. **Заключительные положения**

14.1. Требования настоящего Положения обязательны для всех сотрудников обрабатывающих конфиденциальную информацию (персональные данные).

14.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии
с законодательством Российской Федерации.

Приложение 3

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Положение**

**о режиме безопасности в помещениях,**

**предназначенных для обработки и хранения персональных данных в Администрации сельского поселения Алябьевский**

* + 1. **Общие положения**

1.1. Настоящее Положение о режиме безопасности в помещениях, предназначенных для обработки и хранения персональных данных (далее Положение) в Администрации сельского поселения Алябьевский (далее администрация) определяет требования к пропускному и внутриобъектовому режиму в помещениях, предназначенных для обработки персональных данных в Администрации, а также устанавливает ответственность сотрудников Администрации, допущенных к обработке персональных данных (далее ПДн), за соблюдение режима безопасности.

1.2. Настоящее Положение разработано в соответствии со следующими нормативно-правовыми документами:

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

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

Постановление Правительства Российской Федерации (далее РФ)
от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним НПА, операторами, являющимися государственными или муниципальными органами»;

Постановление Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Постановление Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказ Федеральной службы по техническому и экспортному контролю
от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке
в информационных системах персональных данных»;

1.3. Требования настоящего Положения обязательны для всех сотрудников Администрации, имеющих доступ в помещения, предназначенные для обработки персональных данных.

1.4. Все сотрудники, допущенные к обработке персональных данных, должны быть ознакомлены с настоящим Положением под роспись.

1.5. Положение вступает в силу с момента его утверждения распоряжением Администрации сельского поселения Алябьевский.

1.6. Все изменения в настоящее Положение вносятся в письменном виде и утверждаются распоряжением Администрации сельского поселения Алябьевский с обязательным доведением изменений до допущенных к обработке ПДн сотрудников.

* + 1. **Определения**

2.1. Защищаемые помещения – помещения администрации, в которых ведется обработка персональных данных (в том числе сбор, уточнение, накопление, хранение, использование и уничтожение) – автоматизированным способом или без применения средств автоматизации.

2.2. Пропускной режим – совокупность правил, мероприятий и процедур, определяющих порядок допуска лиц, их перемещения на территории администрации.

* + 1. **Пропускной режим**

3.1. Цели пропускного режима:

исключение несанкционированного доступа посторонних лиц в защищаемые помещения;

исключение бесконтрольного посещения защищаемых помещений сотрудниками и посетителями;

исключение возможности несанкционированного выноса, хищения бумажных носителей персональных данных, иных документов и материальных ценностей.

3.2. Пропускной режим включает в себя:

порядок доступа сотрудников и посетителей в защищаемые помещения;

порядок вноса и выноса документов в защищаемые помещения;

порядок оснащения защищаемых помещений техническими средствами контроля доступа.

3.3. В нерабочее время в защищаемых помещениях, в которых осуществляется обработка и хранение персональных данных, должен быть принят комплекс организационных и инженерно-технических мер, исключающих несанкционированный или случайный доступ посторонних лиц, в том числе:

надежные запираемые двери;

учет ключей и дубликатов ключей от защищаемых помещений;

использование средств охранной сигнализации.

3.5. Доступ посетителей в защищаемые помещения возможен только в рабочее время и в сопровождении допущенных в помещение сотрудников. Во всех остальных случаях доступ посетителей в защищаемые помещения запрещен.

3.6. Ключи от защищаемых помещений выдаются под роспись только допущенным в соответствующее помещение сотрудникам. Дубликаты ключей на случай возникновения экстренной ситуации находятся в приёмной администрации.

3.7. При обнаружении признаков несанкционированного доступа в защищаемое помещение, допущенный в помещение сотрудник обязан немедленно сообщить об этом своему непосредственному руководителю для принятия дальнейших решений по устранению последствий нарушения.

* + 1. **Внутриобъектовый режим**

4.1. Цели внутриобъектового режима:

поддержание порядка в защищаемых помещениях;

соблюдение правил обеспечения безопасности персональных данных и бумажных носителей персональных данных в защищаемых помещениях.

4.2. Оставление открытыми защищаемых помещений без присмотра, либо наличие посетителя в защищаемом помещении без контроля со стороны допущенного в помещение сотрудника, является недопустимым.

4.3. Хранение материальных носителей персональных данных, а также размещение технических средств, предназначенных для обработки персональных данных, должно осуществляться только в пределах защищаемых помещений.

4.4. Мониторы и другие устройства вывода информации должны располагаться
в защищаемых помещениях таким образом, чтобы исключить несанкционированный или случайный просмотр информации, отображаемой на мониторах или выводимой на печать.

4.5. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только сотрудники и должностные лица, получившие доступ к персональным данным.

4.6. Нахождение в помещениях, в которых ведется обработка персональных данных лиц, не являющихся сотрудниками и должностными лицами, получившими доступ
к персональным данным, возможно только в присутствии сотрудников и должностных лиц, получивших доступ к персональным данным на время, ограниченное необходимостью решения вопросов, связанных с исполнением должностных функций.

4.7. Присутствие других лиц в данных помещениях допускается в той мере, в какой этого требуют технологические процессы обработки персональных данных. Доступ
в помещения администрации осуществляется только в сопровождении сотрудника администрации, который предварительно производит оценку целесообразности и требуемого времени нахождения лица в помещении, а также проверяет документы, удостоверяющие личность.

4.8. Сотрудники и должностные лица, получившие доступ к персональным данным не должны покидать помещение, в котором ведется обработка персональных данных, оставляя в нем без присмотра посторонних лиц, включая сотрудников, не уполномоченных на обработку персональных данных.

4.9. Доступ в помещения, в которых осуществляется обработка персональных данных, разрешается только в рабочее время.

4.10. Доступ в помещения, в которых осуществляется обработка персональных данных, в нерабочее время возможен только по письменной заявке работника, согласованной с его непосредственным руководителем и имеющей разрешающую резолюцию главы сельского поселения Алябьевский. Данные заявки хранятся у лица, ответственного за организацию обработки персональных данных в администрации.

4.11. В помещениях, в которых происходит обработка и хранение персональных данных, запрещено использование не предусмотренных служебными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

4.12. Для предотвращения несанкционированного доступа к информации, содержащей ПДн, осуществляется контроль деятельности рабочих. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных главой сельского поселения Алябьевский или его заместителями. Работы проводятся под контролем сотрудников администрации.

4.13. Уборка помещения выполняется обслуживающим персоналом под контролем сотрудников, имеющих право доступа в данное помещение. Во время уборки в помещении должна быть приостановлена работа с ПДн, должны быть выключены все автоматизированные рабочие места, на которых хранятся ПДн, носители, содержащие ПДн, должны быть убраны в сейф.

4.14. После окончания рабочего дня дверь каждого помещения закрывается на ключ, при этом запрещается оставлять ключ в замке помещения.

4.15. В нерабочее время помещения, в которых ведется обработка персональных данных, хранятся документы, содержащиеся персональные данные, должны закрываться на ключ и сдаваться под охрану.

4.16. Перед закрытием (опечатыванием) помещения по окончании работы уполномоченные лица обязаны:

убрать бумажные и электронные носители, содержащие персональные данные, в сейфы;

отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

закрыть окна;

закрыть двери помещения.

4.17. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за безопасность персональных данных. Ответственный за безопасность персональных данных должен составить акт и принять, при необходимости, меры к локализации последствий несанкционированного доступа к ПДн.

Приложение 4

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Положение**

**о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных**

**Администрации сельского поселения Алябьевский**

1. **Общие положения**

1.1. В данном документе представлен перечень групп, участвующих в обработке персональных данных в информационных системах персональных данных, а также их уровень прав доступа к обрабатываемым персональным данным

1.2. Разграничение прав доступа осуществляется на основе анализа исходных данных по информационным системам персональных данных в Администрации сельского поселения Алябьевский, а также исходя из характера и режима обработки персональных данных в информационных системах персональных данных.

1.3. Перечень групп, ответственных за обработку персональных данных в информационных системах персональных данных, а так же их уровень прав доступа представлен в Таблице:

|  |  |  |
| --- | --- | --- |
| **Группа/****должность** | **Уровень доступа к ПДн** | **Разрешенные действия** |
| Администратор ИСПДн | Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн.Обладает полной информацией о технических средствах и конфигурации ИСПДн.Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.Обладает правами конфигурирования и административной настройки технических средств ИСПДн | сборсистематизациянакоплениехранениеуточнениеиспользованиеуничтожение |
| Администратор безопасности | Обладает правами Администратора ИСПДн.Обладает полной информацией об ИСПДн.Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн | сборсистематизациянакоплениехранениеуточнениеиспользованиеуничтожение |
| Операторы ИСПДн с правами записи | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн | сборсистематизациянакоплениехранениеуточнениеиспользованиеуничтожение |
| Операторы ИСПДн с правами чтения | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн | использование |

Приложение 5

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Перечень должностей в Администрации сельского поселения Алябьевский, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным**

1. Глава сельского поселения Алябьевский.
2. Заместитель главы сельского поселения Алябьевский.
3. Ведущий специалист (управляющий делами).
4. Ведущий специалист (отдел кадров).
5. Ведущий специалист по жилищным отношениям и муниципальному имуществу.
6. Ведущий специалист по юридическим вопросам.
7. Начальник финансово-экономического отдела.
8. Главный специалист финансово-экономического отдела.
9. Техник-землеустроитель.
10. Старший инспектор по мобилизационной подготовке.
11. Инженер-программист.

