

**АДМИНИСТРАЦИЯ РОЖДЕСТВЕНСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ
УВЕЛЬСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ЧЕЛЯБИНСКОЙ ОБЛАСТИ**

457011, Челябинская область, Увельский район, с.Рождественка, ул.Совхозная 2

ИНН – 7440000741, КПП – 742401001, ОКОНХ- 97620, ОКПО – 04270021

телефон (факс 8-351-52-1-79), 52-1-16,

e-mail: rog52179@mail.ru

ПОСТАНОВЛЕНИЕ

от «20» ноября 2017 г.

№ 36

Об утверждении Положения
«Об обеспечении безопасности
персональных данных при их
обработке в информационных
системах персональных данных
Администрации
Рождественского сельского
поселения»

На основании Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации 17 ноября 2007 г. № 781, Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных»,

ПОСТАНОВЛЯЮ:

1. Утвердить Положение «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Рождественского сельского поселения» (приложение).
2. Организацию выполнения настоящего постановления возложить на делопроизводителя Горбунову Евгению Викторовну.
3. Настоящее постановление вступает в силу со дня его подписания.

Глава Рождественского сельского поселения:



С.М. Панов

ПОЛОЖЕНИЕ ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ
ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ
АДМИНИСТРАЦИИ РОЖДЕСТВЕНСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ.

1. Общие положения

1.1. Настоящее Положение разработано на основании требований Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации 17 ноября 2007 г. № 781, Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных».

1.2. Под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.3. Положение определяет порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Рождественского сельского поселения.

1.4. Положение разработано с целью обеспечения защиты прав и свобод субъекта персональных данных при обработке его персональных данных, а также с целью установления ответственности должностных лиц Администрации Рождественского сельского поселения, имеющих доступ к персональным данным, за невыполнение требований и норм, регулирующих обработку и защиту персональных данных.

1.5. Требования настоящего Положения являются обязательными для исполнения во всех подразделениях, всеми должностными лицами Администрации Рождественского сельского поселения.

1.6. За общее состояние и организацию работ по защите персональных данных, используемых при их обработке в информационных системах персональных данных Администрации Рождественского сельского поселения отвечает Глава Рождественского сельского поселения.

1.7. Ответственность за организацию и выполнение мероприятий по защите информации в структурных подразделениях Администрации Рождественского сельского поселения возлагается на руководителей структурных подразделений.

1.8. Контроль выполнения требований настоящего Положения возлагается на Главу Рождественского сельского поселения.

1.9. Для организации защиты персональных данных, в том числе для проведения аттестации информационных систем персональных данных могут привлекаться специализированные организации, имеющие лицензию на этот вид деятельности.

1.10. Используемые технические и программные средства защиты информации должны быть сертифицированы в соответствии с требованиями положения «О сертификации средств защиты информации», утвержденного постановлением Правительства Российской Федерации от 26 июня 1995 г. N 608.

2. Термины и сокращения

Администратор ИБ – Администратор информационной безопасности;

ИСПДн - Информационная система персональных данных;

КИС - Комплекс информационных систем;

Начальник отдела ИТ - Начальник отдела информационных технологий;

ПДн - Персональные данные.

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

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

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

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

Личный кабинет – персональный раздел Клиента на веб-сайте XXX, веб-интерфейс к личному счету клиента;

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

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

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

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

Субъект персональных данных – физическое лицо, к которому относятся персональные данные и которой может быть идентифицирован на основании таких данных. В настоящем документе под субъектом персональных данных понимается:

- клиент ХХХ – физическое лицо, с которым ХХХ имеет договорные отношения;
- клиент ХХХ – юридическое лицо, представитель компании контрагента, с которым ХХХ имеет договорные отношения;

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2.1. Результатом защиты информации является предотвращение ущерба Администрации Рождественского сельского поселения Челябинской области из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Целями технической защиты конфиденциальной информации в Администрации Рождественского сельского поселения являются:

- предотвращение утечки охраняемых сведений по техническим каналам;
- предотвращение несанкционированного доступа (НСД) к информации, ее разрушения, искажения, уничтожения, блокировки и несанкционированного копирования в системах и средствах автоматизации.

