РОССИЙСКАЯ ФЕДЕРАЦИЯ
КАМЧАТСКИЙ КРАЙ
ЕЛИЗОВСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН
РАЗДОЛЬНЕНСКОЕ СЕЛЬСКОЕ ПОСЕЛЕНИЕ

П О С Т А Н О В Л Е Н И Е

Администрации Раздольненского сельского поселения

от «13» ноября 2023 года № 195
п. Раздольный

Об утверждении муниципальных правовых актов, регулирующих вопросы обработки и защиты персональных данных в Администрации Раздольненского сельского поселения

В целях осуществления мероприятий по защите и обеспечению безопасности персональных данных при их обработке, в том числе в информационных системах, в Администрации Раздольненского сельского поселения в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением 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», руководствуясь Уставом Раздольненского сельского поселения, Администрация Раздольненского сельского поселения

ПОСТАНОВЛЯЕТ:

1. Утвердить муниципальные правовые акты, регулирующие вопросы обработки и защиты персональных данных в администрации Раздольненского сельского поселения:

1.1. Правила обработки персональных данных в администрации Раздольненского сельского поселения (Приложение № 1);

1.2. Положение об обеспечении безопасности персональных данных в администрации Раздольненского сельского поселения (Приложение № 2);

1.3. Правила работы с обезличенными персональными данными в администрации Раздольненского сельского поселения (Приложение № 3);

1.4. Перечни персональных данных, обрабатываемых в администрации Раздольненского сельского поселения в связи с реализацией трудовых

отношений, а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций (Приложение № 4);

1.5. Перечень должностей в администрации Раздольненского сельского поселения, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных (Приложение № 5);

1.6. Перечень должностей в администрации Раздольненского сельского поселения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (Приложение № 6);

1.7. Форма обязательства о неразглашении информации, содержащей персональные данные в администрации Раздольненского сельского поселения (Приложение № 7);

1.8. Типовая форма согласия на обработку персональных данных в администрации Раздольненского сельского поселения (Приложение № 8);

1.9. Порядок доступа в помещения, в которых ведётся обработка персональных данных, в администрации Раздольненского сельского поселения (Приложение № 9);

1.10. Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации Раздольненского сельского поселения (Приложение № 10);

1.11. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение № 11).

1.12. Инструкция по организации антивирусной защиты в информационных системах персональных данных администрации Раздольненского сельского поселения (Приложение № 12);

1.13. Границы контролируемой зоны информационных систем персональных данных администрации Раздольненского сельского поселения (Приложение № 13);

1.14. Порядок реагирования на инциденты информационной безопасности в администрации Раздольненского сельского поселения (Приложение № 14);

1.15. Инструкция должностного лица, ответственного за организацию обработки персональных данных в информационных системах персональных данных (Приложение № 15);

1.16. Инструкция пользователя информационной системы персональных данных в администрации Раздольненского сельского поселения (Приложение № 16);

1.17. Инструкция должностного лица, ответственного за обеспечение безопасности персональных данных (Приложение № 17);

1.18. Форма журнала проведения инструктажей по информационной безопасности (Приложение № 18);

1.19. Форма журнала учета средств защиты информации в информационных системах персональных данных (Приложение № 19);

1.20. Форма журнала периодического тестирования средств защиты информации в информационных системах персональных данных (Приложение № 20);

1.21. Форма журнала учета мероприятий по контролю обеспечения защиты информации в информационных системах персональных данных (Приложение № 21);

1.22. Перечень информационных систем персональных данных (Приложение № 22).

2. Опубликовать (обнародовать) настоящее постановление в порядке, установленном для опубликования муниципальных правовых актов, а также разместить в сети Интернет на официальном сайте https://www.kamgov.ru/emr/razdolnoe.

3. Настоящее постановление вступает в силу после дня его официального опубликования.

Глава администрации
Раздольненского сельского поселения Л.В. Аносова

Приложение № 1
к постановлению администрации Раздольненского сельского поселения
от 13.11.2023 № 195

Правила
обработки персональных данных в администрации Раздольненского сельского поселения

1. Общие положения

1.1. Настоящие Правила обработки персональных данных в администрации Раздольненского сельского поселения (далее – Правила) определяют категории субъектов, персональные данные которых обрабатываются, цели обработки персональных данных, порядок обработки персональных данных, меры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных и на обеспечение защиты персональных данных, обязанности по защите персональных данных и порядок доступа к персональным данным, сроки обработки и хранения персональных данных, порядок уничтожения персональных данных, порядок распространения персональных данных.

1.2. Администрация Раздольненского сельского поселения (далее – администрация) является оператором, организующим и осуществляющим обработку персональных данных следующих категорий субъектов персональных данных:

1) муниципальные служащие;

2) граждане, претендующие на замещение должностей муниципальной службы;

3) работники администрации, замещающие должности, не являющиеся должностями муниципальной службы (далее - работники администрации);

4) граждане, претендующие на замещение должностей, не являющихся должностями муниципальной службы;

5) лица, замещающие должности руководителей организаций, подведомственных администрации (далее - руководители организаций);

6) граждане, претендующие на замещение должностей руководителей организаций;

7) лица, состоящие в родстве (свойстве) с субъектами персональных данных, указанными в подпунктах 1 - 6 настоящего пункта;

8) лица, представляемые к награждению муниципальными наградами, к поощрению Главой администрации Раздольненского сельского поселения, наградные материалы по которым представлены в администрацию;

9) заявители, обратившиеся в администрацию в соответствии с Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

10) пользователи информацией, обратившиеся в администрацию в соответствии с Федеральным законом от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;

11) граждане, обратившиеся в администрацию в соответствии с Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

12) иные лица, персональные данные которых должны обрабатываться в соответствии с федеральным законодательством, законодательством Камчатского края, муниципальными правовыми актами.

1.3. Лицо, ответственное за организацию обработки персональных данных в администрации, назначается правовым актом администрации Раздольненского сельского поселения.

1.4. Понятия, используемые в настоящих Правилах, применяются в тех же значениях, что и в Федеральных законах от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Порядок обработки персональных данных в администрации Раздольненского сельского поселения

2.1. Обработку персональных данных в администрации осуществляют муниципальные служащие и иные должностные лица, замещение должностей которых предусматривает осуществление обработки персональных данных. Перечень должностей муниципальных служащих и должностей служащих администрации, замещение которых предусматривает осуществление обработки персональных данных (далее – уполномоченные работники), утверждается правовым актом администрации.

Обработка персональных данных осуществляется как с использованием средств автоматизации, так и без использования средств автоматизации.

2.2. Обработка персональных данных основывается на принципах обработки персональных данных, установленных Федеральным законом «О персональных данных».

2.3. Обработка персональных данных осуществляется в целях:

1) организации деятельности администрации Раздольненского сельского поселения для обеспечения соблюдения законов и иных нормативно-правовых актов, реализации права на труд;

2) осуществления, возложенных на администрацию Раздольненского сельского поселения функций, полномочий и обязанностей в связи с оказанием муниципальных услуг и осуществлением муниципальных функций;

3) в иных целях, предусмотренных федеральным законодательством.

2.4. Субъект персональных данных предоставляет свои персональные данные администрации (далее также – Оператор) и дает согласие на их обработку самостоятельно либо через своего представителя. Согласие на обработку персональных данных может быть дано в любой форме, позволяющей подтвердить указанный факт, если иное не установлено

федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Оператором.

В случае отказа субъекта персональных данных на предоставление своих персональных данных ему может быть дано разъяснение юридических последствий отказа предоставить свои персональные данные.

2.5. В случае возникновения необходимости получения персональных данных субъекта персональных данных у третьей стороны Оператор обязан известить об этом субъекта персональных данных заранее, получить его письменное согласие и сообщить о целях, предполагаемых источниках и способах получения персональных данных.

2.6. В администрации не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных Федеральным законом «О персональных данных». Если обработка специальных категорий персональных данных осуществлялась, то она должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась указанная обработка, если иное не установлено федеральным законом.

2.7. В администрации могут быть использованы информационные системы для учета и обработки персональных данных с учетом особенностей, установленных статьей 13 Федерального закона «О персональных данных».

2.8. Срок обработки персональных данных определяется периодом времени, в течение которого Оператор осуществляет действия (операции) в отношении персональных данных, обусловленные заявленными целями их обработки.

2.9. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. При несовместимости целей обработки персональных данных, не допускается объединение баз данных.

При этом, если персональные данные зафиксированы на одном материальном носителе и указанное 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:

а) 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;

б) 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.

2.10. Обработка персональных данных осуществляется с момента их получения Оператором и прекращается:

– по достижении целей обработки;

– в связи с отсутствием необходимости в достижении заранее заявленных целей обработки;

– в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных.

2.11. Передача персональных данных может осуществляться Оператором на основании письменных запросов, в том числе запросов в форме электронного документа, а также в рамках заключенных письменных договоров (соглашений).

Основанием передачи персональных данных органам государственной власти, органам местного самоуправления, судебным органам, органам прокуратуры и следствия, физическим и юридическим лицам является:

– наличие норм законодательства, регламентирующих порядок и случаи передачи персональных данных;

– наличие письменного согласия субъекта персональных данных на обработку (в том числе передачу) его персональных данных.

2.12. При передаче персональных данных уполномоченный работник должен соблюдать следующие требования:

– не сообщать персональные данные третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, прямо установленных законодательством Российской Федерации;

– уведомить получающих их лиц о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены;

– уведомить субъекта персональных данных о факте их передачи;

– не вносить в материальные и электронные носители персональных данных какие-либо пометки, исправления, не вносить новые записи, не извлекать документы или помещать новые, если это нарушает порядок обработки персональных данных.

2.13. При обработке персональных данных Оператор обязан принимать следующие правовые, организационные и технические меры по обеспечению безопасности персональных данных:

– определение типа угроз безопасности персональных данных и соответствующего ему уровня защищенности персональных данных при их обработке;

– разработка в соответствии с актуальными угрозами системы защиты персональных данных для соответствующего уровня защищённости информационных систем;

– учет машинных носителей персональных данных;

– установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации;

– применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на машинных носителях информации;

– осуществление антивирусного контроля, предотвращение внедрения в информационную систему вредоносных программ (программ-вирусов) и программных закладок;

– применение межсетевого экранирования;

– обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

– централизованное управление системой защиты персональных данных;

– резервное копирование информации;

– восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– обучение уполномоченных работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

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

– контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

2.14. Защита персональных данных субъектов персональных данных в администрации от неправомерного их использования или утраты обеспечивается за счет средств, предусмотренных на содержание муниципального органа.

2.15. Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка) может осуществляться в виде документов на бумажных носителях.

При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

При неавтоматизированной обработке персональных данных на бумажных носителях:

– не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;

– персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

– документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

– дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

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).

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.

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.

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.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

2.16. Хранение, блокирование, обезличивание, прекращение обработки, уточнение и уничтожение персональных данных осуществляется в соответствии с разделом 5 настоящих Правил.

3. Меры, направленные на обеспечение выполнения требований законодательства Российской Федерации в сфере персональных данных

3.1. В администрации принимаются меры для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам относятся:

– назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;

– осуществление внутреннего контроля соответствия обработки персональных данных нормам Федерального закона «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, правовым актам, принятым в администрации;

– оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных указанным Федеральным законом;

– ознакомление должностных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и обучение ответственных должностных лиц Оператора;

– определение перечня муниципальных служащих и иных должностных лиц, имеющих доступ к персональным данным.

4. Обязанности уполномоченных работников по защите персональных данных

4.1. Уполномоченные работники обязаны:

– знать и выполнять требования законодательства Российской Федерации в области обеспечения защиты персональных данных, в том числе соблюдать настоящие Правила;

– хранить в тайне известные им персональные данные, информировать руководителя структурного подразделения о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;

– соблюдать порядок хранения и уничтожения персональных данных, исключить доступ к ним посторонних лиц;

– обрабатывать только те персональные данные, к которым получен доступ в силу исполнения должностных обязанностей.

4.2. При обработке персональных данных уполномоченным работникам запрещается:

– использовать сведения, содержащие персональные данные, в неслужебных целях, а также в служебных целях – при ведении переговоров по телефонной сети, в открытой переписке, статьях и выступлениях;

– передавать персональные данные по незащищенным каналам связи (факсимильная связь, электронная почта и т.п.) либо без использования сертифицированных средств криптографической защиты информации;

– снимать копии с документов и других носителей информации, содержащих персональные данные, или производить выписки из них, а равно использовать различные технические средства (видео- и звукозаписывающую аппаратуру) для фиксации сведений, содержащих персональные данные, в неслужебных целях;

– выносить документы и другие носители информации, содержащие персональные данные, из администрации.