Приложение 6

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Инструкция по организации работы с электронными носителями конфиденциальной информации в Администрации сельского поселения Алябьевский**

**Перечень использованных сокращений, единиц и терминов**

АИБ – администратор информационной безопасности;

ИС – информационная система;

ИСПДн – информационная система персональных данных;

КИ – конфиденциальная информация;

НЖМД – накопитель на жёстких магнитных дисках;

ПДн – персональные данные;

СВТ – средства вычислительной техники;

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в АС и ИСПДн, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

1. **Общие положения**

1.1. Настоящая Инструкция устанавливает основные требования к организации учета, использования, передачи и уничтожения электронных носителей информации (далее носители), предназначенных для обработки КИ и ПДн в Администрации сельского поселения Алябьевский (далее администрация).

1.2. Под электронными носителям информации в данном документе понимаются: гибкие магнитные диски, CD- и DVD-диски, USB флеш-диски, НЖМД и др.

1.3. Ответственность за организацию учета, использования, передачи и уничтожения носителей, предназначенных для обработки и хранения КИ и ПДн, затирание (удаление) информации возлагается на АИБа.

1.4. Положения данной инструкции обязательны для выполнения всеми сотрудниками администрации, которые в ходе выполнения своих должностных обязанностей используют носители ПДн и иной КИ, а так же имеющими допуск к обработке КИ и ПДн.

1. **Учёт и хранение электронных носителей информации**

2.1. Учёту подлежат все носители информации, находящиеся в распоряжении администрации и предназначенные для хранения КИ и ПДн.

2.2. Носители учитываются в специальном «Журнале регистрации и учета электронных носителей конфиденциальной информации и персональных данных» (приложение 1 к инструкции) в котором производится непосредственно регистрация и учёт носителей.

2.3. Регистрация и учет носителей информации осуществляется АИБом.

2.4. Учётный номер носителя состоит из сокращенного наименования подразделения (отдела) и порядкового номера по журналу регистрации через дефис (например: уч.
№ ОБ-1/К, где ОБ – отдел бухгалтерии, 1 – порядковый номер в журнале,
К – «Конфиденциально»).

В случае отсутствия утвержденных сокращений названий подразделений учетный номер носителя состоит из порядкового номера по журналу регистрации (например: уч. № 01/К, где 01 – порядковый номер в журнале, К – «Конфиденциально»).

2.5. Каждый носитель информации, применяемый при обработке информации на СВТ, должен иметь гриф конфиденциальности, соответствующий записанной на нём информации: конфиденциальной информации и персональных данных - «К». Исключается хранение на одном носителе информации разных грифов конфиденциальности, а так же хранение информации, имеющей разные цели обработки.

2.6. Для съемных носителей информации реквизиты наносятся непосредственно на носитель (корпус). Если невозможно маркировать непосредственно носитель (корпус), то применяется маркировка упаковки, в которой хранится носитель или другие доступные способы маркировки (бирки, брелоки и т.п.). Надпись реквизитов делается разборчиво и аккуратно. На дискеты и футляры носителей допускается наклеивать заранее заготовленную этикетку.

2.7. Каждому носителю в журнале должна соответствовать отдельная строка.

2.8. НЖМД в серверах и системных блоках компьютеров учитываются в паспорте (формуляре) на поставляемое оборудование с указанием марки носителя информации и его серийного номера.

2.9. Хранение носителей информации осуществляется в условиях (закрываемые шкафы, сейфы и т.п.), исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

2.10. О фактах утраты носителей необходимо незамедлительно докладывать руководителю своего структурного подразделения.

2.11. АИБ не реже одного раза в год осуществляет проверку условий хранения носителей КИ и ПДн.

1. **Выдача/сдача и передача носителей**

3.1. Выдача носителей сотрудникам осуществляется АИБом под подпись с отметкой в «Журнале выдачи/сдачи электронных носителей конфиденциальной информации и персональных данных» (приложение 2 к инструкции). Факт сдачи носителя регистрируется аналогичным образом.

3.2. Носители, как правило, выдаются только непосредственно на время работы
с данным носителем и сдаются сотрудником АИБу сразу по завершению таких работ.

3.3. Носители, которые выдаются сотруднику, должны пройти проверку на отсутствие записанной на ней информации. В случаи наличия какой-либо информации на выдаваемом носителе, АИБ обязан удалить (затереть) информацию согласно п. 4 настоящей инструкции.

3.4. В случае повреждения носителей, содержащих КИ и ПДн, сотрудник,
в пользовании которого они находятся, обязан сообщить о случившемся руководителю своего структурного подразделения (отдела) и АИБу.

3.5. При передаче в другие организации носители информации должны, по возможности, быть упакованы в пакет/конверт, обеспечивающий сохранность (работоспособность) передаваемого носителя. При этом носители информации передаются с сопроводительным письмом, в котором указывается, какая информация содержится на данном носителе, а для подтверждения достоверности информации прилагается таблица с реквизитами файлов (допускается прикладывать скриншот окна архиватора). Данное передвижение (передача) носителей КИ и ПДн регистрируется в «Журнале передачи носителей конфиденциальной информации и персональных данных» (приложение 3 к инструкции), где делается отметка об отправке (куда отправлен (реквизиты адресата), исходящий номер сопроводительного письма, дата отправки, способ отправки (курьер, заказная почта и т.п.)) и отметка о получении (номер «Уведомления о вручении» или «Накладной»). В случае если передача носителей осуществляется лично сотрудником администрации, то у адресата, необходимо взять расписку о получении носителя (приложение 4 к инструкции).

3.6. Для исключения утечки информации, находящейся на жестких дисках компьютеров, при необходимости ремонта компьютера в сервисном центре, жесткий диск с компьютера демонтируется и компьютер отправляется в ремонт без жесткого диска. При необходимости диагностирования самого жесткого диска информация должна быть предварительно скопирована на резервный носитель и затем стёрта с направляемого в ремонт винчестера с использованием специальных средств (сертифицированные программные или программно-аппаратные средства защиты информации, обеспечивающие невозможность восстановления информации), либо путём полного трехкратного его форматирования. Если невозможно произвести данные действия (поломка жесткого диска или ПЭВМ), то отправка такой ПЭВМ в ремонт возможна только по письменному разрешению АИБа.

1. **Порядок уничтожения носителей, затирания информации на носителях**

4.1. Уничтожение носителей информации, пришедших в негодность или утративших практическую ценность, производится путем их физического разрушения без возможности дальнейшего восстановления.

4.2. Перед уничтожением носителя вся информация с него должна быть стерта (уничтожена) путем использования специальных средств (сертифицированные программные или программно-аппаратные средства защиты информации, обеспечивающие невозможность восстановления информации), либо путём полного трехкратного его форматирования, если это позволяют физические принципы работы носителя.

4.3. Уничтожение носителей, затирания (уничтожении) информации с носителей производиться комиссией из 3 человек, назначенной постановлением Администрации сельского поселения Алябьевский. В состав комиссии должен входить АИБ.

4.4. По факту уничтожения носителей, а также затирания (уничтожения) информации на носителях, комиссией составляется Акт (приложение 5 к инструкции). В Акте указываются учётные номера носителей, характер уничтожаемой (затираемой) информации, причина уничтожения носителя (затирания информации на нем). Реквизиты Акта заносятся председателем данной комиссии в графу «Сведения об уничтожении» «Журнала регистрации и учета электронных носителей конфиденциальной информации и персональных данных». Подписанный Акт должен храниться у АИБа.