2.2. Замыслом достижения целей защиты информации является обеспечение защиты информации путем строгого соблюдения действующих норм и требований ФСТЭК России (Гостехкомиссии России), созданием СЗИ объектов информатизации и принятием эффективных режимных мер, предписанных руководящими документами.

2.3. Охраняемые сведения:

- конфиденциальная информация, обрабатываемая с использованием технических средств;
- сведения конфиденциального характера, содержащиеся в речевой информации.

2.4. Потенциальные угрозы информационной безопасности объектов.

В качестве угроз информационной безопасности объектов необходимо рассматривать:

- использование разведками иностранных государств технических средств для получения охраняемых сведений, перехват информации, обсуждаемой в защищаемых помещениях и циркулирующей в основных технических средствах и системах, а также воздействие на информационные ресурсы автоматизированных систем с целью разрушения, искажения и блокирования информации;
- использование криминальными структурами технических средств для получения информации, представляющей ценность в интересах планирования криминальных акций;
- несанкционированный удаленный доступ (из-за пределов контролируемых зон) в сети систем информатизации и связи объектов с целью получения информации ограниченного доступа и использования возможностей систем связи (компьютерная

разведка, дистанционный доступ к программным средствам иностранных цифровых электронных автоматических телефонных станций);

- преднамеренные действия нарушителей и злоумышленников, незаконным путем проникших на объекты, посредством контактного несанкционированного доступа к элементам автоматизированных систем, к носителям информации, к вводимой и выводимой информации, к программному обеспечению, а также подключения к линиям связи;

- непреднамеренные действия персонала, приводящие к утечке, искажению, разрушению информации, подлежащей защите, в том числе ошибки проектирования, разработки и эксплуатации технических и программных средств автоматизированных систем.

2.5. Оценка возможностей технических средств разведки иностранных государств и криминальных структур проводится с использованием модели иностранной технической разведки, методик оценки возможностей иностранной технической разведки и других нормативных документов ФСТЭК России (Гостехкомиссии России) применительно к охраняемым сведениям об объектах, к информации, циркулирующей (обсуждаемой) в защищаемых помещениях и основных технических средствах и системах объектов.

2.6. Для ведения перехвата информации, циркулирующей в средствах и системах информатизации и связи объектов в Администрации Рождественского сельского поселения, могут использоваться следующие виды технической разведки:

- стационарная;
- портативная возимая;
- портативная носимая;
- автономная автоматическая.

2.7. Одной из возможных угроз информационным ресурсам автоматизированных систем при определенных условиях может являться компьютерная разведка, направленная на извлечение, систематизацию и специальную обработку открытой информации из информационно-вычислительных сетей, телекоммуникационных систем, а также информации об особенностях их построения и функционирования. Таким условием может быть несанкционированный выход с отдельных рабочих мест автоматизированных систем в глобальные информационные сети. Бесконтрольное подключение к информационно-вычислительным сетям общего пользования компьютерных средств и оргтехники, находящихся на защищаемых объектах, может служить предпосылкой к утечке охраняемой информации.

3. Порядок аттестации и ввода в эксплуатацию объектов информатизации

3.1. Все объекты информатизации должны быть аттестованы на соответствие установленным нормам и требованиям по защите информации.

3.2. Аттестация по требованиям безопасности информации является необходимым условием для ввода в эксплуатацию объектов информатизации.

3.3. В Администрации Рождественского сельского поселения аттестации подлежат следующие объекты информатизации:

- защищаемые помещения, предназначенные для проведения совещаний по обсуждению конфиденциальной информации;
- объекты вычислительной техники, используемые для обработки конфиденциальной информации.