5. Порядок хранения, блокирования, обезличивания, прекращения обработки, уточнения и уничтожения персональных данных

5.1. Персональные данные хранятся на бумажных или материальных носителях информации (компакт-диск, флэш-карта, дискета), а также в электронной форме в специализированном программном обеспечении в администрации Раздольненского сельского поселения.

5.2. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если иной срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.3. В случае достижения целей обработки персональных данных, в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных, а также в случае утраты необходимости в их достижении уполномоченный работник обязан:

– незамедлительно прекратить или обеспечить прекращение обработки персональных данных;

– уничтожить соответствующие персональные данные или обеспечить их уничтожение в срок, не превышающий 30 дней с даты достижения целей обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

5.4. Обезличивание или уничтожение части персональных данных, если это допускается бумажным носителем, производится закрашиванием, вырезанием или иным способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных персональных данных, зафиксированных на бумажном носителе.

5.5. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных уполномоченный работник обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченный работник обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

5.6. В случае подтверждения факта неточности персональных данных уполномоченный работник на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

5.7. В случае выявления неправомерной обработки персональных данных, уполномоченный работник в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченный работник в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных

нарушений или об уничтожении персональных данных уполномоченный работник обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5.8. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор обязан с момента выявления такого инцидента Оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5.9. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных, уполномоченный работник обязан прекратить обработку персональных данных или обеспечить прекращение такой обработки и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

5.10. В случае обращения субъекта персональных данных с требованием о прекращении обработки персональных данных уполномоченный работник обязан в срок, не превышающий десяти рабочих дней с даты получения соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона «О персональных данных». Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае

направления в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

5.11. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 6.4, 6.8, 6.10 настоящих Правил, уполномоченный работник осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.12. Документы, содержащие персональные данные, при достижении целей обработки или при наступлении других законных оснований, не подлежащие архивному хранению, подлежат уничтожению способом, исключающим дальнейшую обработку персональных данных. 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 информации.

5.13. Контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению, осуществляется специалистом, назначенным правовым актом администрации.

5.14. Вопрос об уничтожении персональных данных рассматривается комиссией, созданной администрацией. По итогам заседания комиссии составляется протокол.

5.15. По окончании процедуры уничтожения персональных данных составляется акт об уничтожении персональных данных.

6. Правила рассмотрения запросов субъектов персональных данных

6.1. Правила рассмотрения запросов субъектов персональных данных оформляются отдельным документом и утверждаются главой администрации Раздольненского сельского поселения.

7. Лица, осуществляющие обработку персональных данных и ответственные за их обработку

7.1. Перечень должностей муниципальной службы, иных должностей, при замещении которых должностные лица допускаются к обработке персональных данных и имеют доступ к персональным данным, утверждается правовым актом администрации Раздольненского сельского поселения.

Должностные лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящими Правилами и подписывают обязательство о неразглашении информации, содержащей персональные данные.

7.2. Ответственный за организацию обработки персональных данных в администрации Раздольненского сельского поселения назначается правовым актом администрации Раздольненского сельского поселения из числа

муниципальных служащих администрации Раздольненского сельского поселения.

Инструкция ответственного за обработку персональных данных утверждается правовым актом администрации Раздольненского сельского поселения.

Ответственный за организацию обработки персональных под роспись знакомиться с инструкцией ответственного за организацию обработки персональных данных.

8. Правила работы с обезличенными данными

8.1. Правила работы с обезличенными персональными данными оформляются отдельным документом и утверждаются правовым актом администрации Раздольненского сельского поселения.

8.2. Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, оформляется отдельным документом и утверждается правовым актом администрации Раздольненского сельского поселения.

9. Порядок доступа в помещения, в которых ведется обработка персональных данных

9.1. Порядок доступа в помещения, в которых ведётся обработка персональных данных оформляется в виде отдельного документа и утверждается правовым актом администрации Раздольненского сельского поселения.

10. Правила осуществления внутреннего контроля

10.1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к обеспечению безопасности персональных данных оформляются отдельным документом и утверждаются правовым актом администрации Раздольненского сельского поселения.

Приложение № 2
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Положение
об обеспечении безопасности персональных данных в администрации Раздольненского сельского поселения

1. В настоящем Положении используются основные понятия в соответствии со статьей 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Используемые сокращения

В настоящем Положении использованы следующие сокращения:

ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ПДн	Персональные данные
СКЗИ	Средство криптографической защиты нформации
СЗПДн	Система защиты персональных данных

3. Область применения

Настоящее Положение об обеспечении безопасности персональных данных в администрации Раздольненского сельского поселения (далее - Положение) предназначено для применения при организации и проведении работ по обеспечению безопасности персональных данных, в том числе в информационных системах, в администрации Раздольненского сельского поселения (далее по тексту - администрация).

Требования настоящего Положения распространяются на сотрудников администрации, принимающих участие в обеспечении безопасности персональных данных.

4. Общие положения

Настоящее Положение определяет содержание и порядок осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных (ИСПДн) администрации, представляющей собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных как с использованием средств автоматизации, так и без использования таких средств.

Безопасность персональных данных при их обработке в ИСПДн достигается путем снижения вероятности осуществления НСД к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

При обработке персональных данных в ИСПДн должно быть обеспечено:

– проведение мероприятий, направленных на предотвращение НСД к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

– своевременное обнаружение фактов НСД к персональным данным;

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

– возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним;

– непрерывный контроль и анализ уровня защищенности персональных данных.

Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных (СЗПДн), включающей организационные мероприятия и средства защиты информации (в том числе криптографические средства, средства предотвращения НСД, программно-технических воздействий на технические средства обработки ПДн), а также используемые в ИСПДн информационные технологии.

Обеспечение безопасности персональных данных в администрации осуществляется на основе следующих принципов:

– соответствие мер и средств защиты актуальным угрозам безопасности;

– построение и модернизация СЗПДн в администрации производится на основе анализа угроз безопасности персональных данных с учетом специфических особенностей ИСПДн;

– соответствие мер и средств защиты требованиям нормативных документов РФ - в администрации используются меры и средства обеспечения безопасности персональных данных в строгом соответствии с действующими нормативными правовыми актами РФ в области обработки и защиты персональных данных;

– комплексность - с целью обеспечения безопасности персональных данных в администрации используется совокупность организационных мер и технических средств защиты;

– патентная чистота - средства защиты информации, входящие в состав СЗПДн, отвечают требованиям по обеспечению патентной чистоты согласно действующим нормативным документам РФ. Используемое общесистемное, специальное и прикладное программное обеспечение имеет соответствующие лицензии производителей;

– удобство пользователей - при построении и модернизации СЗПДн учитываются и по возможности сводятся к минимуму возможные трудности пользователей в работе со средствами защиты и с основными процедурами обеспечения безопасности персональных данных;

– постоянное совершенствование - осуществляется регулярный внутренний контроль выполнения требований по обработке и обеспечению безопасности персональных данных, эффективности применяемых организационных мер и технических средств защиты и уровня защищенности персональных данных, а также регулярно пересматриваются состав угроз и

уровень защищенности ПДн, на основании чего принимаются меры по устранению выявленных недостатков и модернизации/совершенствованию СЗПДн.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в ИСПДн оценивается при проведении государственного контроля и надзора.

Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн администрации включают в себя:

– определение уровня защищенности обрабатываемых ПДн, в том числе отслеживание изменений состояния ИСПДн, которые могут повлиять на классификационные признаки ИСПДн (уровень защищенности ПДн);

– определение угроз безопасности персональных данных при их обработке в ИСПДн;

– разработка на основании определенных угроз и поддержание в актуальном состоянии частной модели безопасности угроз безопасности персональных данных при обработке их в ИСПДн;

– разработку на основе частной модели угроз системы защиты персональных данных (СЗПДн), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для установленного уровня защищенности ПДн;

– установку и ввод в эксплуатацию СЗИ, входящих в состав СЗПДн, в соответствии с проектными решениями по созданию СЗПДн, эксплуатационной и технической документацией к данным СЗИ;

– обучение лиц, использующих СЗИ, входящие в состав СЗПДн, правилам работы с ними;

– учет применяемых СЗИ, входящих в состав СЗПДн, эксплуатационной и технической документации к ним;

– учет носителей персональных данных;

– учет лиц, допущенных к работе с персональными данными в ИСПДн;

– контроль соблюдения условий использования СЗИ, входящих в состав СЗПДн, предусмотренных эксплуатационной и технической документацией к ним;

– разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования СЗИ, входящих в состав СЗПДн, которые могут привести к нарушению заданных характеристик безопасности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– описание состава и режима функционирования компонентов СЗПДн (описание СЗПДн).

Размещение компонентов ИСПДн, охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и СЗИ, входящих в состав СЗПДн, а также исключать

возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Настоящее Положение должно быть доведено до всех работников администрации, участвующих в обеспечении безопасности персональных данных, под роспись.

5. Стадии создания СЗПДн

В администрации обеспечение безопасности персональных данных осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках следующих стадий создания и совершенствования СЗПДн: предпроектная стадия; стадия проектирования; стадия приемки и ввода в действие; модернизация СЗПДн.

СЗПДн включает организационные меры, технические средства защиты информации, а также используемые в ИСПДн информационные технологии, реализующие функции защиты информации.

Выполнение всех вышеуказанных стадий должно проходить по согласованию с должностным лицом, ответственным за организацию работ по обработке персональных данных.

Выполнение всех вышеуказанных стадий должно проходить под контролем должностного лица, ответственного за проведение работ по защите персональных данных.

5.1. Описание требований к предпроектной стадии создания СЗПДн

Целью предпроектной стадии создания СЗПДн является:

– определение категории субъектов персональных данных, чьи данные обрабатываются в администрации, состава и объема обрабатываемых персональных данных, а также цели и правовое основание обработки этих данных;

– определение должностных лиц, участвующих в обработке персональных данных;

– определение угроз безопасности персональных данных применительно к конкретным условиям функционирования ИСПДн;

– определение уровня защищенности ПДн.

Для достижения указанных целей проводится анализ информационных систем администрации, содержащих персональные данные, и определяются все внутренние и внешние процессы обработки персональных данных, осуществляемые как с использованием средств автоматизации, так и без использования таковых.

По результатам предпроектной стадии определяется степень выполнения требований нормативно-правовых документов в области защиты персональных данных, а также разрабатывается план необходимых дальнейших организационных и технических мероприятий по реализации данных требований.

Должностное лицо, ответственное за проведение работ по защите персональных данных, определяет необходимость проведения тех или иных мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели предпроектной стадии.

- Определение обрабатываемых персональных данных

В ходе предпроектной стадии по результатам анализа процессов обработки персональных данных в администрации определяются состав, цели, правовое основание обработки персональных данных и сроки хранения обрабатываемых персональных данных.

На основании полученных данных формируется документ «Перечень персональных данных, обрабатываемых в администрации Раздолненского сельского поселения».

- Определение перечня должностных лиц, допущенных к работе с персональными данными

В ходе предпроектной стадии по результатам анализа процессов обработки персональных данных в администрации определяется перечень лиц, которым необходим доступ к персональных данных для выполнения трудовых обязанностей, а также перечень лиц, которые в рамках выполнения своих трудовых обязанностей имеют право доступа к ресурсам, содержащим персональные данные, без права ознакомления с персональными данными.

На основании полученных данных формируется перечень должностных лиц, допущенных в помещения и к работе со средствами вычислительной техники из состава ИСПДн администрации, который утверждается соответствующим правовым актом администрации.

- Определение конфигурации и топологии ИСПДн

В ходе обследования информационных систем персональных данных администрации определяются все базы данных (хранилища) и отчуждаемые носители информации и содержащиеся в них персональных данных.

Кроме того, определяются конфигурация и топология ИСПДн в целом и ее отдельных компонентов, а именно, перечень серверного оборудования, автоматизированных рабочих мест, общесистемных и прикладных программных средств, задействованных при обработке персональных данных, перечень применяемых средств защиты информации, а также сетевая инфраструктура и перечень сетевого оборудования.

- Определение угроз безопасности персональных данных

С целью определения необходимых мер и средств защиты, соответствующих актуальным угрозам безопасности персональных данных при их обработке в ИСПДн администрации, проводится анализ и оценка вероятности реализации и величины негативных последствий вследствие реализации угроз безопасности персональных данных при их обработке в ИСПДн.

В администрации составляется частная модель угроз безопасности персональных данных, которая разрабатывается на основании:

– ГОСТ Р 51275-2006 «Защита информации. Факторы, воздействующие на информацию. Общие положения»;

– Базовой модели угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 15.02.2008 заместителем директора ФСТЭК России;

– Методики определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 14.02.2008 заместителем директора ФСТЭК России;

– Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/54-144).