Приложение 1

к инструкции по организации работы

с электронными носителями конфиденциальной

информации в Администрации

сельского поселения Алябьевский

**Журнал №\_\_**

**регистрации и учета электронных носителей персональных данных и иной конфиденциальной информации**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Регистрационный номер электронного носителя | Вид (тип, модель) электронного носителя | Характер информации, которая будет содержаться на носителе | Дата регистрации электронного носителя | Ф.И.О. лица, регистри-рующего носитель | Подпись лица, регистри-рующего носитель | Сведения об уничтожении носителя (№ акта, дата) |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Приложение 2

к инструкции по организации работы

с электронными носителями конфиденциальной

информации в Администрации

 сельского поселения Алябьевский

**Журнал №\_\_**

**выдачи/сдачи электронных носителей конфиденциальной информации и персональных данных**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Дата | Время | Регистрационный номер электронного носителя | Сдал | Принял |
| Ф.И.О., должность | Подпись | Ф.И.О., должность | подпись |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение 3

к инструкции по организации работы

с электронными носителями конфиденциальной

информации в Администрации

сельского поселения Алябьевский

**Журнал №\_\_**

**передачи носителей конфиденциальной информации и персональных данных**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Дата | Регистра-ционный номер электрон-ного носителя | Характер информации,содержа-щейся на передава-емом носителе | Исходящий номер сопроводительного письма | Адресат (название организации, отдел, должность, Ф.И.О. и т.п.) | Способ передачи/отправки носителя (лично, курьер, заказная почта) | Отправитель (лицо, записавшее информацию на носитель) | Отметка о доставке (дата, реквизиты документа, подтвержда-ющие доставку) |
| Ф.И.О., должность | Подпись |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

Приложение 4

к инструкции по организации работы

с электронными носителями конфиденциальной

информации в Администрации

 сельского поселения Алябьевский

№\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

заполняется отправителем

**Расписка**

 (составлена в двух экземплярах, по одному для каждой из сторон)

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 202\_ г. с.п.Алябьевский

Настоящим подтверждаю получение электронного носителя информации (Регистрационный номер электронного носителя\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) с сопроводительным письмом (исходящий номер сопроводительного письма\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) от\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Название организации: Администрация сельского поселения Алябьевский

Должность и Ф.И.О. представителя организации:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

**Сведения о получателе:**

Название организации:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Должность и Ф.И.О. получателя:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 202\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

подпись получателя расшифровка

Приложение 5

к инструкции по организации работы

с электронными носителями конфиденциальной

информации в Администрации

сельского поселения Алябьевский

**АКТ №\_\_\_\_**

**о затирании/уничтожении конфиденциальной информации и персональных данных /электронных носителей**

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_202\_ г. с.п.Алябьевский

**Комиссия в составе:**

**Председатель:**

Ф.И.О. должностного лица

**Члены комиссии:**

Ф.И.О. должностного лица

Ф.И.О. должностного лица составила настоящий Акт о том, что в ее присутствии уничтожены следующие электронные носители персональных данных и иной конфиденциальной информации/ информация на следующих электронных носителях

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Регистрационный номер электронного носителя | Вид (тип, модель) электронного носителя | Характер информации, которая содержится на носителе | Причина | Способ уничтожения (физическое разрушение, форматирование, с использованием специальных программных средств (каких)) |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Председатель комиссии: |  | Ф.И.О. должностного лица |
| Члены комиссии: |  | Ф.И.О. должностного лица |
|  |  | Ф.И.О. должностного лица |

Отметку в «Журнал регистрации и учета электронных носителей конфиденциальной информации и персональных данных» произвел администратор информационной безопасности\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 подпись

Приложение 7

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных**

**в Администрации сельского поселения Алябьевский**

**Назначение и область действия**

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее Инструкция), связанные с функционированием информационных систем персональных данных (далее ИСПДн) Администрации сельского поселения Алябьевский, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

определение мер защиты от потери информации;

определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей органа исполнительной власти, 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, но не реже раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор ИСПДн.

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор.

**Порядок реагирования на инцидент**

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

в результате непреднамеренных действий пользователей.

В результате преднамеренных действий пользователей и третьих лиц.

В результате нарушения правил эксплуатации технических средств ИСПДн.

В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале учета инцидентов информационной безопасности в Администрации сельского поселения Алябьевский» (приложение 21 к распоряжению).

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные
за реагирование сотрудники органа исполнительной власти (Администратор безопасности, Администратор и Оператор ИСПДн), предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

**Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов**

**Технические меры**

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, 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.

Все критичные помещения Администрации сельского поселения Алябьевский (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т.д.);

резервные линии электропитания в пределах комплекса зданий;

аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

кластеризация;

технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое
в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку
и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

**Организационные меры**

Резервное копирование и хранение данных должно осуществлять на периодической основе:

для обрабатываемых персональных данных – не реже раза в неделю;

для технологической информации – не реже раза в месяц;

эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

**Ответственность**

Ответственность за поддержание установленного в настоящей инструкции порядка проведения резервирования и восстановления работоспособности технических средств
и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на администратора безопасности информации
в Администрации сельского поселения Алябьевский.

Приложение 8

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Инструкция**

**по организации резервного копирования в информационных системах персональных данных Администрации сельского поселения Алябьевский**

1. **Общие положения**

Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных
(далее ИСПДн).

1. **Резервируемое программное обеспечение и базы персональных данных**

В ИСПДн резервированию подлежит:

общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее АРМ), входящими в состав ИСПДн);

прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);

базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);

программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

1. **Порядок резервирования и хранения резервных копий**

Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны также храниться у администратора информационной безопасности в ИСПДн.

Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

Резервирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

Резервирование осуществляется ежемесячно.

Резервные носители персональных данных хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации персональных данных.

К резервному носителю персональных данных должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

Резервные носители персональных данных не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

1. **Порядок восстановления работоспособности ИСПДн**

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов
и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы осуществляются администратором информационной безопасности
в ИСПДн в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность
их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн
и руководителя структурного подразделения, обеспечивающего ее эксплуатацию.

Приложение 9

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Инструкция**

**по организации парольной защиты Администрации сельского поселения Алябьевский**

Данная инструкция регламентируют организационно-технические мероприятия
по обеспечению процессов генерации, смены и прекращения действия паролей
в информационной системе персональных данных (далее ИСПДн), а также контроль действий пользователей при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора безопасности.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ОВТ самостоятельно с учетом следующих требований:

пароль должен быть не менее 6 символов;

в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, \*, % и т.п.);

символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированных рабочих мест и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущих;

пользователь не имеет права сообщать личный пароль другим лицам.

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

В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение руководителю структурного подразделения. Запечатанные конверты (пеналы) с паролями исполнителей должны храниться в недоступном месте у руководителя структурного подразделения.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 3 месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором безопасности (либо новым постоянным пользователем) немедленно после окончания последнего сеанса работы данного пользователя с системой на основании указания руководителя структурного подразделения.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности.

В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.

Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности.

Приложение 10

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Инструкция**

**по организации антивирусной защите**

**информационных систем персональных данных**

**Администрации сельского поселения Алябьевский**

1. **Общие положения**

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

1.2. Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников администрации, использующих в работе ИСПДн администрации.

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

1.4. Доведение Инструкции до сотрудников администрации, в части их касающейся осуществляется администратором информационной безопасности ИСПДн под роспись
в журнале или на самом документе.

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

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

злоумышленных действий, практическая «глубина» исполнения настоящей Инструкции определяется Администратором информационной безопасности ИСПДн по согласованию с ответственным за обеспечение безопасности персональных данных (далее ПДн) администрации.

1. **Применение средств антивирусной защиты**

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

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

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

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

1. **Функции администратора ИСПДн по обеспечению антивирусной безопасности**

Администратор безопасности ИСПДн обязан:

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

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

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

3.4. При необходимости производить обновление антивирусных программных средств.

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

3.6. При необходимости разрабатывать инструкции по работе пользователей
с программными средствами системы антивирусной защиты.

3.7. Проводить работы по обнаружению и обезвреживанию вирусов.

3.8. Участвовать в работе комиссии по расследованию причин заражения персональных электронно-вычислительных машинах (далее ПЭВМ) и серверов.

3.9. Хранить эталонные копии антивирусных программных средств.

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

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

1. **Функции пользователей**

Пользователи ИСПДн:

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

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

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

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

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора информационной безопасности ИСПДн, а также смежные отделы, использующие эти файлы в работе;

провести анализ необходимости дальнейшего использования зараженных вирусом файлов;

провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь Администратора информационной безопасности ИСПДн);

в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе Администратору информационной безопасности ИСПДн для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;

по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору информационной безопасности ИСПДн, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

1. **Порядок пересмотра инструкции**

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

5.2. В остальных случаях Инструкция подлежит частичному пересмотру.

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

5.4. Вносимые изменения не должны противоречить другим положениям Инструкции.

1. **Ответственные за организацию и контроль выполнения инструкции**

6.1. Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников администрации.

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

6.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за организацию обработки персональных данных ПДн Администрации сельского поселения Алябьевский.

Приложение 11

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Инструкция по обработке персональных данных без использования средств автоматизации в Администрации сельского поселения Алябьевский**

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

2. К обработке персональных данных могут иметь доступ сотрудники Администрации сельского поселения Алябьевский, определённые распоряжением Администрации сельского поселения Алябьевский (Приложение 5 к настоящему распоряжению Администрации сельского поселения Алябьевский), при этом они должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

3. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее персональные данные), 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.

Обработка персональных данных не может быть признана осуществляемой
с использованием средств автоматизации только на том основании, что персональные данные содержаться в информационной системе персональных данных либо были извлечены из нее.

4. Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных.