3.4. Аттестационные испытания проводятся комиссией, формируемой аккредитованным ФСТЭК России органом по аттестации, по программе, согласованной с Администрацией Увельского муниципального района Челябинской области.

3.5. Для проведения испытаний аттестационной комиссии ответственным по защите информации подготавливаются и представляются:

- технический паспорт на объект информатизации;
- акт классификации автоматизированной системы по требованиям защиты информации;
- состав технических и программных средств, входящих в АС, или технических средств, расположенных в выделенном помещении;
- планы размещения ОТСС и ВТСС;
- состав и схемы размещения средств защиты информации;
- план контролируемой зоны;
- схемы прокладки линий передачи данных;
- схемы и характеристики систем электропитания и заземления объекта информатизации;
- перечень защищаемых в АС ресурсов (или конфиденциальность обсуждаемых в защищаемом помещении вопросов);
- организационно-распорядительная документация разрешительной системы доступа персонала к защищаемым ресурсам АС (обсуждаемым вопросам);
- инструкции пользователям и администратору безопасности информации;
- инструкции по эксплуатации средств защиты информации;
- предписания на эксплуатацию технических средств и систем;
- протоколы специальных исследований технических средств и систем;
- сертификаты соответствия требованиям по безопасности информации на используемые средства защиты информации.

3.6. Аттестационные испытания объекта информатизации проводятся до полного их завершения в соответствии с программой испытаний вне зависимости от промежуточных результатов испытаний и завершаются выдачей Аттестата соответствия.

3.7. Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации, указывается в Аттестате соответствия.

3.8. Разрешение на использование технических систем и средств для обработки конфиденциальной информации, защищаемых помещений для проведения переговоров по конфиденциальной тематике выдается Главой Рождественского сельского поселения в письменной форме на основании результатов их аттестации.

3.9. По результатам аттестации специалистом по защите информации разрабатываются и доводятся до исполнителей инструкции, памятки и рекомендации о порядке выполнения мероприятий по защите информации.

3.10. Обсуждение и обработка конфиденциальной информации до окончания аттестации и распоряжения о вводе в строй объектов информатизации запрещается.

4. Организационные и технические мероприятия по защите конфиденциальной информации

4.1. Защита сведений конфиденциального характера в Администрации Рождественского сельского поселения достигается путем создания системы защиты информации, которая включает комплекс организационных, технических и программных мероприятий, направленных на закрытие технических каналов утечки информации.

4.2. Мероприятия по защите информации являются составной частью деятельности Администрации Рождественского сельского поселения, проводятся с целью закрытия возможных технических каналов утечки информации. Эти мероприятия проводятся на всех циклах создания, развития и эксплуатации используемых технических систем и средств, а также при ремонте, реконструкции и эксплуатации защищаемых помещений.

4.3. С целью закрытия возможных технических каналов утечки речевой информации в Администрации Рождественского сельского поселения рекомендуется проведение следующих мероприятий:

4.3.1. Применение организационно-режимных мероприятий:

- временное увеличение контролируемой зоны;
- закрытие дверей в защищаемые помещения между мероприятиями и в нерабочее время на ключ;
- выдача ключей от защищаемых помещений только лицу, ответственному за это помещение;
- установка и замена оборудования, мебели, ремонт только по согласованию и под контролем специалиста по защите информации.

4.3.2. Обеспечение необходимой звукоизоляции защищаемых помещений (закрытие акустического и виброакустического каналов утечки информации) путем:

- обивки входных дверей звукопоглощающими материалами;
- оборудования подвесных звукопоглощающих потолков со звукоизолирующим слоем;
- усиления стен и перегородок конструкциями типа "стена на откосе";
- применения надежных шумопоглотителей для вентиляционных отверстий;
- оборудования двойных дверей с тамбуром с вибрационной развязкой дверных коробок;
- использования штор из плотной материи на окнах;
- применения звукопоглощающих материалов для покрытия стен, потолка и пола.