- Определение уровня защищенности ПДн

Определение уровня защищенности ПДн осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». При определении уровня защищенности ПДн используется модель угроз безопасности ПДн, в которой проведен анализ актуальных угроз безопасности ПДн.

5.2. Стадия проектирования СЗПДн

Цели проектирования СЗПДн:

– определить требования по обеспечению безопасности персональных данных;

– определить структуру и характеристики создаваемой СЗПДн, состав технических средств защиты информации, предполагаемых к использованию в СЗПДн, требования к настройке и эксплуатации этих средств, параметры их взаимодействия, а также план мероприятий по подготовке СЗПДн к вводу в действие;

– определить требования и регламентировать деятельность работников администрации по организации легитимной обработки персональных данных и обеспечению безопасности персональных данных, обрабатываемых как с использованием средств автоматизации, так и без использования таковых.

Для достижения указанных целей в администрации разрабатывается комплект организационно-распорядительных документов, определяющих требования и порядок действий при обработке и обеспечении безопасности персональных данных.

Должностное лицо, ответственное за проведение работ по защите персональных данных в администрации, определяет необходимость проведения мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели стадии проектирования СЗПДн.

- Определение требований по обеспечению безопасности персональных данных

По результатам предпроектной стадии, в зависимости от определенного уровня защищенности ПДн и определенного перечня актуальных угроз безопасности персональных данных, задаются конкретные требования по обеспечению безопасности ПДн при их обработке в ИСПДн Администрации, выполнение которых обеспечивает минимизацию вероятности реализации предполагаемых угроз безопасности персональных данных.

- Определение конфигурации СЗПДн

На основании требований, указанных выше, осуществляется проектирование СЗПДн, определяется состав и характеристики средств защиты информации, которые будут входить в состав создаваемой СЗПДн.

В администрации разрабатывается комплект организационно-распорядительной документации на СЗПДн, описывающей требования и процедуры по управлению и обеспечению безопасности персональных данных.

За разработку и, при необходимости, пересмотр организационно-распорядительной документации на СЗПДн в администрации отвечает должностное лицо, ответственное за проведение работ по обеспечению безопасности персональных данных в администрации.

5.3. Стадия ввода в действие СЗПДн

Цели стадии ввода в действие СЗПДн: внедрить технические средства защиты информации; проверить работоспособность средств защиты информации в составе ИСПДн; принять организационные меры по обеспечению безопасности персональных данных; ознакомить работников администрации с требованиями и обучить порядку обработки и обеспечения безопасности персональных данных.

Для достижения перечисленных целей выполняются следующие мероприятия:

– осуществляется закупка, установка и настройка средств защиты информации;

– проводятся опытная эксплуатация и приемо-сдаточные испытания средств защиты информации;

– утверждается и вводится в действие комплект организационно-распорядительных документов, определяющих требования и порядок действий при обработке и обеспечении безопасности персональных данных;

– проводится обучение работников по направлению обеспечения безопасности персональных данных.

Должностное лицо, ответственное за проведение работ по защите персональных данных в администрации, определяет необходимость проведения тех или иных мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели стадии ввода в действие СЗПДн.

- Внедрение средств защиты информации

Согласно требованиям, определенным в документации, осуществляется закупка, установка и настройка программных и технических средств защиты информации с составлением соответствующих актов установки.

Установка и ввод в эксплуатацию средств защиты информации осуществляется строго в соответствии с эксплуатационной и технической документацией к ним. Перед установкой средств защиты информации проверяется их готовность к использованию, и составляются заключения о возможности их эксплуатации.

В администрации необходимо применять средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия и имеющие соответствующие сертификаты ФСТЭК и ФСБ России.

- Внедрение организационных мер по обеспечению безопасности персональных данных

В администрации утверждается и вводится в действие комплект организационно-распорядительной документации на СЗПДн.

Все должностные лица, допущенные к обработке персональных данных, и лица, ответственные за обеспечение безопасности персональных данных, в обязательном порядке изучают организационно-распорядительные документы на СЗПДн в части, их касающейся, и руководствуются ими в своей работе.

Общий контроль за исполнением требований организационно-распорядительной документации на СЗПДн в администрации возлагается на должностное лицо, ответственное за обеспечение безопасности ПДн.

- Обучение работников по направлению обеспечения безопасности персональных данных

В администрации все работники, участвующие в обработке персональных данных, в обязательном порядке проходят обучение по следующим направлениям:

– общие вопросы обеспечения информационной безопасности;

– правила автоматизированной и неавтоматизированной обработки персональных данных и обеспечения безопасности персональных данных;

– правила использования прикладных систем и технических средств обработки персональных данных;

– правила использования средств защиты информации, входящих в состав СЗПДн;

– ответственность за нарушение правил обработки и обеспечения безопасности персональных данных.

Ответственным за организацию и контроль проведения обучения работников администрации, участвующих в обработке и обеспечении безопасности персональных данных, является должностное лицо, ответственное за обеспечение безопасности персональных данных в администрации.

Обучение может проводиться как самим должностным лицом, ответственным за обеспечение безопасности персональных данных в администрации, так и с привлечением сторонних организаций.

Новые работники администрации, принимаемые на работу, в обязательном порядке проходят первичный инструктаж. Ответственным за направление работника на первичный инструктаж является должностное лицо, ответственное за организацию работ по обработке персональных данных в администрации.

Перед допуском работников администрации к работе с ПДн должностное лицо ответственное за обеспечение безопасности ПДн проводит ознакомление с нормативной документацией, утвержденной в администрации в области безопасности ПДн.

5.4. Модернизация СЗПДн

В случаях изменения состава или структуры ИСПДн администрации, состава угроз безопасности персональных данных или уровня защищенности ПДн, обработка которых осуществляется в ИСПДн администрации, проводится модернизация СЗПДн.

6. Мероприятия по организации и обеспечению безопасности персональных данных

Под организацией обеспечения безопасности персональных данных при их обработке в ИСПДн администрации понимается формирование и реализация совокупности согласованных по целям, задачам, месту и времени

организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

Организационные мероприятия по обеспечению безопасности персональных данных в администрации включает в себя мероприятия по обеспечению охраны и физической защиты помещений, в которых расположены технические средства ИСПДн, исключающие несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности; обучение работников администрации правилам обработки и защиты персональных данных.

В целях осуществления технического обеспечения безопасности персональных данных при их обработке в ИСПДн администрации реализовываются мероприятия по защите от НСД к ПДн.

Планирование мероприятий по обеспечению безопасности персональных данных осуществляется в соответствии с Разделом 8 настоящего Положения.

6.1. Мероприятия по обеспечению управления доступом

- Общие требования

Для организации системы допуска и учета должностных лиц, допущенных к работе с персональными данными в администрации, должен быть определен перечень должностных лиц и утвержден соответствующим правовым актом администрации.

В администрации должна быть реализована разрешительная система допуска пользователей и разграничение прав доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации с помощью функциональных возможностей операционной системы, прикладных систем обработки персональных данных либо специализированных средств защиты информации.

Работникам администрации предоставляется доступ к ПДн и средствам их обработки в объеме, минимально необходимом для выполнения их трудовых обязанностей.

Для идентификации и аутентификации пользователей ИСПДн администрации должны применяться пароли условно-постоянного действия. Требования к формированию пароли и периодичности их смены определены в эксплуатационной документации на СЗПДн (Руководство администратора информационной безопасности, и Инструкция работника по правилам обработки ПДн).

- Порядок проведения мероприятий

Своевременное предоставление работникам администрации прав доступа к персональным данным и средствам их обработки, а также изменение их полномочий обеспечивает должностное лицо, ответственное за обеспечение безопасности ПДн в администрации.

Порядок генерации, смены и прекращения действия паролей в ИСПДн администрации определен в эксплуатационной документации на СЗПДн.

6.2. Мероприятия по обеспечению регистрации и учета

- Учет и хранение носителей ПДн

В администрации должен вестись учет как машинных, так и бумажных носителей ПДн. Также должно быть организовано хранение и использование этих носителей, исключающее их хищение, подмену и уничтожение.

В администрации учету подлежат следующие типы машинных носителей ПДн:

– отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD, BD и прочее);

– неотчуждаемые носители информации (жесткие магнитные диски).

- Порядок проведения мероприятий

Порядок учета, хранения, использования носителей персональных данных (машинных), а также порядок их уничтожения определены в документе «Регламент учета, хранения и уничтожения машинных носителей персональных данных в Администрации Раздольненского сельского поселения».

Ответственность за ведение учета машинных носителей персональных данных, организацию надлежащего хранения, а также уничтожение машинных носителей персональных данных возлагается на должностное лицо, ответственное за защиту ПДн.

Контроль и ответственность за ведение учета бумажных носителей персональных данных, организацию надлежащего хранения, а также уничтожение бумажных носителей персональных данных возлагается на должностное лицо, ответственное за организацию работ по обработке ПДн.

6.3. Мероприятия по обеспечению целостности

Сохранность и целостность программных средств ИСПДн и персональных данных являются обязательными и обеспечиваются, в том числе за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн.

В администрации должен быть определен и документально зафиксирован состав и назначение ПО, используемого в ИСПДн. Порядок внесения изменений в установленное ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО, должен быть регламентирован.

Эталонные копии ПО должны быть учтены, доступ к ним должен быть регламентирован.

С целью недопущения изменения состава ПО ИСПДн, из него должны быть исключены программные средства, предназначенные для разработки и отладки ПО (либо содержащие средства разработки, отладки и тестирования программно-аппаратного обеспечения).

Средства восстановления функций обеспечения безопасности персональных данных в ИСПДн должны предусматривать ведение не менее двух независимых копий программных средств.

В администрации должны быть реализованы механизмы восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним и/или возникновения форс-мажорных ситуаций или воздействия опасных факторов окружающей среды.

- Порядок проведения мероприятий

Порядок организации резервного копирования и восстановления массивов информации в администрации осуществляется в соответствии с законодательством РФ о защите персональных данных.

Ответственность за организацию своевременного резервного копирования и восстановления информации, а также за надлежащее хранение резервных носителей, содержащих резервные копии данных, возлагается на должностное лицо, ответственное за защиту ПДн.

6.4. Мероприятия по обеспечению антивирусной защиты

Для предотвращения возможности внедрения в ИСПДн вредоносного программного обеспечения в администрации должны применяться антивирусные средства:

Требования к настройке антивирусных средств защиты определены в проектной документации на СЗПДн, процедуры по управлению антивирусными средствами определены в эксплуатационной документации на СЗПДн.

- Порядок проведения мероприятий

Порядок использования антивирусных средств защиты определен в эксплуатационной документации на СЗПДн.

Специалист, назначенный правовым актом администрации Раздольненского сельского поселения, осуществляет:

– установку антивирусных средств защиты в соответствии с эксплуатационной и технической документацией к ним;

– настройку параметров антивирусных средств защиты согласно требованиям по обеспечению безопасности, определенным в проектной документации на СЗПДн;

– контроль эффективности работы антивирусных средств защиты.

Контроль соблюдения условий использования антивирусных средств защиты, предусмотренных эксплуатационной и технической документацией, возлагается на должностное лицо, ответственное за защиту ПДн.

6.5. Мероприятия по обеспечению криптографической защиты

В администрации должны применяться следующие типы средств криптографической защиты информации, сертифицированные ФСБ России:

– СКЗИ для обеспечения безопасности ПДн, передаваемых по каналам связи между администрацией и ИС сторонних организаций;

– средства электронной подписи, т.е. шифровальные (криптографические) средства, используемые для подписания передаваемых документов и проверки электронной подписи получаемых документов.

– СКЗИ, применяемые в администрации для защиты ПДн, должны иметь класс, определенный в Частной модели угроз безопасности ПДн при их обработке в ИСПДн администрации. Частная модель угроз безопасности ПДн составляется на каждую ИСПДн.

Правила использования СКЗИ при обмене информацией со сторонними организациями СКЗИ должны быть определены условиями заключаемых договоров между администрацией и данными организациями.

В администрации ведется учет всех применяемых СКЗИ, эксплуатационной и технической документации к ним, а также учет лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности ПДн.

- Порядок проведения мероприятий

Организация криптографической защиты в администрации осуществляется в соответствии с законодательством Российской Федерации.

На должностное лицо, ответственное за выполнение работ по защите ПДн в администрации, возлагается ответственность за обеспечение функционирования и безопасности СКЗИ согласно требованиям руководящих документов ФСБ России.