Согласие субъекта персональных данных не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании Федерального закона Российской Федерации, устанавливающего её цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

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

4) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи;

5) осуществляется обработка персональных данных, подлежащих опубликованию
в соответствии с федеральными законами, в том числе кандидатов на выборные муниципальные должности;

6) в иных случаях определённых Федеральным законом Российской Федерации
от 27.07.2006 № 152-ФЗ «О персональных данных».

5. Хранение персональных данных должно происходить в порядке, исключающем их утрату, неправомерное использование, распространение (в том числе передачу) без согласия субъекта персональных данных и несанкционированный доступ.

6. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных, в специальных разделах или на типовых формах документов.

7. Сотрудники, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть ознакомлены с настоящей инструкцией.

8. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

9. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации - при необходимости получения письменного согласия на обработку персональных данных;

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

10. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

11. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

12. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

**Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации**

13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

14. Сотрудник при работе с персональными данными обязан:

принимать необходимые меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий;

предоставлять информацию субъекту персональных данных при его обращении, касающейся обработки персональных данных, в том числе содержащей:

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

б) способы обработки персональных данных;

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

г) перечень обрабатываемых персональных данных и источник их получения;

д) сведения о том, какие юридические последствия может повлечь за собой обработка его персональных данных;

осуществить блокирование персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора;

устранять допущенные нарушения в случае выявления неправомерных действий
с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления;

сообщать непосредственному начальнику о попытках несанкционированного доступа к персональным данным.

Приложение 12

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Инструкция по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в Администрации сельского поселения Алябьевский**

1. **Общие положения**

1.1. Настоящее Инструкция разработана в соответствии с Федеральным законом
от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» и другими нормативными правовыми актами, и устанавливает порядок использования носителей информации, предоставляемых органом исполнительной власти (далее ОИВ) для использования в информационных системах (далее ИС).

1.2. Действие настоящей Инструкции распространяется на сотрудников Администрации сельского поселения Алябьевский, подрядчиков и третью сторону.

1. **Основные термины, сокращения и определения**

2.1. Администратор ИС – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения и оборудования вычислительной техники.

2.2. АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

2.3. ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

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

2.5. Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации.

2.6. Паспорт ПК – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

2.7. ПК – персональный компьютер.

2.8. ПО – Программное обеспечение вычислительной техники.

2.9. ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.10. ПО коммерческое – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

2.11. Пользователь – работник Организации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

1. **Порядок использования носителей информации**

3.1. Под использованием носителей информации в ИС органа исполнительной власти понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью органа исполнительной власти и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным органам исполнительной власти носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

3.4. Носители конфиденциальной информации предоставляются сотрудникам органа исполнительной власти по инициативе Руководителей структурных подразделений в случаях:

необходимости выполнения вновь принятым работником своих должностных обязанностей;

возникновения у сотрудника органа исполнительной власти производственной необходимости.

1. **Порядок учета, хранения и обращения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации**

4.1. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в Администрации сельского поселения Алябьевский.

4.2. Каждый съемный носитель с записанными на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

4.4. Сотрудники Администрации сельского поселения Алябьевский 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.

1. **При использовании сотрудниками носителей конфиденциальной информации необходимо:**

5.1. Соблюдать требования настоящего Положения.

5.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.

5.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения.

5.4. Бережно относится к носителям конфиденциальной информации.

5.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами.

5.6. Извещать администраторов ИС о фактах утраты (кражи) носителей конфиденциальной информации.

1. **При использовании носителей конфиденциальной информации запрещено:**

6.1. Использовать носители конфиденциальной информации в личных целях.

6.2. Передавать носители конфиденциальной информации другим лицам
(за исключением администраторов ИС).

6.3. Хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

6.4. Выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т.д.

6.5. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником администрации городского поселения Таёжный между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администраторами ИС заранее). Администратор ИС оставляет за собой право блокировать или ограничивать использование носителей информации.

6.6. Информация об использовании сотрудником Администрации сельского поселения Алябьевский носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена Руководителям структурных подразделений, а также главе сельского поселения Алябьевский.

6.7. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей конфиденциальной информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется главой сельского поселения Алябьевский.

6.8. По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Организации и действующему законодательству.

6.9. Информация, хранящаяся на носителях конфиденциальной информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

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

6.11. Вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

6.12. В случае утраты или уничтожения съемных носителей конфиденциальной информации (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 конфиденциальной информации (персональных данных).

6.13. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт по прилагаемой форме.

6.14. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются.

**8. Ответственность**

8.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами Администрации сельского поселения Алябьевский.

Приложение 13

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Руководство**

**администратора информационной безопасности информационной системы персональных данных Администрации сельского поселения Алябьевский**

1. **Общие положения**

Настоящее Руководство определяет функции, права и обязанности Администратора безопасности по вопросам обеспечения информационной безопасности конфиденциальной информации, в т.ч. персональных данных при работе в информационной системе персональных данных (далее ИСПДн) Администрации сельского поселения Алябьевский (далее администрация).

Администратор информационной безопасности назначается распоряжением Администрации сельского поселения Алябьевский и обеспечивает правильность использования и нормальное функционирование установленной системы защиты информации (далее СЗИ).

1. **Основные функции Администратора информационной безопасности**

2.1. Контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности и защиты персональных данных при проведении работ в ИСПДн администрации.

2.2. Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом в ИСПДн:

реализация полномочий доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру, сетевым ресурсам и т.д.);

ввод описаний пользователей ИСПДн в информационную базу СЗИ от несанкционированного доступа (далее НСД);

своевременное удаление описаний пользователей из базы данных СЗИ при изменении списка допущенных к работе в ИСПДн лиц.

2.3. Контроль за периодическим проведением смены паролей для доступа к ИСПДн пользователями.

2.4. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн:

введение в базу данных СЗИ от НСД, внедренной в ИСПДн, описания событий, подлежащих регистрации в системном журнале;

регулярное проведение анализа системного журнала для выявления попыток НСД к защищаемым ресурсам;

своевременное информирование руководителя, ответственного за эксплуатацию ИСПДн администрации о несанкционированных действиях персонала и проведение расследования попыток НСД.

2.5. Сопровождение антивирусной подсистемы и системы защиты от программно-математических воздействий:

поддержание установленного порядка и правил антивирусной защиты информации в ИСПДн от компьютерных вирусов;

периодическое обновление антивирусных средств (баз данных), внедрённых в ИСПДн, контроль за соблюдением пользователями порядка и правил проведения антивирусного тестирования ИСПДн администрации;

* 1. Сопровождение, подсистемы межсетевого экранирования:

анализ журнала межсетевого экрана на предмет выявления запрещенных взаимодействий.

1. **Обязанности Администратора безопасности**

3.1. Администратор безопасности обязан:

обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных функций;

проводить инструктаж пользователей по правилам работы в ИСПДн с внедренными средствами защиты;

докладывать руководителю, ответственному за эксплуатацию ИСПДн администрации о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

следить за выполнением пользователями своих обязанностей, в т. ч. за проведением периодических антивирусных проверок;

по всем вопросам, касающимся функционирования средств защиты информации и неотраженным в настоящей инструкции, обращаться к руководствам конкретных средств защиты, имеющимся на установочных дисках этих средств.

1. **Права Администратора безопасности:**
	1. Администратор безопасности имеет право:

участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

Приложение 14

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Руководство пользователя по обеспечению безопасности информационной системы персональных данных в Администрации сельского поселения Алябьевский**

1. **Общие положения**

1.1. Пользователь информационной системы персональных данных (далее Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных (далее ИСПДн).

1.2. Пользователем является сотрудник Администрации сельского поселения Алябьевский, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных без использования средств автоматизации, обработки персональных данных с использованием средств автоматизации, а также смешанной обработке персональных данных и сопутствующей выполнению должностных обязанностей информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами Федеральная служба по техническому и экспортному контролю (далее ФСТЭК России) и регламентирующими документами Администрации сельского поселения Алябьевский (далее администрации).

1.5. Методическое руководство работой пользователя осуществляется ответственным за соблюдение требований по защите информации, а также ответственным за организацию обработки персональных данных (далее ПДн).

1. **Должностные обязанности**

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Иметь доступ и использовать для выполнения своих должностных обязанностей на автоматизированном рабочем месте (далее АРМ) персональные данные согласно перечня конфиденциальной информации в соответствии с Указом Президента Российской Федерации от 06 марта 1997 года № 188 в редакции от 13 июля 2015 года, а также списка лиц допущенных к обработке ПДн.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов в соответствии с действующим законодательством Российской Федерации.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью администрации, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться в информационно аналитический отдел управления по организации деятельности Администрации сельского поселения Алябьевский (далее Отдел ИБ).

2.8. Пользователям запрещается:

разглашать защищаемую информацию третьим лицам;

копировать защищаемую информацию на внешние носители для целей, не связанных
с исполнением своих должностных обязанностей;

самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

несанкционированно открывать общий доступ к папкам на своей рабочей станции;

запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

отключать (блокировать) средства защиты информации;

обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.9. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.10. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

1. **Организация парольной защиты**

3.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором ИСПДн.