4.3.3. Принятие мер по закрытию электроакустического канала за счет установки в защищаемых помещениях:

- устройств телефонной связи, радиотрансляции, оповещения, сигнализации и электрочасофикации, сертифицированных по требованиям безопасности информации либо прошедших специальные исследования, имеющие предписание на эксплуатацию;
- защищенных от утечки информации за счет электроакустических преобразований и «навязывания» оконечных устройств телефонной связи (телефонные аппараты, концентраторы, телефаксы и т.п.), включенных в городскую АТС;
- систем пожарной и охранной сигнализации, построенных только по проводной схеме сбора информации.

4.3.4. Запрещение использования в защищаемых помещениях радиотелефонов, оконечных устройств сотовой, пейджинговой и транкинговой связи, незащищенных переносных магнитофонов и других средств аудио- и видеозаписи.

4.3.5. Отключение от сети телефонных и факсимильных аппаратов с автоответчиками или сикерфоном, а также телефонных аппаратов с автоматическим определителем номера в защищаемых помещениях.

4.3.6. Проведение специальной проверки защищаемых помещений на наличие возможно внедренных в них специальных подслушивающих устройств по решению Главы Рождественского сельского поселения.

4.4. С целью закрытия возможных каналов утечки сведений, отнесенных к конфиденциальной информации, при их обработке и хранении в технических системах и средствах рекомендуется применение следующих мер защиты:

- использование технических средств, сертифицированных по требованиям безопасности информации;
- использование сертифицированных средств защиты информации;
- проведение объектовых измерений в местах обработки конфиденциальной информации с оценкой эффективности и достаточности принятых мер защиты;
- предотвращение организационными мерами несанкционированного доступа к обрабатываемой информации;
- выполнение положений Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30 августа 2002 г. № 282, при организации обработки информации в локальных вычислительных сетях;
- выполнение требований Указа Президента РФ от 17 марта 2008 г. № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";
- осуществление учета машинных носителей информации и их хранение в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах);
- организация процесса резервного копирования и архивирования как неотъемлемой части политики защиты информации.

4.5. Документальное оформление мероприятий по защите информации включает:

- приказ об утверждении перечня защищаемых помещений и объектов вычислительной техники, предназначенных для обработки конфиденциальной информации;
- приказ о вводе в эксплуатацию объектов информатизации;
- план-схему контролируемой зоны;
- акты классификации АС по требованиям защиты от НСД к информации;
- паспорта защищаемых помещений и объектов ВТ;
- аттестаты соответствия объектов информатизации.

5. Обязанности и права должностных лиц

5.1. Глава Рождественского сельского поселения:

- отвечает за организацию работ по защите информации в Администрации Рождественского сельского поселения;
- утверждает перечень защищаемых помещений, основных технических систем и средств, также другие документы по вопросам защиты информации;
- утверждает акты классификации АС.

5.2. Специалист по защите информации:

- совместно с начальниками основных подразделений Администрации Рождественского сельского поселения осуществляет планирование мероприятий по защите информации, мероприятий по подготовке помещений и объектов информатизации к работе со сведениями конфиденциального характера, организует их выполнение и контроль эффективности принятых мер;
- разрабатывает организационно-распорядительные документы по вопросам защиты информации;
- разрабатывает предложения по финансированию мероприятий, связанных с защитой информации;
- координирует работы по защите информации, проводимые в структурных подразделениях, оказывает им практическую и методическую помощь;