6.6. Мероприятия по обеспечению физической защиты

- Основные требования по обеспечению физической защиты

В целях предотвращения несанкционированного входа (вскрытия) в помещения, а также исключения возможности неконтролируемого проникновения в эти помещения посторонних лиц, в администрации организуется и обеспечивается физическая охрана и техническая защита помещений администрации, с использованием охранной сигнализации, обеспечивающие сохранность технических средств обработки персональных данных, носителей персональных данных и средств защиты информации.

Защите подлежат следующие типы помещений:

– помещения, в которых осуществляется непосредственно обработка ПДн пользователями ИСПДн администрации;

– серверные помещения, в которых установлено серверное, сетевое оборудование и технические средства защиты информации;

– архивные помещения, в которых организовано хранение бумажных документов, содержащих ПДн.

Перечень лиц, которые допускаются в указанные помещения, определяется правовым актом администрации.

В целях обеспечения физической защиты помещений применяются следующие средства защиты и контроля за несанкционированным вскрытием: система охранной сигнализации; двери помещений оборудуются замками для защиты от несанкционированного проникновения и местами для их опечатывания и сдачи под охрану; устанавливаются металлические двери для защиты от несанкционированного проникновения в серверные и архивные помещения.

В целях организации противопожарной безопасности в администрации устанавливается система пожарной сигнализации.

- Порядок проведения мероприятий по обеспечению физической защиты

Контроль обеспечения безопасности помещений, в которых расположены компоненты ИСПДн, возлагается на должностное лицо, ответственное за защиту ПДн.

Доступ в защищаемые помещения осуществляется согласно перечню, утвержденному правовым актом администрации.

Лица, не указанные в Перечне, при наличии необходимости могут посещать помещения администрации только в сопровождении допущенных лиц.

Одиночное, бесконтрольное пребывание лиц, не допущенных к работе по обработке ПДн, в служебных помещениях строго запрещено.

Пребывание посторонних лиц в серверных помещениях допускается в целях производственной необходимости, только в присутствии должностного лица, ответственного за защиту ПДн.

В случае утраты ключей (либо подозрении на утрату) к замкам в защищаемые помещения предпринимаются следующие меры:

– оповещаются должностные лица, ответственные за организацию работ по обработке ПДн, за защиту ПДн служебной запиской;

– производится немедленная замена запираемых замков;

– назначается административная проверка всех режимных помещений с составлением акта, виновные лица привлекаются к ответственности, установленном законом.

При возникновении форс-мажорных обстоятельств в защищаемых помещениях (возникновение пожара, затопление помещения, возгорание электропроводки и прочее) в отсутствии лиц, имеющих доступ в эти помещения, осуществляется вскрытие помещений с соблюдением следующих условий:

– оповещаются должностные лица, ответственные за организацию работ по обработке и защите ПДн;

– помещения вскрываются группой в составе не менее двух человек;

– при вскрытии помещения составляется акт о вскрытии, в котором указываются должности и фамилии лиц, вскрывших помещение, дата, время и причины вскрытия.

7. Обязанности, права и ответственность должностных лиц при обеспечении безопасности ПДн

Обязанности, права и ответственность должностных лиц, участвующих в обеспечении безопасности ПДн в администрации определены в соответствующих инструкциях.

8. Планирование работ по защите ПДн

Планирование работ по защите информации, требования к содержанию плана, порядок разработки, согласования, утверждения и оформления плана, порядок отчетности и контроля над его выполнением определяются действующими нормативными документами РФ.

План определяет перечень основных проводимых организационно-технических мероприятий по защите информации (в том числе ПДн) в администрации с указанием сроков выполнения мероприятий и ответственных за выполнение соответствующих пунктов Плана работников.

В План включаются мероприятия по контролю состояния защищенности ПДн.

План на очередной календарный год разрабатывается должностным лицом, ответственным за защиту информации в ИС ПДн, который осуществляет общий контроль над выполнением работ по защите информации.

Утвержденный план хранится у должностного лица, ответственного за организацию работ по обработке ПДн.

Отчет о результатах выполнения запланированных мероприятий по обеспечению безопасности ПДн за текущий год формируется должностным лицом, ответственным за защиту ПДн, в рамках общего отчета работы за текущей год.

9. Контроль состояния защищенности ПДн

Контроль состояния защищенности ПДн в администрации осуществляется с целью своевременного выявления и предотвращения утечки конфиденциальной

информации, отнесенной к категории ПДн, вследствие НСД к ней, преднамеренных программно-технических воздействий на персональные данные и оценки защищенности ПДн (далее по тексту - Контроль).

Контроль заключается в проверке выполнения требований действующих нормативных документов в области обработки и обеспечения безопасности ПДн, в оценке обоснованности и эффективности принятых мер по защите ПДн.

Контроль эффективности внедренных мер и СЗИ, входящих в состав СЗПДн, должен проводиться в соответствии с требованиями эксплуатационной документации на СЗПДн в целом на конкретные СЗИ, а также требованиями других нормативных документов не реже одного раза в год.

Обязательным является контроль СЗИ, входящих в состав СЗПДн, при вводе их в эксплуатацию после проведения ремонта таких средств, а также при изменении условий и расположения их эксплуатации.

Контроль обеспечения безопасности ПДн в администрации организовывается должностным лицом, ответственным за проведение работ по защите ПДн в Администрации.

Контроль состояния и эффективности СЗПДн может осуществляться в соответствии с планом основных мероприятий по защите информации на текущий год или носить внеплановый характер.

Результаты периодического контроля оформляются отдельными протоколами или актами.

По всем выявленным нарушениям требований по защите ПДн должностное лицо, ответственное за обеспечение безопасности ПДн в Администрации, в пределах предоставленных ему прав и своих функциональных обязанностей обязано добиваться их немедленного устранения.

Должностное лицо, ответственное за организацию работ по обработке ПДн в администрации, обязано принять все необходимые меры по немедленному устранению выявленных нарушений. При невозможности их немедленного устранения должна быть прекращена обработка ПДн и организованы работы по устранению выявленных нарушений.

Работники администрации, осуществляющие обработку ПДн в ИСПДн, обязаны выполнять требования должностного лица ответственного за обеспечение безопасности ПДн, по устранению допущенных ими нарушений норм и требований по обработке и/или обеспечении безопасности ПДн.

Работники несут персональную ответственность за соблюдение требований по обеспечению безопасности ПДн в ходе проведения работ.

Учет, хранение и выдача работникам паролей и ключей для системы защиты ПДн от НСД, оперативный контроль действий работников, осуществляющих обработку ПДн, осуществляет должностное лицо, ответственное за обеспечение безопасности ПДн.

10. Управление инцидентами информационной безопасности

В администрации в целях своевременного устранения выявленных нарушений безопасности определен и задокументирован порядок действий при возникновении инцидентов информационной безопасности, связанных с нарушением требований по обработке и обеспечению безопасности ПДн.

10.1. Требования к мероприятиям

К инцидентам информационной безопасности, связанным с нарушением требований по обработке и обеспечению безопасности ПДн, относятся любые нарушения, приводящие к снижению уровня защищенности ИСПДн, в том числе несоблюдение условий хранения носителей ПДн и использования средств защиты информации, которые могут привести к нарушению конфиденциальности, целостности или доступности ПДн.

В администрации в случаях возникновения подобных инцидентов информационной безопасности проводятся разбирательства, составляются заключения по фактам возникновения инцидентов, разрабатываются и принимаются меры по предотвращению возможных последствий инцидентов.

10.2. Порядок проведения мероприятий

Организация и контроль процесса реагирования на инциденты информационной безопасности, связанные с обработкой и обеспечением безопасности ПДн, в администрации возлагается на должностное лицо, ответственное за обеспечение безопасности ПДн.

Процедура управления инцидентами информационной безопасности, связанными с нарушением требований по обработке и обеспечению безопасности ПДн, регламентирована в документе «Порядок реагирования на инциденты информационной безопасности в администрации Раздольненского сельского поселения».

Дополнительно порядок действий работников Администрации в случаях возникновения инцидентов информационной безопасности определен в документе «Инструкция пользователю информационной системы ПДн в администрации Раздольненского сельского поселения».

11. Модернизация системы защиты ПДн

Для определения необходимости модернизации СЗПДн не реже одного раза в год должностным лицом, ответственным за обеспечение безопасности ПДн, проводится проверка состава и структуры СЗПДн, состава угроз и уровня защищенности ПДн, обработка которых осуществляется в ИСПДн Администрации.

Модернизация СЗПДн в обязательном порядке проводится в случаях, если: изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав обрабатываемых ПДн, состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн и пр.); изменился состав угроз безопасности ПДн в ИСПДн; изменился уровень защищенности ПДн.

Выбор мер и СЗИ, входящих в состав СЗПДн, проводится на основании проведенного анализа угроз и проведенной классификации ИСПДн (определения уровня защищенности ПДн).

Должностное лицо, ответственное за обеспечение безопасности ПДн, ежегодно разрабатывает план работ по обеспечению безопасности ПДн в администрации, в котором определяется перечень необходимых мероприятий по обеспечению безопасности ПДн с учетом выполненных мероприятий.

В план работ по обеспечению безопасности ПДн включаются организационные и технические мероприятия, направленные на выполнение требований нормативно-правовых документов в области безопасности ПДн и на

совершенствование СЗПДн, а также контрольные мероприятия и мероприятия по проведению обучения работников администрации.

В плане указываются дата, сроки проведения мероприятий, их периодичность (разовые или регулярные) и назначаются ответственные за их организацию и выполнение лица.

Работники, участвующие в обеспечении безопасности ПДн в администрации, вправе формировать предложения по совершенствованию СЗПДн и направлять их на рассмотрение должностному лицу, ответственному за защиту ПДн, которое, в свою очередь, формирует сводный перечень предложений по совершенствованию СЗПДн.

Ежегодно должностное лицо, ответственное за защиту ПДн, формирует отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности ПДн, обрабатываемых в администрации, и предоставляет его Главе администрации совместно со сводным перечнем предложений по совершенствованию СЗПДн.

Ежегодный отчет по выполнению плана работ включает в себя:

– результаты проведенной проверки состава и структуры, состава угроз и уровня защищенности ПДн;

– результаты проведенных контрольных мероприятий по защите ПДн;

– результаты проверок регулирующими органами;

– результаты анализа инцидентов информационной безопасности;

– результаты плановых мероприятий по обеспечению безопасности ПДн;

– предложения по совершенствованию СЗПДн на основе полученных результатов.

На основании решения, принятого Главой администрации, по результатам рассмотрения ежегодного отчета и предложений по совершенствованию СЗПДн должностное лицо, ответственное за защиту ПДн, составляет план работ по обеспечению безопасности ПДн, обрабатываемых в администрации, на следующий год.

12. Привлечение сторонних организаций для проведения мероприятий по обеспечению безопасности ПДн

В администрации могут привлекаться сторонние организации для проведения следующих мероприятий по обеспечению безопасности ПДн:

– разработка нормативно-методических материалов по вопросам обеспечения безопасности ПДн;

– поставка СЗИ и СКЗИ;

– выполнение организационных и технических мероприятий в области защиты ПДн, на проведение которых у администрации отсутствует соответствующее разрешение либо отсутствуют технические средства и подготовленные работники (специалисты);

– выполнение организационных и технических мероприятий в области защиты ПДн, выполнение которых силами администрации экономически нецелесообразно;

– подтверждение соответствия мер по защите ИСПДн требованиям нормативно-правовой базы РФ в области безопасности ПДн, путем проведения

аттестационных испытаний ИСПДн Администрации по требованиям безопасности информации;

– контроль и аудит эффективности проводимых мероприятий по защите ПДн.

Привлекаемые для оказания услуг в области защиты ПДн сторонние организации должны иметь лицензии на соответствующие виды деятельности.

Перечень совместно выполняемых организационных и технических мероприятий в области защиты ПДн определяется с учетом планируемых работ по созданию (реконструкции) ИСПДн и включается в План основных мероприятий по защите ПДн.

В данном разделе определен порядок взаимодействия с вышеперечисленными сторонними организациями.

12.1. Привлечение сторонних организаций для проведения мероприятий по созданию и модернизации СЗПДн и/или проведению контрольных мероприятий

Привлекаемая сторонняя организация должна обладать соответствующими, проводимым работам, лицензиями и сертификатами.

Должностное лицо, ответственное за обеспечение безопасности ПДн, является ответственным за выбор организации, привлекаемой для проведения мероприятий по созданию или модернизации СЗПДн и проведению контрольных мероприятий.

Должностное лицо, ответственное за защиту ПДн, осуществляет подбор подходящих организаций и формирует предложения для согласования с главой администрации.

Существенным условием договора является обязательство привлекаемой организации обеспечить конфиденциальность получаемой информации, ставшей известной в ходе выполнения работ по обеспечению безопасности ПДн в администрации.