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

3.3. Правила формирования пароля:

пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

пароль должен состоять не менее чем из 8 символов;

в пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

запрещается использовать в качестве пароля комбинацию символов, набираемых
в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

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

во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. 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 и регистрировать их в системе под своим паролем.

3.6. Обеспечить надежное хранение носителей информации ограниченного распространения.

3.7. Лица, использующие паролирование, обязаны:

четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

своевременно сообщать в Отдел ИБ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

1. **Правила работы в сетях общего доступа и (или) международного обмена**

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

осуществлять работу при отключенных средствах защиты (антивирус и других);

передавать по Сети защищаемую информацию без использования средств защиты каналов связи;

запрещается скачивать из Сети программное обеспечение и другие файлы;

запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие);

запрещается нецелевое использование подключения к сети.

Приложение 15

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Инструкция**

**ответственного за организацию обработки персональных данных**

**в Администрации сельского поселения Алябьевский**

1. **Основные понятия**

Применяемые в настоящей Инструкции термины и понятия означают:

Администратор безопасности - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

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

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Защита информации от разглашения – защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа (ЗИ от НСД) – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

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

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Лицо, ответственное за организацию обработки персональных данных (далее Ответственный), - лицо, назначенное нормативным правовым актом Администрации сельского поселения Алябьевский, ответственное за регламентацию процесса обработки и защиты персональных данных.

Персональные данные (ПДн) – 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.

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

Средство защиты информации (СЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание ПДн в ИСПДн или в результате которых уничтожаются материальные носители ПДн.

1. **Общие положения**
	1. Настоящая инструкция разработана на основании следующих нормативных правовых документов:

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

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

постановление Правительства Российской Федерации от 21 марта 2012 года № 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»;

специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), Государственная техническая комиссия при президенте Российской Федерации, 2002 год;

2.2. Инструкция определяет основные задачи, функции, обязанности и права Ответственного за организацию обработку ПДн ИСПДн;

2.3. В своей деятельности Ответственный руководствуется требованиями действующих Федеральных законов, общегосударственных нормативных правовых документов, (указанных в п. 2.1.), а также нормативно правовых актов Администрации сельского поселения Алябьевский по вопросам защиты ПДн и обеспечивает их выполнение.

2.4. Ответственный за организацию обработки персональных данных, получает указания непосредственно от главы сельского поселения Алябьевский и подотчетно ему.

1. **Задачи и функции Ответственного**

3.1. Основными задачами Ответственного являются:

разработка нормативной правовой документации, регламентирующей порядок обработки и защиты ПДн;

организация доведения до сведения сотрудников, допущенных к ПДн, положений законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

осуществление внутреннего контроля соблюдения требований законодательства Российской Федерации и инструкций при обработке ПДн, в том числе требований к защите ПДн;

организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов;

заполнение и отправка уведомления об обработке (о намерении осуществлять обработку) ПДн;

организация контроля эффективности защиты ПДн.

3.2. Для выполнения поставленных задач на Ответственного возлагаются следующие функции:

организация допуска пользователей (разработчиков, эксплуатационного персонала)
к техническим, программным средствам и информационным ресурсам ИСПДн
в соответствии с матрицей доступа пользователей к защищаемым ПДн ИСПДн на всех стадиях жизненного цикла ИСПДн;

участие на стадии проектирования (внедрения) ИСПДн, в разработке технологии обработки ПДн по вопросам:

организации порядка учета, хранения и обращения с документами и носителями информации;

подготовка новых инструкций и внесение изменений и дополнений в настоящую Инструкцию, определяющих задачи, функции, ответственность, права и обязанности администраторов и пользователей ИСПДн по вопросам защиты ПДн;

организация контроля выполнения требований действующих нормативных документов по вопросам защиты информации при обработке ПДн в ИСПДн;

оперативный контроль хода технологического процесса обработки ПДн;

методическое руководство работой пользователей ИСПДн в вопросах обеспечения информационной безопасности.

1. **Обязанности Ответственного**

4.1. Для реализации поставленных задач и возложенных функций Ответственный обязан:

осуществлять учет и периодический контроль состава и полномочий пользователей различных ПЭВМ, на которых ведется обработка ПДн;

своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СЗИ от НСД, установленных на ПЭВМ;

контролировать обеспечение защиты ПДн при взаимодействии пользователей
с информационными сетями общего пользования;

требовать прекращения обработки ПДн, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

Организовывать контроль эффективности защиты ПДн:

по выявлению возможности вмешательства в процесс функционирования ПЭВМ и осуществления НСД к информации и техническим средствам ПЭВМ;

проводить занятия с администраторами и пользователями ИСПДн по правилам работы на ПЭВМ, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков, выявленных при контроле эффективности защиты информации;

организовывать учет, хранение, прием и выдачу персональных идентификаторов ответственным исполнителям, осуществлять контроль правильности их использования;

осуществлять периодический контроль порядка учета, создания, хранения и использования резервных и архивных копий массивов данных;

участвовать в проведении внутреннего расследования по фактам разглашения ПДн, нарушения условий функционирования системы обработки и защиты ПДн.

4.2. Ответственному запрещается:

использовать в своих и в чьих-либо личных интересах ресурсы ИСПДн, предоставлять такую возможность другим;

производить действия, приводящие к нарушению обработки ПДн.

1. **Права Ответственного**

5.1. Ответственный имеет право:

получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИСПДн и ПЭВМ пользователей;

требовать от пользователей ИСПДн выполнения правил обработки ПДн и инструкций по обеспечению безопасности ПДн в ИСПДн;

участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности с последующим отчетом главе сельского поселения Алябьевский.

5.2. Ответственный несет ответственность за:

реализацию утвержденных в Администрации сельского поселения Алябьевский документов, регламентирующих порядок обработки и обеспечения безопасности ПДн;

разглашение ПДн и сведений ограниченного распространения, ставших известными ему по роду работы;

качество и последствия проводимых им работ по контролю действий пользователей при работе в ИСПДн.

1. **Проведение внутреннего расследования по фактам разглашения персональных данных, нарушения условий функционирования системы обработки и защиты персональных данных**

6.1. Основными целями проведения внутреннего расследования являются:

выявление предпосылок утраты ПДн в результате нарушения порядка их обработки;

выявление лиц из числа сотрудников (далее Сотрудник) Администрации сельского поселения Алябьевский виновных в утрате ПДн;

определение ущерба в результате утраты ПДн;

проверка полноты и качества исполнения нормативных документов по работе со средствами защиты ПДн;

документальное подтверждение соответствия обработки, хранения и передачи ПДн нормам и правилам, установленным федеральными правовыми и нормативными актами;

определение фактического состояния системы защиты ПДн.

6.2. Сотрудник Администрации сельского поселения Алябьевский, по вине которого произошло нарушение, обязан по требованию Ответственного представить объяснения в письменной форме не позднее одного рабочего дня с момента получения соответствующего требования. Ответственный вправе увеличить указанный срок, а также поставить перед служащим перечень вопросов, на которые Сотрудник обязан ответить.

6.3. В целях внутреннего расследования все служащие Администрации сельского поселения Алябьевский, по первому требованию Ответственного, должны предъявить для проверки все числящиеся за ними материалы, содержащие ПДн представить устные или письменные объяснения, в том числе об известных им фактах разглашения ПДн, утраты документов и изделий, содержащих ПДн.

6.4. В случае давления на служащего Администрации сельского поселения Алябьевский со стороны других служащих Администрации сельского поселения Алябьевский или третьих лиц (просьб, угроз, шантажа и др.) по вопросам, связанным с проведением внутреннего расследования, Сотрудник Администрации сельского поселения Алябьевский обязан сообщить об этом Ответственному.

6.5. Для проведения внутреннего расследования глава сельского поселения Алябьевский формирует комиссию из опытных и квалифицированных служащих Администрации сельского поселения Алябьевский в составе не менее трех человек. Председателем комиссии является Ответственный.

6.6. До вынесения решения, членам комиссии запрещается разглашать сведения остальным служащим Администрации сельского поселения Алябьевский о ходе проведения внутреннего расследования и ставших известными им в связи с этим обстоятельствах.

6.7. В процессе проведения внутреннего расследования выясняются:

перечень разглашенных сведений, составляющих ПДн;

причины разглашения ПДн;

круг лиц, виновных в разглашении ПДн;

размер причиненного ущерба;

недостатки и нарушения, допущенные служащими Администрации сельского поселения Алябьевский при работе с ПДн;

иные обстоятельства.

6.8. По результатам расследования комиссией составляется акт с отражением в нем лиц, виновных в разглашении ПДн, размера причиненного ущерба Администрации сельского поселения Алябьевский, наличии ущерба субъектам персональных данных, а также иных выясненных обстоятельствах.

6.9. На основании акта комиссия выносит решение о:

применении мер дисциплинарного воздействия к служащему;

информировании регулятора о факте нарушения;

информировании правоохранительных органов;

информировании субъектов персональных данных.