- в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации, разрабатывает предложения по дальнейшему совершенствованию системы защиты информации при использовании технических средств;
- обеспечивает защиту информации, циркулирующей в АС, в том числе передаваемой по каналам связи, организывает работы по проведению специальных исследований технических средств обработки и передачи информации, по аттестации объектов ВТ на соответствие нормативным требованиям;
- проводит систематический контроль работы средств защиты информации, применяемых на объектах ВТ, а также следит за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;
- обобщает и анализирует сведения о противоправных устремлениях к информации, попытках преодоления систем защиты информации, используемых при этом методах и средствах;
- анализирует состояние защищенности информационных ресурсов сети, готовит предложения по совершенствованию систем защиты, систематизирует и распространяет положительный опыт работы;
- участвует в проведении обследования подразделений с целью выявления сведений конфиденциального характера, циркулирующих в средствах вычислительной техники, а также с целью выявления существующих угроз безопасности информации, определяет практические мероприятия по устранению имеющихся недостатков;
- принимает меры по предупреждению угроз безопасности информации, возникающих в результате случайных ошибок персонала при обработке электронных документов с учетом специфики конкретного места обработки и применяемых средств защиты;
- принимает участие в оценке реальной опасности утечки информации, подлежащей защите при использовании технических средств, в разработке эффективных и экономически обоснованных мер по ее защите;
- организывает работу по эксплуатации системы защиты информации в автоматизированных системах обработки электронных документов;
- проводит работы по внедрению технических и программных средств защиты информации от несанкционированного доступа к ней на действующих автоматизированных системах и отдельных средствах вычислительной техники;
- обеспечивает эксплуатацию технических и программных средств защиты информации на действующих автоматизированных системах и отдельных средствах вычислительной техники, контролирует работоспособность и эффективность функционирования этих средств;
- распределяет между пользователями средств вычислительной техники необходимые реквизиты криптографической защиты (пароли, ключи защиты и т.п.), формирует и распределяет между пользователями необходимые реквизиты защиты от НСД (в зависимости от системы защиты);
- проводит контроль целостности СЗИ, программного обеспечения с целью выявления несанкционированных изменений в них;
- принимает участие в разработке документов по обеспечению безопасности информации при эксплуатации ЛВС;
- не допускает подключения к локальной сети или к СВТ нештатных блоков и устройств, не прошедших специальные исследования, не имеющих предписания на эксплуатацию;
- осуществляет контроль прав доступа сотрудников государственного органа к информационным ресурсам локальной вычислительной сети;
- осуществляет контроль разграничения прав доступа к защищаемой информации на несъемных носителях информации рабочих мест пользователей;
- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток неправомерного доступа к охраняемым сведениям или попыток хищения, копирования,

изменения сообщает начальнику отдела и незамедлительно принимает меры пресечения нарушений.

Специалист по защите информации имеет право:

- контролировать исполнение приказов и распоряжений вышестоящих организаций и главы Рождественского сельского поселения по вопросам сохранения конфиденциальной информации;
- требовать от руководителей проверяемых подразделений устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;
- рекомендовать запрещать эксплуатацию систем обработки и передачи информации при несоблюдении требований по защите информации;
- готовить проекты договоров на выполнение работ по защите информации со сторонними организациями, имеющими необходимые лицензии;
- вносить предложения по совершенствованию системы защиты информации, изменению категорий объектов информатизации, степени конфиденциальности обрабатываемой информации;
- иметь доступ к средствам обработки и передачи информации подразделений, постоянно осуществлять проверки состояния защиты информации, контролировать состояние защищенности объектов информатизации;
- требовать от пользователей автоматизированных систем безусловного соблюдения установленной технологии обработки электронных документов и выполнения требований по информационной безопасности.

5.4. Пользователи объекта ВТ обязаны:

- строго соблюдать меры по защите информации и правила эксплуатации СВТ;
- обеспечивать сохранность комплекта ПЭВМ, машинных носителей информации и целостность установленного программного обеспечения;
- знать и соблюдать установленные требования по учету, хранению и пересылке машинных, бумажных и иных носителей информации;
- применять антивирусные программы при включении СВТ или при использовании гибких магнитных носителей информации;
- по окончании обработки конфиденциальной информации "обнулить" оперативную память компьютера путем перезагрузки или временного выключения ПЭВМ;
- перед началом обработки убедиться в работе средств защиты информации (генераторы шума и т.д.).