В случае привлечения сторонней организации для проведения мероприятий по созданию или модернизации СЗПДн в договоре прописываются обязательства привлекаемой организации по проведению необходимых организационно-технических мероприятий, включающих в себя: организацию и проведение работ по созданию СЗПДн; реализацию требований нормативно-правовых документов РФ в области обработки и защиты ПДн; своевременное совершенствование СЗПДн; поддержание работоспособности и сопровождение СЗПДн.

В случае привлечения сторонней организации для проведения контрольных мероприятий (аудит обеспечения безопасности ПДн) в договоре прописываются обязанности привлекаемой организации по выполнению необходимых работ, включающих в себя: проверку выполнения требований нормативно-правовых документов РФ в области обработки и защиты ПДн; оценку обоснованности и эффективности принятых в администрации мер по обеспечению безопасности ПДн.

Должностное лицо, ответственное за обеспечение безопасности ПДн, осуществляет контроль над выполнением привлекаемой организацией взятых на себя обязательств.

12.2. Привлечение сторонних организаций для проведения обучения работников

К организациям, привлекаемым для проведения обучения работников администрации по направлению обеспечения безопасности ПДн, предъявляются следующие требования:

– организация должна иметь лицензию на осуществление образовательной деятельности, выданную Министерством образования РФ, государственными органами управления образованием субъектов РФ или органами местного самоуправления, наделенными соответствующими полномочиями;

– предлагаемые организацией программы и курсы обучения должны быть согласованы с регулирующими и надзорными органами;

– по результатам проведенного обучения организация должна проводить итоговую аттестацию работников.

12.3. Привлечение сторонних организаций (подрядчиков) для ремонтно-восстановительных работ

Организацией обслуживания, настройки и ремонта средств обработки и СЗИ, входящих в состав СЗПДн, в администрации занимается специалист, назначенный правовым актом администрации.

В случае необходимости, ремонт технических средств может быть произведен с привлечением специалистов сторонних организаций на договорной основе с составлением актов выполненных работ.

Сопровождение и контроль сторонних организаций (подрядчиков) обеспечивается должностным лицом, ответственным за обеспечение безопасности ПДн.

Обязательным условием при передаче технических средств обработки ПДн и машинных носителей ПДн для осуществления ремонтных работ сторонней организацией является удаление ПДн с носителей, установленных на передаваемых устройствах, либо извлечение носителей ПДн. Контроль исполнения данного требования возлагается на должностное лицо, ответственное за защиту ПДн.

В случае, когда выполнить данное требование не представляется возможным, должностным лицом, ответственным за защиту ПДн, составляется двусторонний протокол, в котором указано, что сторонняя организация осведомлена о том, какие именно персональные данные содержатся на носителе и обязана принять все необходимые меры по обеспечению их безопасности.

После проведения ремонта средств защиты или средств обработки ПДн, при изменении условий их расположения или эксплуатации обязательно осуществляется проверка готовности этих средств к использованию с составлением заключений о возможности их эксплуатации.

Приложение № 3
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Правила работы
с обезличенными персональными данными в администрации Раздольненского сельского поселения

Статья 1. Условия обезличивания

Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса используемых информационных систем персональных данных и по достижению сроков обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законодательством Российской Федерации.

Статья 2. Способы обезличивания

1. К способам обезличивания персональных данных при условии дальнейшей обработки персональных данных относятся:

1) замена части сведений идентификаторами;

2) обобщение (понижение) точности некоторых сведений;

3) деление сведений на части и обработка их в разных информационных системах;

4) другие способы.

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

Статья 3. Правила работы с обезличенными данными

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

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

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

1) использование средств защиты информации;

2) использование антивирусных программ;

3) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных.

4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

1) хранения бумажных носителей в условиях, исключающих доступ к ним посторонних лиц;

2) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных.

Приложение № 4
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

**Перечни персональных данных,
обрабатываемых в администрации Раздольненского сельского поселения в связи с реализацией трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением муниципальных функций**

Перечень персональных данных, обрабатываемых в администрации Раздольненского сельского поселения в связи с реализацией трудовых отношений:

- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Адрес регистрации;
- Адрес проживания (реальный);
- Телефонный номер (домашний, рабочий, мобильный);
- Адрес электронной почты;
- Паспортные данные (серия, номер, кем и когда выдан);
- Семейное положение и состав семьи (муж/жена, дети);
- Места рождения, работы, домашние адреса близких родственников;
- Оклад и другие доходы;
- Индивидуальный номер налогоплательщика;
- Номер пенсионного страхования;
- Данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- Информация о трудовой деятельности до приема на работу;
- Информация о знании иностранных языков;
- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- Данные о медицинской страховке;
- Данные об аттестации работников;
- Данные о повышении квалификации;
- Данные о наградах, медалях, поощрениях, почетных званиях;
- Информация о состоянии здоровья;
- Информация о негосударственном пенсионном обеспечении;
- Данные об имущественном и социальном положении;

- Сведения о доходах, имуществе и обязательствах имущественного характера, а также о доходах, об имуществе и обязательствах имущественного характера членов семьи;
- Сведения о социальных льготах и социальном статусе;
- Сведения о наличии (отсутствии) судимости;
- Номера расчетных счетов, банковских карт;
- Сведения о допуске к государственной тайне;
- Сведения о пребывание за границей.

Перечень персональных данных, обрабатываемых в администрации Раздольненского сельского поселения в связи с оказанием муниципальных услуг и осуществлением муниципальных функций:

- Фамилия, Имя, Отчество;
- Дата рождения;
- Адрес регистрации (адрес проживания);
- Паспортные данные (серия, номер, кем и когда выдан);
- Семейное положение и состав семьи (муж/жена, дети);
- Оклад и другие доходы;
- Номера контактных телефонов;
- Адрес электронной почты;
- Индивидуальный номер налогоплательщика;
- Номер пенсионного страхования;
- Имущественное положение;
- Социальное положение;
- Образование;
- Место работы;
- Причина и место смерти (серия, номер, кем выдано свидетельство о смерти, сведения об актовой записи).

Обезличенные и (или) общедоступные персональные данные:

-сведения о трудовой деятельности (общие данные о трудовой занятости на текущее время, общий и непрерывный стаж работы);

-сведения об образовании, квалификации, о наличии специальных знаний или специальной подготовки (дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками);

-сведения о повышении квалификации и переподготовке (дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения);

-сведения о заработной плате (в том числе данные по окладу, надбавкам, налогам);

-сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (военно-учетная специальность, воинское звание, данные о принятии/снятии с учета);

-сведения о семейном положении (состоянии в браке, наличие детей и их возраст);

-наличие (отсутствие) судимости.

Приложение № 5
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Перечень должностей
в администрации Раздольненского сельского поселения, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных

- Заместитель Главы администрации
- Советник администрации

Приложение № 6
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Перечень должностей
в администрации Раздольненского сельского поселения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

- Глава администрации;
- заместитель главы администрации;
- главный бухгалтер;
- советник;
- консультант;
- главный специалист-эксперт;
- ведущий специалист бухгалтерии;
- инспектор-делопроизводитель;
- специалист ВУС;
- паспортист.

Приложение № 7
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Форма обязательства
о неразглашении информации, содержащей персональные данные

Я, _____

(фамилия, имя, отчество лица, допущенного к обработке персональных данных)

_____,

исполняющий(ая) должностные обязанности _____

_____

_____,

предупрежден(а) о том, что на период исполнения должностных обязанностей мне будет предоставлен допуск к информации, содержащей персональные данные.

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.
3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.
4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.
5. В случае расторжения договора (контракта) и (или) прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден(а) о том, что нарушение данного обязательства является основанием привлечения к дисциплинарной и(или) иной ответственности в соответствии с законодательством Российской Федерации.

«____» _____ 20 г _____/_____

(подпись) (расшифровка подписи)

Приложение № 8
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Согласие на обработку персональных данных

_____
(наименование (Ф.И.О.) оператора, получающего согласие субъекта персональных данных)

_____
(адрес оператора)

_____
(Ф.И.О. субъекта персональных данных)

_____
(адрес, где зарегистрирован субъект персональных данных)

_____
(номер основного документа, удостоверяющего его личность, сведения о дате выдачи документа и выдавшем его органе)

Даю своё согласие на обработку следующих персональных данных:

_____
(перечень персональных данных)

с целью:_____
(указывается цель обработки персональных данных)

Даю своё согласие на совершение следующих действий с моими персональными данными (**ненужное зачеркнуть**):
сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Даю своё согласие на использование следующих способов обработки моих персональных данных (**ненужное зачеркнуть**):

с использованием средств автоматизации (автоматизированная обработка);

без использования средств автоматизации (неавтоматизированная обработка);

смешанная обработка.

Срок, в течение которого действует согласие_____
(указывается срок действия согласия)

В случае неправомерных действий или бездействия оператора настоящее согласие может быть отозвано мной заявлением в письменном виде.

«____» _____ 20 г _____ _____
(подпись) (инициалы, фамилия)

Приложение № 9
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

**Порядок доступа в помещения,
в которых ведётся обработка персональных данных, в администрации
Раздольненского сельского поселения**

1. Общие положения

Порядок доступа в помещения, в которых ведётся обработка персональных данных, в администрации Раздольненского сельского поселения разработан в целях обеспечения безопасности персональных данных, средств вычислительной техники информационных систем персональных данных, материальных носителей персональных данных, а также обеспечения внутри объектового режима.

Объектами охраны являются:

- помещения, в которых происходит обработка персональных данных, как с использованием средств автоматизации, так и без таковых;
- помещения, в которых установлены компьютеры, сервера и коммутационное оборудование, участвующее в обработке персональных данных;
- помещения, в которых хранятся материальные носители персональных данных;
- помещения, в которых хранятся резервные копии персональных данных.

Бесконтрольный доступ посторонних лиц в указанные помещения должен быть исключен.

Ответственность за соблюдение положений настоящего порядка несут руководители и сотрудники структурных подразделений администрации Раздольненского сельского поселения, обрабатывающих персональные данные.

Контроль за соблюдением требований настоящего порядка обеспечивает ответственный за организацию обработки персональных данных.

Некоторые положения данного порядка могут не применяться в зависимости от специфики обработки персональных данных структурными подразделениями по согласованию с ответственным за организацию обработки персональных данных.

2. Допуск в помещения, в которых ведется обработка персональных данных

Доступ посторонних лиц в помещения, в которых ведется обработка персональных данных, должен осуществляется только ввиду служебной необходимости.

При этом на момент присутствия посторонних лиц в помещении должны быть приняты меры по недопущению ознакомления посторонних лиц с персональными данными.

Пример: мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

Допуск сотрудников в помещения, в которых ведется обработка персональных данных, оформляется после подписания сотрудником обязательства о неразглашении при трудоустройстве в администрацию Раздольненского сельского поселения.

В нерабочее время в помещениях, в которых ведется обработка персональных данных, все окна и двери в смежные помещения должны быть надежно закрыты, материальные носители персональных данных должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в специальные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спец помещения.

Охрана и организация пропускного режима должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц.

В служебных помещениях применяются технические и организационные меры, направленные для защиты персональных данных от нецелевого использования, несанкционированного доступа, раскрытия, потери, изменения и уничтожения обрабатываемых персональных данных.

Приложение № 10
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации Раздольненского сельского поселения

Статья 1. Право субъектов персональных данных на получение сведений

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

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

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

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

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

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

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

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных

данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

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

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

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

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

Статья 2. Порядок предоставления оператором сведений по запросу субъекта персональных данных

1. При обращении либо при получении запроса субъекта персональных данных или его представителя сведения должны быть предоставлены в доступной форме. Запрос регистрируется в день поступления в установленном порядке.

2. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.

3. Оператор при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных, обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными в течении 30 (тридцати) дней с даты получения запроса.

В случае отказа в предоставлении информации о наличии персональных данных оператор обязан дать в письменной форме мотивированный ответ с ссылкой на действующее законодательство, являющегося основанием для такого отказа. Отказ в предоставлении информации направляется в срок, не превышающий 30 (тридцати) дней со дня получения запроса субъекта персональных данных.

4. В случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор в срок, не превышающий 7 (семь) рабочих дней, вносит в них необходимые изменения. О внесённых изменениях уведомляется субъект персональных данных или его представитель.

5. В случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные в срок, не превышающий 7 (семь) рабочих дней. Об уничтоженных персональных данных уведомляется субъект персональных данных или его представитель.

6. При получении запроса из уполномоченного органа по защите прав субъектов персональных данных оператор обязан сообщить необходимую информацию в течении 30 (тридцати) дней с даты получения такого запроса.