1. **Порядок реагирования на аварийную ситуацию**

7.1. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

7.2. В кратчайшие сроки, не превышающие одного рабочего дня, Ответственный предпринимает меры по восстановлению нарушенной работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

7.3. При реагировании на инцидент, важно правильно классифицировать критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 – Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты.

Уровень 2 – Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты.

Уровень 3 – 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 нарушению работоспособности ИСПДн и средств защиты на сутки и более.

7.4. 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.

7.5. Все помещения Администрации сельского поселения Алябьевский, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации.

7.6. Ответственным должно быть организовано обучение должностных лиц, 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.

7.7. 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.

Приложение 16

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Инструкция**

**ответственного за обеспечение безопасности персональных данных**

**в информационной системе персональных данных**

**Администрации сельского поселения Алябьевский**

1. **Общие положения**

1.1. Данная Инструкция определяет основные обязанности, права ответственного лица за обеспечение безопасности персональных данных Администрации сельского поселения Алябьевский (далее администрация).

1.2. Ответственное лицо за обеспечение безопасности персональных данных является штатным работником администрации и назначается распоряжением Администрации сельского поселения Алябьевский.

1.3. Ответственное лицо за обеспечение безопасности персональных данных (далее Ответственный) - лицо, отвечающее за организацию и состояние процесса обработки персональных данных (далее ПДн) в информационных системах персональных данных (далее ИСПДн).

1.4. Решение вопросов организации защиты персональных данных, обрабатываемых в информационных системах администрации, входит в прямые трудовые обязанности администрации.

1.5. Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение соответствующих работ.

1.6. Ответственный в своей работе руководствуется Федеральным законом
от 27 июля 2006 № 152-ФЗ «О персональных данных», постановлениями Правительства, руководящими и нормативными документами Управлением Федеральной службы
по техническому и экспортному контролю России, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации, настоящей Инструкцией и иными регламентирующими документами Администрации сельского поселения Алябьевский.

1.7. Требования Ответственного, связанные с выполнением им своих трудовых обязанностей, обязательны для исполнения всеми работниками, имеющими санкционированный доступ к персональным данным.

1.8. Ответственный обладает правами доступа к любым носителям персональных данных Администрации сельского поселения Алябьевский.

1. **Обязанности Ответственного**

Ответственный обязан:

2.1. Обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации ИСПДн, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранностью.

2.2. Знать и предоставлять ответственному за организацию обработки персональных данных изменения к списку лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей.

2.3. Проводить инструктаж и консультации пользователей ИСПДн по соблюдению режима конфиденциальности.

2.4. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

2.5. Организовывать периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами.

2.6. Взаимодействовать с администратором безопасности по вопросам обеспечения и выполнения требований обработки персональных данных.

2.7. Контролировать осуществление мероприятий по установке и настройке средств защиты.

2.8. Организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа.

2.9. Контролировать периодическое резервное копирование баз персональных данных и сопутствующей защищаемой информации.

2.10. По указанию руководства своевременно и точно отражать изменения
в локальных нормативно-правовых актах по управлению средствами защиты информации
в ИСПДн и по правилам обработки персональных данных.

2.11. Знать перечень и условия обработки персональных данных в Администрации сельского поселения Алябьевский.

2.12. Знать перечень установленных в подразделении технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

2.13. Обеспечивать соблюдение работниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров
и серверов из состава информационных систем.

2.14. Осуществлять контроль за порядком учета, создания, хранения и использования машинных (выходных) документов, содержащих персональные данные.

2.15. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем и осуществления несанкционированного доступа к персональным данным и техническим средствам из состава информационных систем подразделения, сообщать о них должностному лицу Администрации сельского поселения Алябьевский.

2.16. Инструктировать работников по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами зашиты информации.

2.17. Знать законодательство Российской Федерации о персональных данных, следить за его изменениями.

2.18. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

2.19. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

**3. Права Ответственного**

Ответственный имеет право:

3.1. Требовать от всех пользователей информационных систем персональных данных выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

3.2. Инициировать блокирование доступа работников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

3.3. Участвовать в разработке мероприятий по совершенствованию системы защиты персональных данных.

3.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.5. Обращаться к руководителю подразделения 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.

3.6. Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

**4.Действия при обнаружении попыток несанкционированного доступа**

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

4.1.2. действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа Ответственный обязан:

4.2.1. по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

4.2.2. доложить должностному лицу Администрации сельского поселения Алябьевский служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

4.2.4. известить ответственного за организацию обработки персональных данных и администратора безопасности о факте несанкционированного доступа.

1. **Ответственность**

5.1. Ответственный несет персональную ответственность за:

5.1.1. соблюдение требований настоящей Инструкции,

5.1.2. правильность и объективность принимаемых решений,

5.1.3. качество и своевременность проводимых им работ по обеспечению безопасности персональных данных,

5.1.4. за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

5.2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 17

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Инструкция**

**ответственного за эксплуатацию информационных систем персональных данных**

1. **Общие положения**

Ответственный за эксплуатацию информационной системы персональных данных (далее ИСПДн) в Администрации сельского поселения Алябьевский назначается распоряжением Администрации сельского поселения Алябьевский.

Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных
в Администрации сельского поселения Алябьевский.

Ответственный за эксплуатацию в своей работе руководствуется положениями, руководящими и нормативными документами Федеральная служба по техническому
и экспортному контролю (ФСТЭК России) и Федеральная служба безопасности Российской Федерации по защите информации и организационно-распорядительными документами для данной ИСПДн, а также иными нормативными документами в части защиты информации.

Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия,
и действия сотрудников вверенного структурного подразделения в соответствии
с действующим законодательством Российской Федерации.

1. **Функции ответственного за эксплуатацию ИСПДн**

Осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.

Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.

Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.

Представление заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.

Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

1. **Обязанности ответственного за эксплуатацию ИСПДн**

Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

Обеспечивать контроль выполнения установленного комплекса мероприятий
по обеспечению безопасности ПДн.

Контролировать целостность печатей (пломб) на устройствах ИСПДн.

Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их
в ремонт.

Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.

Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа
к информационным ресурсам ИСПДн.

Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

Приложение 18

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Положение**

**о порядке выявления и реагирования на инциденты информационной безопасности в Администрации сельского поселения Алябьевский**

1. **Общие положения**

1.1. Настоящее Положение устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования информационной системы Администрации сельского поселения Алябьевский (далее администрация) и (или) возникновению угроз безопасности конфиденциальной информации администрация (далее инциденты ИБ), а также регулирует порядок проведения служебного расследования нарушений режима служебной тайны (далее служебное расследование) в администрации.

Процесс управления инцидентами ИБ включает:

учет и регистрацию инцидентов ИБ;

оповещение ответственного лица о возникновении инцидентов ИБ;

расследование обнаруженных инцидентов ИБ;

устранение причин и последствий инцидентов ИБ;

определение плана корректирующих и превентивных мероприятий.

1.2. Требования настоящего Положения являются обязательными для выполнения всеми работниками администрации.

1. **Учет и регистрация инцидентов информационной безопасности**

2.1. Для выявления инцидентов ИБ должны использоваться встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также специализированные средства анализа защищенности информационных систем администрации.

2.2. В обязательном порядке должны регистрироваться следующие события безопасности:

попытки входа (выхода) пользователей в операционную систему (из операционной системы);

загрузка и инициализация операционной системы и ее программного останова для рабочих станций и серверов;

попытка доступа к средствам виртуализации;

факт изменения конфигурации средств виртуализации;

запуск и остановка служб (системных сервисов) средств виртуализации;

попытки подключения к рабочим станциям и серверам мобильных устройств и внешних носителей информации.

2.3. В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:

тип события;

дата и время события;

результат события;

источник события;

идентификатор пользователя информационной системы, предъявленный при попытке доступа.

2.4. Хранение информации об инцидентах ИБ должно осуществляться в течение срока, достаточного для проведения служебного расследования.

2.5. Учет инцидентов ИБ осуществляется администратором информационной безопасности информационных систем (далее администратор ИБ), назначенным приказом по Организации. Допускается ведение учета инцидентов ИБ в электронном виде.

2.6. При обнаружении инцидента ИБ администратор ИБ проводит его классификацию в соответствии с приложением к настоящему положению.

Инциденты ИБ и их последствия классифицируются по значимости на текущие, значимые и имеющие признаки преступления.

1. **Порядок оповещения ответственного лица о возникновении инцидентов информационной безопасности**

Средства защиты информации должны обеспечивать возможность информирования администратора ИБ о критических событиях безопасности в информационной системе по электронной почте или посредством смс.

В случае, если зафиксированный инцидент ИБ был классифицирован как «значимый» или «имеющий признаки компьютерного преступления», администратор ИБ обязан незамедлительно сообщить о выявленном инциденте ИБ ответственному за обеспечение безопасности конфиденциальной информации по электронной почте или иному средству связи.