5.5. Глава администрации Рождественского сельского поселения:

- участвует в определении помещений, в которых необходимо проводить мероприятия с обсуждением вопросов конфиденциального характера (защищаемые помещения), мест установки и количества СВТ, необходимых для обработки информации, требующей защиты.

5.6. Руководители структурных подразделений Администрации Рождественского сельского поселения:

- лично отвечают за защиту информации в структурном подразделении, сохранность машинных и иных носителей информации;
- организуют выполнение мероприятий по защите конфиденциальной информации при использовании технических средств;
- участвуют в определении правил разграничения доступа к информации в системах и средствах информатизации, используемых в Администрации Рождественского сельского поселения;

- согласовывают со специалистом, ответственным по защите информации, установку, замену и перемещение технических средств в помещениях, где обрабатывается конфиденциальная информация.

6. Планирование работ по защите конфиденциальной информации

6.1. Планирование работ по защите информации проводится на основании:

- рекомендаций актов проверок контрольными органами ФСТЭК России;
- результатов анализа деятельности в области защиты информации;
- рекомендаций и указаний ФСТЭК России;
- рекомендаций актов проверок Информационно-технического управления Администрации Губернатора Челябинской области.

6.2. Для подготовки и реализации организационных и технических мероприятий по защите информации, а также для увязки этих мероприятий с планами работ подразделений Администрации Рождественского сельского поселения составляется годовой план работ по защите информации.

6.3. Годовой план работ по защите информации составляется специалистом, ответственным по защите информации, и утверждается главой Рождественского сельского поселения.

В годовом плане указываются:

- планируемые работы по защите информации и контролю ее эффективности;
- подразделения, должностные лица, отвечающие за выполнение указанных работ, и исполнители этих работ;
- сроки выполнения работ.

6.4. Контроль выполнения годового плана возлагается на специалиста, ответственного по защите информации.

7. Контроль состояния защиты конфиденциальной информации

7.1. С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность систем информатизации, осуществляется контроль состояния и эффективности защиты информации.

7.2. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

7.3. Повседневный контроль выполнения организационных и технических мероприятий, направленных на обеспечение защиты информации, проводится руководителями структурных подразделений и специалистом по защите информации.

7.4. Периодический контроль может осуществляться представителями ФСТЭК России, территориальных органов ФСБ России, Информационно-технического управления Администрации Губернатора Челябинской области.

7.5. Допуск представителей этих органов для проведения контроля состояния защиты информации осуществляется в установленном порядке по предъявлению служебных удостоверений и предписаний на право проверки, подписанных руководителем (заместителем) соответствующего органа.

7.6. К контролю эффективности мероприятий по защите информации могут привлекаться специалисты проверяемых подразделений.

7.7. Результаты проверок отражаются в техническом паспорте объекта информатизации.

7.8. Периодичность проверок объектов информатизации, где обрабатывается (обсуждается) конфиденциальная информация, - 1 раз в год и при каждом изменении состава и расположения основных технических средств и систем.

7.9. Специалист, ответственный по защите информации, обязан присутствовать при всех проверках Администрации Рождественского сельского поселения по вопросам защиты информации.

7.10. По результатам проверок контролирующими органами глава Рождественского сельского поселения с привлечением других заинтересованных специалистов в десятидневный срок разрабатывает план устранения выявленных недостатков.

7.11. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

7.12. При обнаружении нарушений глава Рождественского сельского поселения обязан принять необходимые меры по их устранению в сроки, согласованные с органом или лицом, проводившим проверку.

1. Утвердить Положение «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Рождественского сельского поселения» (приложение).

2. Организацию выполнения данного постановления возложить на заместителя Горюхиной Евгению Викторовну.

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

Глава Рождественского сельского поселения:

С.М. Панов