7. Возможность ознакомления с персональными данными предоставляется на безвозмездной основе лицом ответственным за обработку персональных данных.

Приложение № 11
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Правила осуществления
внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Статья 1. Цель внутреннего контроля

1. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных осуществляется с целью проверки соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами администрации Раздольненского сельского поселения.

Статья 2. Виды и периодичность внутреннего контроля

1. Внутренний контроль соответствия обработки персональных данных делится на текущий и периодический.
2. Текущий внутренний контроль осуществляется на постоянной основе ответственным за обеспечение безопасности персональных данных.
3. Периодический внутренний контроль осуществляется комиссией в соответствии с поручением Главы администрации Раздольненского сельского поселения.

Периодичность проверки – не реже одного раза в шесть месяцев.

Статья 3. Порядок создания комиссии для осуществления внутреннего контроля

1. Проверки осуществляются комиссией, созданной распоряжением администрации Раздольненского сельского поселения, из числа сотрудников администрации, допущенных к обработке персональных данных, так же возможно привлечение в качестве членов комиссий экспертов.

В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.

2. Проверки осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

Статья 4. Порядок проведения внутренней проверки

1. При проведении внутренней проверки комиссией должны быть полностью, объективно и всесторонне установлены:

– порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

– порядок и условия применения средств защиты информации;

– эффективность принимаемых мер по обеспечению безопасности персональных данных;

– состояние учёта бумажных и машинных носителей персональных данных;

– соблюдение правил доступа к персональным данным;

– наличие (отсутствие) фактов несанкционированного доступа к персональным данным;

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

– осуществление мероприятий по обеспечению целостности персональных данных.

2. Осуществление мероприятий внутреннего контроля проводится комиссией периодически в соответствии с Перечнем мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных. Перечень мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных приведен в Приложении 1 к настоящим Правилам.

Для каждой проверки составляется протокол проведения внутренней проверки. Форма протокола приведена в Приложении 2 к настоящим Правилам.

3. При выявлении в ходе проверки нарушений в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

4. Протоколы хранятся у председателя комиссии в течение текущего года. Уничтожение протоколов проводится комиссией самостоятельно по истечении срока хранения.

5. О результатах проверки и мерах, необходимых для устранения нарушений председатель комиссии докладывает Главе администрации Раздольненского сельского поселения.

6. Срок проведения проверки не может составлять более 30 (тридцати) дней со дня принятия решения о её проведении.

Приложение 1

Перечень
мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных

№ п/п	Краткое описание мероприятий
1	Контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны
2	Проверка выполнения требований по условиям размещения автоматизированных рабочих мест (далее - АРМ) в помещениях, в которых размещены средства информационных систем персональных данных (далее - ИСПДн)
3	Проверка соответствия состава и структуры программно-технических средств ИСПДн документированному составу и структуре средств, разрешенных для обработки персональных данных
4	Проверка режима допуска в помещения, где размещены средства ИСПДн и осуществляется обработка персональных данных
5	Проверка соответствия реального уровня полномочий по доступу к персональным данным различных пользователей, установленному в списке лиц, допущенных к обработке персональных данных, уровню полномочий
6	Проверка наличия и соответствия средств защиты информации в соответствии с указанными в техническом паспорте на ИСПДн
7	Проверка правильности применения средств защиты информации
8	Проверка неизменности настроенных параметров антивирусной защиты на рабочих станциях пользователей
9	Контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн
10	Проверка соблюдения правил парольной защиты
11	Проверка работоспособности системы резервного копирования
12	Проведение мероприятий по проверке организации учета и условий хранения съемных носителей персональных данных
13	Проверка соблюдения требований по обеспечению безопасности при использовании ресурсов сети "Интернет"
14	Проверка знаний работниками руководящих документов, технологических инструкций, предписаний, актов, заключений и уровня овладения работниками технологией безопасной обработки информации, изложенных в инструкциях
15	Проверка знаний инструкций по обеспечению безопасности информации пользователями ИСПДн
16	Проверка наличия документов, подтверждающих возможность применения технических и программных средств вычислительной техники для обработки персональных данных и применения средств защиты (сертификатов соответствия и других документов)

Приложение 2

Протокол
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Настоящий Протокол составлен в том, что __.__.202_ комиссией по внутреннему контролю проведена проверка _____
_____.

(место проверки)

Проверка осуществлялась в соответствии с требованиями
_____
_____

В ходе проверки проверено:

_____

_____

_____

_____
_____

Выявленные нарушения:

_____
_____

_____

_____

_____

Меры по устранению нарушений:

_____

_____

_____

_____
_____

Срок устранения нарушений: _____.

Председатель комиссии _____ И.О. Фамилия

Члены комиссии:

Должность _____ И.О. Фамилия

Должность _____ И.О. Фамилия

Должность руководителя

проверяемого подразделения _____ И.О. Фамилия

Приложение № 12
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Инструкция
по организации антивирусной защиты в информационных системах персональных данных администрации Раздольненского сельского поселения

1. Общие положения

Инструкция определяет правила и основные требования по обеспечению антивирусной защиты в информационных системах персональных данных (далее –ИСПДн) и устанавливает ответственность за их выполнение.

2. Основные определения

Вредоносное программное обеспечение (далее ПО) - специально разработанное программное обеспечение, программный модуль, блок, группа команд, имеющая способность к самораспространению, которая может попадать в общее и специальное программное обеспечение ИСПДн и приводить к:

– дезорганизации вычислительного процесса (нарушению или существенному замедлению обработки информации);

– модификации или уничтожению программ, или данных;

– приведению в негодность носителей информации и других технических средств;

– нарушению функционирования средств защиты информации.

3. Инструкция по применению средств антивирусной защиты

Защита ПО ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

К использованию допускаются только лицензионные антивирусные средства, обладающие необходимой сертификацией в регулирующих органах РФ.

Решение задач по установке и сопровождению средств антивирусной защиты возлагается на специалиста, назначенного распоряжением Администрации.

Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.

Всё впервые вводимое в эксплуатацию ПО должно проходить обязательный антивирусный контроль.

Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места специалиста, назначенного распоряжением Администрации.

Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ИСПДн.

Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов ИСПДн.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.

Контроль входящей информации необходимо проводить непосредственно после ее приема.

Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

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, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции либо обратиться к специалисту, назначенному распоряжением Администрации.

При получении информации о возникновении вирусной эпидемии вне ИС должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.

В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения вируса специалиста, назначенного распоряжением Администрации;

– провести лечение зараженных файлов;

– в случае невозможности лечения обратиться к администратору безопасности ИСПДн.

По факту обнаружения зараженных вирусом файлов специалист, назначенный распоряжением Администрации, должен составить служебную записку, в которой должен указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.

Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

Ответственный за организацию обработки ПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению, проводить периодическое тестирование функций средств антивирусной защиты, проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).

С данной инструкцией пользователи должны быть ознакомлены под роспись.

Приложение № 13
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Границы контролируемой зоны
информационных систем персональных данных администрации
Раздольненского сельского поселения

В целях исключения неконтролируемого пребывания посторонних лиц при обработке персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ « О персональных данных», приказом ФСТЭК России от 18.02.2013 № 1 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» определить границы контролируемой зоны по периметру здания, расположенного по адресу: 684020, Камчатский край, Елизовский р-н, п. Раздольный, ул. Советская, 2а, в пределах которого исключено присутствие посторонних лиц без допуска.

Контролируемая зона включает пространство здания, в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска к объектам информационной системы персональных данных, а также технических и иных материальных средств.

Приложение № 14
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Порядок реагирования
на инциденты информационной безопасности в администрации
Раздольненского сельского поселения

1. Термины и определения

В настоящем Порядке используются основные понятия в соответствии со статьей 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Используемые сокращения

В настоящем Порядке использованы следующие сокращения:

ИБ	Информационная безопасность
ИСПДн	Информационная система ПДн
НСД	Несанкционированный доступ
ПДн	Персональные данные

3. Область применения

Настоящий Порядок реагирования на инциденты информационной безопасности (далее - Порядок) предназначен для определения единого порядка реагирования на возникшие инциденты информационной безопасности, проведения служебных расследований, а также проведения мероприятий, нацеленных на предотвращение наступления повторных инцидентов в администрации Раздольненского сельского поселения (далее по тексту - администрация).

Требования настоящего Порядка распространяются на должностных лиц администрации, отвечающих за обеспечение безопасности ПДн.

4. Общие положения

Настоящий Порядок разработан в соответствии Федеральным законом от 27.07. 2006 № 152-ФЗ «О персональных данных».

В соответствии с настоящим Порядком к инцидентам ИБ в администрации относятся:

1) нарушение конфиденциальности, целостности или доступности ПДн;

2) отказ оборудования, сервисов, средств обработки и (или), входящих в состав ИСПДн;

3) несоблюдение требований внутренних организационно-распорядительных документов и действующих нормативных документов РФ в области обработки и защиты ПДн (нарушение правил обработки ПДн);

4) заражение программных компонентов ИСПДн вредоносным программным обеспечением.

К инцидентам ИБ в ИСПДн также относятся попытки и факты получения НСД к ИСПДн:

1) сеансы работы в ИСПДн незарегистрированных пользователей;

2) сеансы работы Пользователей ИСПДн, срок действия полномочий, которых истек, либо в состав полномочий, которых не входят выявленные действия с ПДн;

3) действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой выгоды, методом подбора пароля или иными методами (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

4) совершение попыток несанкционированного доступа к рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);

5) несанкционированное внесение изменений в параметры конфигурации программных или аппаратных средств обработки, или защиты, входящих в состав ИСПДн.

Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для возникновения описанных выше инцидентов.

5. Оповещение об инциденте информационной безопасности

В случае выявления инцидента ИБ устанавливается следующая последовательность действий сотрудников администрации:

– прекратить работу с ресурсом, в котором выявлен инцидент ИБ;

– оповестить своего непосредственного руководителя о факте выявления инцидента ИБ;

– руководитель должен оповестить должностное лицо, ответственное за защиту информации и обеспечение безопасности ПДн;

– после извещения указанных должностных лиц по их требованию предоставить всю необходимую информацию.

Должностное лицо, ответственное за защиту информации и обеспечение безопасности ПДн, проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его возникновению, и составляет краткую справку, в которой описывается произошедший инцидент ИБ, его последствия и оценка необходимости проведения расследования инцидента ИБ. Справка направляется главе администрации для принятия решения о проведении расследования инцидента ИБ.

Порядок проведения расследования инцидента ИБ описан в разделе 7 настоящего Порядка.

Мероприятия по устранению причин и недопущению повторного возникновения инцидента ИБ описаны в разделе 8 настоящего Порядка.

6. Мероприятия при возникновении инцидента информационной безопасности, ставшего причиной возникновения негативных последствий для субъекта ПДн

В случае если инцидент ИБ может стать или уже стал причиной возникновения негативных последствий для субъектов ПДн, необходимо немедленно блокировать ПДн этих субъектов до устранения причин, повлекших

за собой возникновение инцидента ИБ. Решение о блокировании ПДн принимает должностное лицо, ответственное за защиту информации и обеспечение безопасности ПДн.

ПДн остаются заблокированными до устранения причин, повлекших за собой возникновение инцидента ИБ.

7. Проведение расследования инцидента информационной безопасности

Внутреннее расследование и составление заключений должно в обязательном порядке проводиться в случае выявления:

– нарушения конфиденциальности, целостности или доступности ПДн;

– халатности и несоблюдения требований по обеспечению безопасности ПДн;

– несоблюдения условий хранения носителей ПДн;

– использования СЗИ, которые могут привести к нарушению заданных характеристик безопасности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

Задачами внутреннего расследования являются:

– установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

– установление лиц, непосредственно виновных в данном нарушении;

– выявление причин и условий, способствовавших нарушению.

Проведение внутреннего расследования проводится по решению Главы администрации. С целью проведения расследования в обязательном порядке формируется комиссия, в состав которой входят должностное лицо, ответственное за защиту информации и обеспечение безопасности ПДн, и иные должностные лица администрации, участие которых может потребоваться.

Комиссия должна приступить к работе по расследованию не позднее следующего рабочего дня после даты выявления инцидента ИБ.

Общая продолжительность внутреннего расследования не должна превышать одного месяца.

В рамках проведения расследования инцидента ИБ комиссия уполномочена:

– проводить опрос сотрудников администрации, по вине которых предположительно произошел инцидент ИБ, а также должностных лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента ИБ;

– проводить осмотр объектов и предметов, которые могут иметь отношение к инциденту ИБ.

По решению Главы администрации на комиссию могут быть возложены дополнительные обязанности и права.

Работник, в отношении которого проводится расследование, должен быть ознакомлен с распоряжением о проведении расследования.