Ответственный за обеспечение безопасности конфиденциальной информации должен провести внеплановый анализ выявленного инцидента ИБ и, в случае необходимости, инициировать процедуру служебного расследования в соответствии с порядком, установленным данным Положением.

1. **Порядок расследования обнаруженных инцидентов информационной безопасности**

Проведение служебного расследования инициируется распоряжением Администрации сельского поселения Алябьевский. В этом же распоряжении устанавливается состав Комиссии для проведения служебного расследования (далее Комиссия).

Комиссия для проведения служебного расследования в рабочем порядке
в максимально короткие сроки, привлекая все необходимые ресурсы, проводит служебное расследование.

Результаты работы Комиссии оформляются в виде аналитического экспертного заключения на имя главы сельского поселения Алябьевский, с предложениями:

по внесению изменений в организационные и (или) технические меры по защите конфиденциальной информации;

по внесению изменений и улучшений в комплект организационно-​распорядительной документации администрации;

по расширению или дополнению списка инцидентов ИБ, установленного данным Положением, если это необходимо.

В аналитическом экспертном заключении должен быть приведен перечень ответственных за выполнение запланированных работ и сроки выполнения запланированных работ.

Материалы служебного расследования, его выводы и заключения могут быть использованы как основание для реализации уголовной, гражданской, административной или дисциплинарной ответственности, в порядке, определяемом действующим законодательством и локальными правовыми актами администрации.

1. **Устранение причин и последствий инцидентов информационной безопасности**

5.1. Для инициирования работ по устранению причин и последствий инцидентов ИБ ответственный за обеспечение безопасности конфиденциальной информации направляет аналитическое экспертное заключение главе сельского поселения Алябьевский и ответственным за выполнение запланированных работ.

Если ответственный за выполнение запланированных работ не согласен
с установленными сроками, он вправе обратиться к ответственному за обеспечение безопасности конфиденциальной информации с просьбой перенести срок с обоснованием причин переноса.

При изменении сроков реализации действий, ответственный за обеспечение безопасности конфиденциальной информации вносит необходимые изменения в экспертное заключение и информирует о них ответственного за выполнение запланированных работ и главу сельского поселения Алябьевский.

После реализации запланированных работ ответственное лицо должно направить по электронной почте ответственному за обеспечение безопасности конфиденциальной информации подтверждение выполнения работ, не позднее срока реализации, установленного в экспертном заключении.

5.2. Ответственный за обеспечение безопасности конфиденциальной информации вправе запросить у назначенного лица информацию о выполнении в случае, если ему не поступило подтверждение выполнения работ в течение 2 рабочих дней с даты, установленной в экспертном заключении.

5.3. Оценку результативности предпринятых мер осуществляет ответственный за обеспечение безопасности конфиденциальной информации ежемесячно на основании анализа информации, содержащейся в отчетах о проведении служебного расследования
и в сводном отчете об инцидентах ИБ.

5.4. О результативности предпринятых корректирующих и превентивных мер свидетельствует отсутствие повторных инцидентов ИБ.

**6. Определение плана корректирующих и превентивных мероприятий**

Ежемесячно администратор ИБ готовит сводный отчет по инцидентам ИБ, предоставляемый ответственному за обеспечение безопасности конфиденциальной информации администрации.

В сводном отчете администратор ИБ должен провести анализ выявленных инцидентов ИБ, в качестве приложения к отчету должен быть предложен перечень корректирующих и превентивных мероприятий, направленных на устранение причин и последствий инцидентов ИБ и на предотвращение подобных нарушений в будущем. Данный перечень должен устанавливать сроки реализации и ответственных за проведение указанных мероприятий.

После согласования указанного перечня с ответственным за обеспечение безопасности конфиденциальной информации, данная информация доводится администратором ИБ до всех работников, назначенных ответственными за проведение корректирующих и превентивных мероприятий.

Контроль за своевременным и качественным выполнением работ по проведению корректирующих и превентивных мероприятий осуществляет ответственный за обеспечение безопасности конфиденциальной информации.

**7. Ответственность**

7.1. Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет ответственный за обеспечение безопасности конфиденциальной информации.

7.2. Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет администратор ИБ, назначенный распоряжением Администрации сельского поселения Алябьевский.

Приложение

к Положению о порядке

выявления и реагирования

на инциденты информационной безопасности

**Перечень**

**инцидентов информационной безопасности**

**Администрации сельского поселения Алябьевский**

|  |  |
| --- | --- |
| **№ п/п** | **Описание инцидента информационной безопасности** |
| 1 | 2 |
| **1. Текущие нарушения** |
| 1.1. | Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (однократная) |
| 1.2. | Периодические попытки неудачного доступа к объектам: компьютерам, принтерам, файлам, документам |
| 1.3. | Несанкционированный перевод времени на рабочей станции либо на других элементах информационной инфраструктуры Организации |
| 1.4. | Выполнение производственных обязанностей с использованием компьютерного оборудования в нерабочее время |
| 1.5. | Оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время |
| 1.6. | Перезагрузка рабочей станции при сбоях в работе (однократная), в том числе аварийная перезагрузка путем нажатия кнопки горячей перезагрузки или полного отключения питания |
| 1.7. | Нецелевое использование элементов информационной инфраструктуры (печать, сервисы сети Интернет, электронная почта, и т.п.) |
| **2. Значимые нарушения** |
| 2.1. | Ошибка при регистрации в информационной Системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (многократная) |
| 2.2. | Неоднократное оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время |
| 2.3. | Утрата учтенного магнитного, оптического или иного носителя конфиденциальной информации |
| 2.4. | Утрата носителя информации с резервной копией |
| 2.5. | Неудачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) (многократная) |
| 2.6. | Удачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) |
| 2.7. | Нерегламентированная очистка журналов событий безопасности информационных систем  |
| 2.8. | Нерегламентированное подключение неучтенных внутренних и (или) периферийных устройств и носителей информации |
| 2.9. | Нерегламентированное изменение аппаратной конфигурации компьютерного оборудования |
| 2.10. | Нерегламентированное копирование информации (файлов) на флеш-накопители или иные внешние носители информации, а также нерегламентированная передача подобной информации с использованием сервисов электронной почты, мгновенных сообщений (ICQ и т.п.) и других сервисов сети Интернет |
| 2.11. | Нерегламентированная установка (удаление) прикладного программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах |
| 2.12. | Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем (повышение уровня прав доступа, получение прав на отладку программ и т.п.) |
| 2.13. | Заражение программного обеспечения рабочих станций и серверов вредоносным кодом (непреднамеренное) |
| 2.14. | Нерегламентированное использование сканирующего (на различные уязвимости) программного обеспечения |
| 2.15. | Нерегламентированное использование анализаторов протоколов (снифферов) |  |
| 2.16. | Нерегламентированный просмотр, вывод на печать, передача третьим лицам сведений, содержащих конфиденциальные данные (информацию, подлежащую защите) |  |
| 2.17. | Несанкционированное проведение обновления версий системного и прикладного программного обеспечения |  |
| **3. Haрушения, имеющие признаки преступления** |  |
| 3.1. | Несанкционированное получение привилегированного доступа к любым элементам информационной инфраструктуры Организации |  |
| 3.2. | Несанкционированное изменение конфигурации элементов информационной инфраструктуры Организации |  |
| 3.3. | Утрата резервных копий |  |
| 3.4. | Утечка конфиденциальной информации (баз данных информационных систем и др.) |  |
| 3.5. | Подозрение в умышленном нарушении работоспособности информационной сети Организации, элементов информационной инфраструктуры Организации, системного и прикладного программного обеспечения |  |
| 3.6. | Юридически необоснованная передача (распространение) конфиденциальной информации |  |
| 3.7. | Несанкционированное внесение изменений в базы данных информационных систем Организации |  |
| 3.8. | Несанкционированное уничтожение конфиденциальной информации |  |
| 3.9. | Проведение обновления версии информационных систем Организации (равно как и другого программного обеспечения), повлекшее за собой потерю конфиденциальной информации |  |
| 3.10. | Намеренное заражение информационных систем Организации вредоносным кодом |  |

 Приложение 19

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**ЖУРНАЛ**

**учёта съемных носителей конфиденциальной информации (персональных данных)**

**в Администрации сельского поселения Алябьевский**

На \_\_\_\_\_ лист\_\_\_

Начат: «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

Окончен: «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

Ответственный \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №п/п | Регистрацион-ный номер/дата | Тип/ёмкость машинного носителя персональных данных | Номер экземпляра/количество экземпляров | Место установки (использова-ния)/дата установки | Ответственное должностное лицо (Ф.И.О.) | Расписка в получении (Ф.И.О., подпись, дата) | Расписка в обратном приеме (Ф.И.О., подпись, дата) | Место хранения машинного носителя персональных данных | Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата) |
| 1. |  |  |  |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |  |  |  |
| 3. |  |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |  |
| № |  |  |  |  |  |  |  |  |  |

Приложение 20

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**ЖУРНАЛ**

**учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в информационной системе персональных данных Администрации сельского поселения Алябьевский**

На \_\_\_\_\_ лист\_\_\_

Начат: «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

Окончен: «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

Ответственный \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Ф.И.О. субъекта | Дата обращения | Цель обращения | Отметка об исполнении | Ф.И.О. исполнителя | Роспись |
| 1. | 2 | 3 | 4 | 5 | 6 | 7 |
| 2. |  |  |  |  |  |  |
| 3. |  |  |  |  |  |  |
| … |  |  |  |  |  |  |
| № |  |  |  |  |  |  |

Приложение 21

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**ЖУРНАЛ**

**учета инцидентов информационной безопасности**

**в Администрации сельского поселения Алябьевский**

На \_\_\_\_\_ лист\_\_\_

Начат: «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

Окончен: «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

Ответственный \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Дата инцидента | №, дата справки или акта по результатамрасследования или краткое содержаниеинцидента | Ф.И.О. проверяющего | Подписьпроверяющего |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| 3. |  |  |  |  |
| … |  |  |  |  |
| № |  |  |  |  |

Приложение 22

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Положение об уничтожении персональных данных,**

**обрабатываемых в Администрации сельского поселения Алябьевский**

1. **Общие положения**

1.1. Целью данного Положения является определение порядка уничтожения персональных данных, обрабатываемых в Администрации сельского поселения Алябьевский (далее администрация).