Все действия членов комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (акты, протоколы, справки и т.п.).

Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник

отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами комиссии в виде протокола.

В целях исключения возможности какого-либо воздействия на процесс расследования члены комиссии обязаны соблюдать конфиденциальность расследования до принятия по нему решения Главой администрации.

Для оперативного проведения внутреннего расследования должностное лицо, ответственное за защиту ПДн, составляет план проведения расследования.

Одновременно с проведением внутреннего расследования, Глава администрации может поручить комиссии определить ущерб для администрации и (или) для субъекта ПДн от произошедшего инцидента ИБ. В отдельных случаях такая оценка может быть осуществлена с привлечением специализированной организации.

По окончании внутреннего расследования комиссия представляет Главе администрации отчет по результатам расследования, в котором излагаются:

- основания и время проведения расследования;
- проделанная работа (кратко);
- время, место и обстоятельства факта нарушения;
- причины и условия совершения нарушения;
- виновные лица и степень их вины;
- наличие умысла в действиях виновных лиц;
- предложения по возмещению ущерба;
- предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;
- рекомендации по исключению подобных нарушений;
- другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т. д.).

К отчету прилагаются:

- письменные объяснения лиц, которых опрашивали члены Комиссии;
- акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т. д.;
- другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба.

Отчет должен быть подписан всеми членами комиссии. При несогласии с выводами или содержанием отдельных положений член комиссии, подписывая заключение, приобщает к нему свое особое мнение (в письменном виде).

Отчет подлежит утверждению Главой администрации.

Работник, в отношении которого проводится расследование, или его уполномоченный представитель имеют право ознакомления с материалами расследования и требовать приобщения к материалам расследования представляемых ими документов и материалов.

Работник, в отношении которого проведено расследование, должен быть ознакомлен под роспись с отчетом по результатам расследования.

Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется правовым актом администрации.

При наличии в действиях работника признаков административного правонарушения или преступления Глава администрации обязан обратиться в

правоохранительные органы для привлечения виновного к ответственности, в соответствии с законодательством РФ.

В соответствии с Трудовым кодексом РФ, возмещение ущерба производится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нанесение ущерба.

Первый экземпляр отчета с резолюцией Главы администрации, копия правового акта по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле. Дела о внутренних расследованиях хранятся у Главы администрации.

8. Превентивные меры по недопущению повторного возникновения инцидентов информационной безопасности

Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение, в зависимости от произошедшего инцидента ИБ, включают в себя:

- мониторинг событий в информационной системе ПДн;
- своевременное удаление неиспользуемых учетных записей;
- контроль и мониторинг действий пользователей в информационной системе ПДн;
- проведение обучения (повторного обучения) пользователей правилам обработки и обеспечения безопасности ПДн;
- ознакомление пользователей с мерами ответственности, установленными нормативными документами РФ, за нарушение норм и правил обработки ПДн, а также за разглашение полученных данных.

Приложение № 15
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Инструкция
должностного лица, ответственного за организацию обработки персональных данных в информационных системах персональных данных

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность лица, ответственного за организацию обработки персональных данных в информационных системах персональных данных администрации Раздольненского сельского поселения (далее - ИСПДн).

1.2. Ответственный за организацию обработки персональных данных назначается из числа штатных пользователей ИСПДн на основании распоряжения администрации «О назначении ответственного за организацию обработки персональных данных в администрации Раздольненского сельского поселения».

1.3. Ответственный за организацию обработки персональных данных в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Правилами обработки персональных данных в администрации Раздольненского сельского поселения, Положением об обеспечении безопасности персональных данных в администрации Раздольненского сельского поселения, настоящей инструкцией, руководящими и нормативными документами ФСТЭК России, регламентирующими документами ИСПДн.

1.4. Ответственный за организацию обработки персональных данных является должностным лицом, уполномоченным на проведение работ по организации обработки персональных данных в ИСПДн.

2. Обязанности должностного лица, ответственного за организацию обработки персональных данных в ИСПДн

2.1. Должностное лицо ответственное за организацию работ по обработке персональных данных обязано:

– взаимодействовать с регулирующими органами по вопросам обработки и обеспечения безопасности персональных данных;

– передавать ответственному за защиту информации ИСПДн сведения по взаимодействию с регулирующими органами в рамках его компетенции;

– контролировать договоры с третьими лицами на предмет их соответствия требованиям организационно-распорядительных документов по обработке и обеспечению безопасности персональных данных;

– предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении контрольных мероприятий по обеспечению безопасности персональных данных;

– обеспечивать выполнение требований по обработке и обеспечению безопасности персональных данных в соответствии с Правилами обработки персональных данных в администрации Раздольненского сельского поселения, Положением об обеспечении безопасности персональных данных в администрации Раздольненского сельского поселения, Положением «Об организации работы с персональными данными работников Администрации Раздольненского сельского поселения и ведении личных дел», и иными нормативными документами в области обработки и защиты персональных данных;

– осуществлять непрерывный контроль действий, пользователей при обработке персональных данных, разъяснять и требовать от пользователей выполнения требований нормативных документов в области обработки и защиты персональных данных;

– участвовать в процессе разработки организационно-распорядительных документов, регламентирующих требования по обеспечению информационной безопасности персональных данных, обрабатываемых в ИСПДн;

– определять необходимость и направлять на обучение пользователей ИСПДн;

– предоставлять консультации пользователей ИСПДн по вопросам автоматизированной и неавтоматизированной обработки персональных данных в рамках своих компетенций;

– организовывать и контролировать своевременное предоставление пользователями ИСПДн доступа к персональным данным и средствам их обработки в объеме, необходимом для выполнения ими своих трудовых обязанностей;

– определять права доступа к персональным данным и автоматизированным средствам обработки персональных данных в рамках своих компетенций;

– сообщать о выявленных нарушениях требований по обработке персональных данных должностному лицу, ответственному за защиту информации;

– обеспечивать выполнение плана периодических проверок условий обработки персональных данных в пределах своих функциональных обязанностей;

– участвовать в разработке плана периодических проверок условий обработки персональных данных.

3. Права должностного лица, ответственного за организацию обработки персональных данных в ИСПДн

3.1. Должностное лицо, ответственное за организацию работ по обработке персональных данных, имеет право:

– формировать предложения по совершенствованию системы защиты информации для должностного лица, ответственного за защиту информации, обрабатываемой в ИСПДн;

– формировать предложения о необходимости проведения контрольных мероприятий по обеспечению безопасности персональных данных для должностного лица, ответственного за защиту информации;

– формировать предложения по внесению изменений в организационно-распорядительные документы, регламентирующие требования по обеспечению информационной безопасности персональных данных, обрабатываемых в ИСПДн;

– организовывать проведение периодических проверок условий обработки персональных данных;

– осуществлять ознакомление служащих, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, муниципальными актами по вопросам обработки персональных данных;

– в случаях, установленных нормативными правовыми актами Российской Федерации, в соответствии с требованиями и методами, установленными уполномоченным органом по защите прав субъектов персональных данных, осуществлять обезличивание персональных данных, обрабатываемых в ИСПДн.

4. Нештатные ситуации

4.1. В случае возникновения нештатных ситуаций ответственный за организацию обработки персональных данных обязан незамедлительно принять все необходимые меры по устранению причины возникновения нештатной ситуации для минимизации ее последствий.

4.2. В случае возникновения нештатных ситуаций ответственный за организацию обработки персональных данных обязан немедленно оповестить руководство о нештатной ситуации.

5. Ответственность

5.1. На лицо, ответственное за организацию обработки персональных данных, возлагается персональная ответственность за организацию обработки персональных данных в ИСПДн в соответствии с функциональными обязанностями.

5.2. Лицо, ответственное за организацию обработки персональных данных, несет ответственность по действующему законодательству за разглашение информации ограниченного доступа, ставшей известной ему по роду работы.

Приложение № 16
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Инструкция
пользователя информационной системы персональных данных в администрации Раздольненского сельского поселения

1. Общие положения

1.1. Пользователь информационной системы персональных данных (далее – ИСПДн) осуществляет обработку персональных данных (далее – ПДн) в ИСПДн, используемых в администрации Раздольненского сельского поселения (далее - администрация).

1.2. Пользователем ИСПДн (далее – пользователь) является каждый сотрудник администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность согласно действующему законодательству Российской Федерации за свои действия и за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

1.4. Пользователь в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Правилами обработки персональных данных в администрации Раздольненского сельского поселения, Положением об обеспечении безопасности персональных данных в администрации Раздольненского сельского поселения, настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами администрации.

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

2. Обязанности пользователя

2.1. 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.

2.2. Выполнять только те процедуры, которые определены для него правовыми актами администрации о системе допуска пользователей и обслуживающего персонала к информационным ресурсам и системе защиты персональных данных.

2.3. Знать и соблюдать установленные требования по режиму обработки ПДн, учету, хранению и пересылке носителей информации, защите ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 3).

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 4).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключить 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 также для получения консультаций по вопросам информационной безопасности, необходимо обращаться к специалисту по обеспечению безопасности и защите персональных данных администрации.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к специалисту по обеспечению безопасности и защите персональных данных администрации.

2.9. Пользователям запрещается:

– разглашать защищаемую информацию третьим лицам;

– копировать защищаемую информацию на внешние носители без разрешения Ответственного за организацию обработки ПДн;

– 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 своем автоматизированном рабочем месте (далее – АРМ);

– подключать к АРМ 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.

2.10. При отсутствии визуального контроля за АРМ доступ к нему должен быть немедленно заблокирован.

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

3. Организация парольной защиты

3.1. Личные пароли доступа к элементам ИСПДн выдаются Пользователям специалистом по обеспечению безопасности и защите персональных данных администрации (далее - администратор ИСПДн).

3.2. Полная плановая смена паролей в ИСПДн проводится администратором ИСПДн.

3.3. 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.).

3.4. Правила хранение пароля:

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

– запрещается сообщать другим Пользователям личный пароль и регистрировать их в системе под своим паролем.

3.5. Лица, использующие пароли, обязаны:

– четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов о порядке ввода и хранения паролей;

– своевременно сообщать администратору ИСПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. 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 др.);

– передавать по Сети защищаемую информацию без использования средств шифрования;

– посещать Интернет-ресурсы, содержащие информацию экстремистского, расистского, порнографического и криминального характера, а также загружать данные, содержащие подобную информацию;

– использовать адрес корпоративной почты при регистрации на Интернет-ресурсах, в ходе деятельности, не связанной с выполнением должностных обязанностей;

– скачивать из Сети медиа-файлы развлекательного характера, программное обеспечение и другие файлы;

– размещать в сети Интернет информацию, классифицированную как «для служебного пользования», «персональные данные», «конфиденциальная информация».

4.3. Ответственный за организацию обработки ПДн оставляет за собой право:

– осуществлять мониторинг использования сотрудниками администрации сети Интернет;

– определять перечень запрещенных Интернет-ресурсов и осуществлять блокировку доступа к ним;

– осуществлять мониторинг появления адресов корпоративной почты на страницах Интернет-ресурсов;

– осуществлять мониторинг появления информации конфиденциального характера о деятельности администрации в сети Интернет, в

том числе и на страницах социальных сетей (www.vk.com, www.odnoklassniki.ru и др.);

– предоставлять информацию об использовании Интернет-ресурсов сотрудниками администрации правоохранительным органам в случаях, предусмотренных законодательством Российской Федерации;

– принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей инструкции.

5. Правила работы с корпоративной электронной почтой

5.1. Электронная почта является собственностью администрации и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

5.2. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию Главы администрации.

5.3. При работе с корпоративной системой электронной почты сотрудникам запрещается:

– использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с Главой администрации;

– публиковать свой адрес, либо адреса других сотрудников на общедоступных Интернет-ресурсах (форумы, конференции и т.п.);

– отправлять сообщения с вложенными файлами, общий объем которых превышает 5 Мегабайт;

– открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;

– осуществлять массовую рассылку почтовых сообщений внешним адресатам без их на то согласия;

– осуществлять массовую рассылку почтовых сообщений рекламного характера;

– рассылка через электронную почту материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;

– распространять информацию, содержание и направленность которой запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;

– распространять информацию ограниченного доступа, представляющую коммерческую тайну;

– предоставлять, кому быто ни было пароль доступа к своему почтовому ящику.

6. Порядок действия пользователя при возникновении инцидента информационной безопасности

При выходе из строя средств защиты информации (СЗИ) необходимо:

– немедленно прекратить обработку информации на объекте;

– обратиться к администратору информационной безопасности.

При выходе из строя составных частей ИСПДн:

– немедленно прекратить обработку информации на объекте;

– обратиться к специалисту по обеспечению безопасности персональных данных.

7. Ответственность пользователя

На пользователя возлагается персональная ответственность за соблюдение установленного режима защиты информации ограниченного распространения в соответствии с его функциональными обязанностями, определенными настоящей Инструкцией.

Пользователь несет ответственность в соответствии с действующим законодательством РФ за нарушение требований настоящей Инструкции.

Приложение № 17
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Инструкция
должностного лица, ответственного за обеспечение безопасности персональных данных

1. Общие положения

1.1. Инструкция является правовым актом, регламентирующим деятельность должностного лица, ответственного за обеспечение безопасности персональных данных (далее – Ответственное лицо) в администрации Раздольненского сельского поселения (далее – администрация), в том числе при выполнении функции по защите ПДн в ИСПДн.

1.2. Целью настоящей Инструкции является регламентирование работы должностного лица, ответственного за обеспечение безопасности персональных данных в практической реализации мер защиты и обеспечения безопасности информации в используемых информационных системах персональных данных Оператора.

1.3. Назначение Ответственного лица, закрепление за ним определенных полномочий и обязанностей производится распоряжением Главы администрации.

1.4. Ответственное лицо должно иметь образование в области защиты информации и стаж работы в данной области не менее трех лет.

1.5. Ответственное лицо должно знать и применять в своей повседневной деятельности:

– законодательные акты, нормативные и методические материалы по вопросам, связанным с обеспечением защиты ПДн;

– структуру ИСПДн, особенности обработки ПДн в ней, перспективы её развития и модернизации;

– функции системы защиты персональных данных (далее СЗПДн);

– документацию на используемые в СЗПДн средства защиты информации;

– методы и средства контроля эффективности защиты ПДн, выявления каналов утечки информации;

– методы планирования и организации проведения работ по защите ПДн;

– технические средства контроля и защиты информации, перспективы и направления их совершенствования.

2. Основные функции Ответственного лица

2.1. Обеспечение устойчивой работоспособности и безопасности ИСПДн в соответствии с нормативными правовыми актами по вопросам обработки и защиты персональных данных.

2.2. Организация работ по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники в ИСПДн, а также правильность использования и штатного

функционирования средств защиты информации, подготовку сотрудников (пользователей ИСПДн) по вопросам безопасной обработки информации в ИСПДн.

3. Права и обязанности Ответственного лица

3.1. Ответственный за обеспечение безопасности персональных данных должен организовывать выполнение следующих мероприятий:

1) по техническому обеспечению безопасности персональных данных при их обработке в ИСПДн, в том числе:

– мероприятий по предоставлению и разграничению доступа в информационные системы персональных данных;

– мероприятий по закрытию технических каналов утечки персональных данных, при их наличии;

– мероприятий по защите от несанкционированного доступа к персональным данным;

– мероприятий по выбору средств защиты персональных данных;

2) своевременное обнаружение фактов несанкционированного доступа к персональным данным, обрабатываемым в ИСПДн;

3) недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование;

4) обеспечение возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5) обеспечение хранения двух копий программных компонент средств защиты информации, их периодическое обновление и контроль работоспособности;

6) постоянный контроль за обеспечением уровня защищенности персональных данных, при их обработке в ИСПДн;

7) проведение внутренних проверок состояния технической защиты персональных данных не менее двух раз в год;

8) определение событий безопасности, подлежащих регистрации, и сроков их хранения, а также состава и содержания информации о событиях безопасности, подлежащих регистрации;

9) определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных;

10) осуществление контроля за соблюдением условий использования средств защиты информации (в том числе криптографических), предусмотренных эксплуатационной и технической документацией;

11) организация периодической проверки электронных журналов автоматизированных средств ИСПДн с целью анализа запросов пользователей ИСПДн на получение доступа к персональным данным, а также актов предоставления персональных данных по этим запросам;

12) организация периодической проверки электронных журналов средств защиты информации с целью анализа событий, представляющих опасность для защищаемых персональных данных;

13) организация ведения поэкземплярного учета носителей персональных данных, применяемых средств защиты (в том числе криптографических), а также эксплуатационной и технической документации к ним;

14) подготовка отчетов о состоянии работ по обеспечения технической защиты персональных данных;

15) осуществление текущего и периодического контроля работоспособности средств и систем защиты ПДн;

16) осуществление периодического контроля за действиями сотрудников при работе с паролями, соблюдением правил их хранения и использования;

17) осуществление планирования и проведения мероприятий по антивирусной защите;

18) обеспечение формирования и поддержания в актуальном состоянии матрицы доступа сотрудников к защищаемым ресурсам ИСПДн;

19) осуществление автоматизированного контроля текущего функционального состояния ИСПДн, включающего просмотр журнала активных сеансов, контроль за работой конкретного рабочего места;

20) поддержание непрерывного функционирования системы защиты персональных данных;

21) проведение ознакомления пользователей ИСПДн с правилами работы со средствами защиты информации. Ответственный за обеспечение безопасности персональных данных обязан:

22) участвовать в подготовке объектов Оператора к аттестации по выполнению требований обеспечения безопасности персональных данных, в случае принятия руководством Оператора решения о необходимости проведения аттестации;

23) участвовать в проводимых работах по совершенствованию системы защиты персональных данных;

24) участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой ПДн, попыток несанкционированного доступа в ИСПДн, несоблюдения правил и условий работы в ИСПДн, хранения носителей персональных данных, использования средств защиты информации (в том числе криптографических) и иных нарушений, снижающих уровень защищенности персональных данных, разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений;

25) информировать лицо, ответственное за организацию обработки персональных данных о фактах нарушения установленного порядка работ, попытках несанкционированного доступа к информационным ресурсам ИСПДн, действиях сотрудников, нарушающих установленные требования к обеспечению безопасности персональных данных.

4. Права Ответственного за обеспечение безопасности персональных данных

4.1. Ответственный за обеспечение безопасности персональных данных имеет право:

1) контролировать работу пользователей в ИСПДн;

2) требовать от должностных лиц, допущенных к обработке персональных данных, безусловного соблюдения установленных правил обработки и защиты персональных данных;

3) вносить свои предложения по совершенствованию мер защиты персональных данных;

4) ходатайствовать перед Главой сельского поселения о прекращении обработки информации, как в целом в ИСПДн, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн;

5) обращаться к лицу, ответственному за организацию обработки персональных данных, с просьбами об оказании необходимой нормативной и методической помощи в работе;

6) получать доступ во все помещения, в которых осуществляется обработка персональных данных;

7) привлекать в установленном порядке необходимых специалистов из числа сотрудников для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам организации технической защиты персональных данных;

8) вносить руководству предложения о наказании отдельных сотрудников, допущенных к работе в ИСПДн и допустивших серьезные нарушения, приведшие к нарушению безопасности персональных данных.

5. Ответственность Ответственного лица

5.1. Ответственное лицо несет персональную ответственность за:

1) выполнение возложенных на него обязанностей, предусмотренных настоящей инструкцией;

2) правильность и объективность принимаемых решений;

3) качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями;

4) соблюдение трудовой дисциплины, охраны труда, разглашение сведений ограниченного распространения, ставших известными ему в ходе выполнения должностных обязанностей.

Приложение № 18
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

УТВЕРЖДАЮ

Глава администрации
Раздольненского сельского
поселения

_____
«__»_____ 20__ г.

ЖУРНАЛ
проведения инструктажей по информационной безопасности

Начат « » _____ 20__ г.
Окончен « » _____ 20__ г.

Инструкция по ведению журнала

Записи в журнале делаются с периодичностью, установленной в разделе «Информирование и обучение персонала» утвержденного плана мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации.

В графе **«Дата инструктажа»** указывается дата проводимого инструктажа.

В графе **«Тема инструктажа»** указывается краткое содержание проводимого инструктажа, например: «Доведение до сотрудников методов противодействия социальной инженерии».

В графе **«Инструктируемый»** указываются фамилии, инициалы и росписи лиц, прослушавших инструктаж.

В графе **«Инструктирующий»** указываются фамилия, инициалы и роспись лица, проводившего инструктаж.

№ п/п	Инструктаж		Инструктируемый		Инструктирующий	
	Дата	Тема	ФИО	Подпись	ФИО	Подпись

Приложение № 19
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

УТВЕРЖДАЮ

Глава администрации
Раздольненского сельского
поселения

_____
«__»_____ 20__ г.

ЖУРНАЛ
учета средств защиты информации в информационных системах
персональных данных

Начат « » _____ 20__ г.
Окончен « » _____ 20__ г.

Инструкция по ведению журнала

Записи в журнале делаются по мере установки и настройки средств защиты информации.

В графе «**Название средства защиты информации**» указывается наименование средства защиты информации.

В графе **«Тип средства защиты информации»** указывается тип средства защиты информации – программные или программно-аппаратный.

В графе **«Зав. номер (номер знака соответствия)»** указывается заводской номер и номер знака соответствия согласно формуляру на средство защиты (знак соответствия – голограмма ФСТЭК, которая вклеена либо в формуляр, либо наклеена на коробку диска дистрибутива средства защиты). Для средств защиты, сертифицированных ФСБ (например, ViPNet Client) вместо знака соответствия указывается регистрационный номер ФСБ.

В графе **«Сертификат»** указывается номер сертификата ФСТЭК России и/или ФСБ России и дата до которого он действует.

В графе **«Место и дата установки»** указывается номер АРМ согласно техпаспорту на систему (если он разработан), либо доменное имя АРМ (или виртуальной машины/сервера), а также дата установки (в ОС Windows можно узнать в меню «Панель задач» - «Программы и компоненты»).

В графе **«Примечание»** можно делать любые пометки, например: об удалении данного экземпляра средства защиты.

№ п/п	Наименование средства защиты информации	Тип средства защиты информации	Зав. номер (номер знака соответствия)	Сертификат	Место и дата установки	Примечание

Приложение № 20
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

УТВЕРЖДАЮ

Глава администрации
Раздольненского сельского
поселения

_____
«__»_____ 20__ г.

ЖУРНАЛ
периодического тестирования средств защиты информации в информационных системах персональных данных

Начат « » _____ 20__ г.
Окончен « » _____ 20__ г.

Инструкция по ведению журнала

Записи в журнале делаются с периодичностью, установленной в разделе «Тестирование работоспособности средств защиты информации» утвержденного плана мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации.

В графе **«Наименование средства защиты информации»** указывается название тестируемого средства защиты, например «ViPNet Client»

В графе **«Регистрационные номера средства защиты информации»** указывается номер голограммы для средств защиты, сертифицированных ФСТЭК и регистрационные номера для средств защиты, сертифицированных ФСБ.

В графе **«Дата тестирования»** указывается дата проведения тестирования.

В графе **«Фамилия и подпись ответственного пользователя, проводившего тестирование»** указывается ФИО и подпись администратора безопасности и/или другого лица, проводившего тестирование.

В графе **«Наименование теста, используемые средства для проведения теста»** вносится краткое описание методики и инструментов тестирования, например, следующее: «Анализ сетевого трафика с помощью Wireshark».

В графе **«Результат тестирования»** коротко описывается полученные в результате тестов результат, например: «Успешный. Трафик на защищаемые узлы и ресурсы передается в зашифрованном виде».

В графе **«Дата очередного тестирования»** указывается предполагаемая дата очередного идентичного теста.

№ п/п	Наименование средства защиты информации	Регистрационные номера средства защиты информации	Дата тестирования	Фамилия и подпись ответственного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования	Дата очередного тестирования

Приложение № 21
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

УТВЕРЖДАЮ

Глава администрации
Раздольненского сельского
поселения

_____
«__»_____20__ г.

ЖУРНАЛ
учета мероприятий по контролю обеспечения защиты информации в информационных системах персональных данных

Начат « » _____ 20__ г.
Окончен « » _____ 20__ г.

Инструкция по ведению журнала

Записи в журнале делаются с периодичностью, установленной в разделах утвержденного плана мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации (за исключением разделов «Информирование и обучение персонала» и «Тестирование работоспособности средств защиты информации»).

В графе **«Мероприятие»** указывается краткое описание мероприятия в соответствии с планом мероприятий.

В графе **«Дата»** указывается дата проведения мероприятия.

В графе **«Исполнитель»** указывается фамилия, инициалы и роспись лица, проводившего мероприятие.

В графе **«Результат»** указывается краткое описание результата проведенного мероприятия.

№ п/п	Мероприятие	Дата	Исполнитель (ФИО, подпись)	Результат

Приложение № 22
к постановлению администрации Раздольненского сельского поселения от 13.11.2023 № 195

Перечень информационных систем персональных данных

1. Информационная система «Заработная плата и кадровый учет» (Веснин).
2. Информационная система «1-С».