1.2. Настоящее Положение разработано с учетом положений Конституции Российской Федерации, Федеральных законов от 27 июля 2006 года № 152-ФЗ «О персональных данных» и от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлений Правительства Российской Федерации
от 15 сентября 2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3. Настоящее Положение является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным, обрабатываемым в администрации.

1. **Организация уничтожения персональных данных**

2.1. Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2.2. Персональные данные, обрабатываемые и хранящиеся в администрации, подлежат уничтожению в случае:

достижения цели обработки персональных данных или утраты необходимости в их обработке;

выявления неправомерных действий с персональными данными и невозможности устранения допущенных нарушений;

отзыва субъектом персональных данных согласия на обработку своих персональных данных;

истечения срока хранения персональных данных.

2.3. Решение об уничтожении персональных данных принимается комиссией
по уничтожению носителей, содержащих персональные данные (далее Комиссия).

Основной функцией Комиссии является организация и проведение отбора
и подготовки документов, электронных носителей к передаче на уничтожение.

Комиссия создается распоряжением Администрацией сельского поселения Алябьевский, которым определяются состав комиссии и порядок ее работы.

Состав Комиссии утверждается распоряжением Администрации сельского поселения Алябьевский. Все члены комиссии при принятии решений обладают равными правами.

Комиссия производит отбор персональных данных, подлежащих уничтожению, и включает их в Акт уничтожения документов, содержащих персональные данные, или в Акт уничтожения носителей персональных данных.

После этого документы (электронные носители), перечисленные в них, отделяются от остальных дел и хранятся в специально отведенном месте до уничтожения. Приготовленные к уничтожению персональные данные (их носители), передаются на переработку специализированной организации или уничтожаются в администрации.

Использование персональных данных, включенных в акты уничтожения, запрещено.

2.4. Комиссия обязана принять решение об уничтожении соответствующих персональных данных в срок, не превышающий трех рабочих дней, с момента их выявления.

2.5. О решении об уничтожении персональных данных Комиссия обязана уведомить субъект персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

2.6. Ответственным за организацию и проведение мероприятий по уничтожению персональных данных (их носителей) в администрация является Комиссия.

1. **Виды уничтожения конфиденциальной информации**

Уничтожение персональных данных делится на два вида:

плановое уничтожение конфиденциальной информации. Уничтожение планируется заранее, назначается комиссия, отбираются носители с информацией, подлежащей уничтожению, определяется день, место и время уничтожения;

экстренное уничтожение конфиденциальной информации. Уничтожение производится экстренно под воздействием неблагоприятных событий (в военной области - внезапное нападение, когда создается реальная угроза захвата противником важных документов и их компрометации).

1. **Способы уничтожения персональных данных**

В зависимости от типа носителя информации (бумажный или электронный) выделяют два способа уничтожения персональных данных:

физическое уничтожение носителя;

уничтожение информации с носителя.

4.1. Физическое уничтожение носителя.

Бумажный носитель: используются 2 вида уничтожения - уничтожение через шредирование (измельчение и гидрообработка) и уничтожение через термическую обработку (сжигание).

Электронный носитель: уничтожение заключается в таком воздействии на рабочие слои дисков, в результате, которого разрушается физическая, магнитная или химическая структура рабочего слоя: механическое разрушение дисков (прессование, механическое эрозирование поверхности - пескоструй, ультразвуковое и электрохимическое эрозирование), химическое травление в агрессивных средах и обжиг или переплавка дисков. Съём данных с магнитных дисков, подвергшихся таким воздействиям, становится невозможным.

4.2. Уничтожение информации с носителя.

Алгоритм уничтожения персональных данных основывается на многократной перезаписи в секторах магнитного диска. С физической точки зрения, они основываются на многократном перемагничивании материала записывающей поверхности диска.

Алгоритмы национальных стандартов предусматривают запись в каждый байт каждого сектора жесткого диска единиц, случайных чисел, а также чисел, дополнительных
к записанным на предыдущем проходе. Предполагается несколько перезаписей для одного материального носителя.

Стандарты уничтожения данных:

ГОСТ P50739-95;

DoD 5220.22-M; NAVSO P-5239-26 (RLL);

NAVSO P-5239-26 (MFM);

VSITR.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Утверждаю:

глава сельского поселения Алябьевский

\_\_\_\_\_\_\_\_\_\_Ю.А. Кочурова

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_г.

**АКТ №\_\_\_**

**об уничтожении носителей, содержащих персональные данные**

Комиссия в составе:

Председатель – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

провела отбор бумажных, электронных, магнитных носителей персональных данных и другой конфиденциальной информации (далее носители) и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации подлежит гарантированному уничтожению и составила настоящий акт о том, что произведено уничтожение носителей персональных данных в составе:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №п/п | Дата | Тип носителя | Учетный номер носителя | Примечание |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Всего носителей:

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

(цифрами и прописью количество)

На указанных носителях персональные данные уничтожены путем

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

(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПДн уничтожены путем

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

(разрезания/сжигания/размагничивания/физического уничтожения/ механического уничтожения / иного способа)

Председатель комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_/

Члены комиссии: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_/

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_/

Приложение 23

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**Правила работы с обезличенными персональными данными**

**Администрации сельского поселения Алябьевский**

**1. Общие положения**

Настоящие Правила работы с обезличенными персональными данными Администрации сельского поселения Алябьевский (далее администрация) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 21.03.2012 № 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» и определяют порядок работы с обезличенными данными Администрации сельского поселения Алябьевский.

**2. Термины и определения**

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в настоящих Правилах используются следующие понятия:

персональные данные - любая информация, относящаяся прямо или косвенно
к определенному или определяемому физическому лицу (субъекту персональных данных);

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

обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**3. Условия обезличивания**

3.1. 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 достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. 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 населенный пункт)

деление сведений на части и обработка в разных информационных системах;

другие способы.

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

3.4. Перечень должностей муниципальных служащих администрации, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приведен в приложении 1 к Правилам работы с обезличенными персональными данными администрации:

глава сельского поселения Алябьевский принимает решение о необходимости обезличивания персональных данных;

руководители структурных подразделений администрации, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания;

муниципальные служащие структурных подразделений администрации, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

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

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

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

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

парольной политики;

антивирусной политики;

правил работы со съемными носителями (если они используется);

правил резервного копирования;

правил доступа в помещения, где расположены элементы информационных систем.

4.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

правил хранения бумажных носителей;

правил доступа к ним и в помещения, где они хранятся.

Приложение 1

к Правилам работы

с обезличенными персональными данными

Администрации сельского

поселения Алябьевский

**Перечень**

**должностей Администрации сельского поселения Алябьевский, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных**

* + - 1. Глава сельского поселения Алябьевский.
			2. Заместитель главы сельского поселения Алябьевский.
			3. Ведущий специалист (управляющий делами).
			4. Ведущий специалист (отдел кадров).
			5. Ведущий специалист по жилищным отношениям и муниципальному имуществу.
			6. Ведущий специалист по юридическим вопросам.
			7. Начальник финансово-экономического отдела.
			8. Главный специалист финансово-экономического отдела.
			9. Техник-землеустроитель.
			10. Старший инспектор по мобилизационной подготовке.
			11. Инженер-программист.

Приложение 24

к постановлению Администрации

сельского поселения Алябьевский

от 29.05.2020 г. № 82

**ЖУРНАЛ**

**ознакомления служащих, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локально-нормативными актами по защите персональных данных в Администрации сельского поселения Алябьевский**

На \_\_\_\_\_ лист\_\_\_

Начат: «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

Окончен: «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

Ответственный \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Фамилия, имя, отчество | Должность | Дата | Подпись |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| 3. |  |  |  |  |
| … |  |  |  |  |
| № |  |  |  |  |