Г Е Р Б
МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ
«**РОМАНОВСКОЕ СЕЛЬСКОЕ ПОСЕЛЕНИЕ**»
ВСЕВОЛОЖСКОГО МУНИЦИПАЛЬНОГО РАЙОНА
ЛЕНИНГРАДСКОЙ ОБЛАСТИ
АДМИНИСТРАЦИЯ

ПОСТАНОВЛЕНИЕ

22.10.2018 № 442
пос.Романовка

Об утверждении Положения по обеспечению безопасности информации в администрации МО «Романовское сельское поселение»

Руководствуясь Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в соответствии с Уставом МО «Романовское сельское поселение», постановлением главы администрации МО «Романовское сельское поселение» от 22.10.2018 № 441 «Об утверждении Правил обработки персональных данных в администрации МО «Романовское сельское поселение» Всеволожского муниципального района Ленинградской области»,
ПОСТАНОВЛЯЮ:

1. Утвердить Положение по обеспечению безопасности информации в администрации МО «Романовское сельское поселение» (Приложение № 1);
2. Назначить администраторов безопасности информационных систем персональных данных в администрации МО «Романовское сельское поселение» (Приложение №2);
3. Утвердить инструкцию администратора безопасности информационной системы персональных данных в администрации МО «Романовское сельское поселение» (Приложение №3);
4. Утвердить Перечень информационных систем персональных данных в администрации МО «Романовское сельское поселение» (Приложение №4);
5. Настоящее постановление разместить на официальном сайте муниципального образования в сети Интернет по адресу:www.romanovka.ru для сведения.
6. Контроль за исполнением настоящего постановления оставляю за собой.

Глава
администрации С.В.Беляков

Приложение № 1
к постановлению главы
администрации
от _____2018 № ___

ПОЛОЖЕНИЕ
по обеспечению безопасности информации в администрации
МО «Романовское сельское поселение»

1.**Общие положения**

1.1. Настоящее Положение устанавливает комплекс организационных, технических и правовых мер защиты информации.
1.2. Положение является обязательным для всех сотрудников администрации, осуществляющих обработку персональных данных и иной конфиденциальной информации.
1.3. Специалисты администрации организуют работу по обеспечению информационной безопасности и осуществляют контроль за соблюдением требований безопасности информации.
1.4. Термины и формулировки, использующиеся в настоящем Положении:
- конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
- распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
- электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
- документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
- электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;
- оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации

информационной системы,в том числе по обработке информации, содержащейся в ее базах данных;

- система защиты информации – это совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам и нормам, устанавливаемыми соответствующими документами в области защиты информации;

- техника защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации;

- средство криптографической защиты информации (далее - СКЗИ) – программа (служба), которая обеспечивает шифрование и расшифровку документов, отвечает за работу с электронной подписью. СКЗИ может быть встроена в носитель или представлена как отдельный программный продукт;

- информации – это средства автоматизированное рабочее место (далее - АРМ) – рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных с целью получения информации, обеспечивающей поддержку принимаемых им решений при выполнении профессиональных функций;

- информационная система (далее - ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

- доступ к информации - возможность получения информации и ее использования;

- несанкционированный доступ к информации – действия, нарушающие установленный порядок доступа или правила разграничения, установленные в администрации;

- информационная безопасность – защищенность информации от ее перехвата, утечки по техническим и иным каналам, модификации, блокирования, уничтожения, несанкционированного доступа к ней, а также защищенность технических и программных средств сбора, обработки, накопления, хранения, поиска и передачи информации, информационных и телекоммуникационных систем от нарушения их функционирования или от вывода их из строя;

- системный администратор – специалист администрации, обеспечивающий эксплуатацию АРМ;

- средства защиты информации – программные, технические, программно-технические средства, предназначенные для защиты информации;

- матрица доступа - таблица, отображающая правила разграничения доступа.

1.5. Допуск пользователей ИС для работы с конфиденциальными данными, находящимися в ИС, осуществляется в соответствии со списком лиц, допущенных к работе, утвержденным актом администрации.

1.6. На основании списка лиц, допущенных к персональным данным и иной конфиденциальной информации системный администратор разрабатывает таблицу разграничения доступа к персональным данным и иной конфиденциальной информации, обрабатываемой в администрации (приложение 1 к настоящему Положению).

1.7. Вход пользователя ИС в ИС осуществляется на основе ввода (по запросу системы) личных пароля и электронного идентификатора конкретного пользователя ИС.

1.8 Правами администратора в операционной системе АРМ может обладать только системный администратор администрации.

2. **Цели и основные меры по защите информации**

2.1. **Целями по защите информации являются**:

1. Информирование сотрудников администрации о мерах и требованиях по защите информации;

2. Соблюдение конфиденциальности информации ограниченного доступа;

3. Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

4.Обеспечение реализации права граждан о неразглашении их персональных данных;

5. Информационная безопасность в администрации обеспечивается средствами защиты информации и комплексом организационных и технических мер.

6. **К организационным мерам относятся**:

- организация охранного режима на территории администрации;
- контроль за соблюдением сотрудниками должностных инструкций и иной документации в сфере обеспечения информационной безопасности;
- своевременное информирование сотрудников об изменениях законодательства в сфере обеспечения информационной безопасности;
- назначение должностных лиц, ответственных за организацию работы по обеспечению информационной безопасности;
- применение утвержденной в установленном порядке эксплуатационной документации;
- соблюдение установленных правил обеспечения безопасности информации при работе с программными и техническими средствами, в том числе со средствами защиты информации и антивирусной защиты в администрации;

- Разграничение доступа к файлам, каталогам и дискам;
- Разграничение доступа к комплексам программ;
- Идентификация пользователей.

2.2. **К техническим мерам относятся:**

Применение сертифицированных специальных и лицензионных программных средств общего назначения, а также сертифицированных технических средств и средств связи.

3. Соблюдение мер защиты информации при использовании средств автоматизации

3.1. Защита информации, содержащейся в информационной системе

Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в ИС;
- разработка системы защиты информации ИС;
- внедрение системы защиты информации ИС;
- аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;
- обеспечение защиты информации, в ходе эксплуатации аттестованной ИС;
- обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации.

3.2. **При принятии решения о необходимости защиты информации, содержащейся в ИС, осуществляется**:

- анализ целей создания ИС и задач, решаемых этой ИС;
- определение информации, подлежащей обработке в ИС;
- анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС;

3.2.1. Принятие решения о необходимости создания системы защиты информации ИС, а также определение целей и задач защиты информации в ИС, основных этапов создания системы защиты информации ИС и функций по обеспечению защиты информации, содержащейся в ИС, обладателя информации (заказчика), оператора и уполномоченных лиц.

3.3. **Разработка и внедрение системы защиты информации ИС**.

Требования к системе защиты информации ИС включаются в техническое задание на создание ИС и (или) техническое задание (частное техническое задание) на создание системы защиты информации ИС, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать: цель и задачи обеспечения защиты информации в ИС; класс защищенности ИС; перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС; перечень объектов защиты ИС; требования к мерам и средствам защиты

информации, применяемым в ИС; стадии (этапы работ) создания системы защиты ИС; требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации; функции заказчика и оператора по обеспечению защиты информации в ИС; требования к защите средств и систем, обеспечивающих функционирование ИС (обеспечивающей инфраструктуре); требования к защите информации при информационном взаимодействии с иными ИС и информационно-телекоммуникационными сетями, в том числе с ИС уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

3.4. **Угрозы безопасности информации определяются** по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей ИС, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

3.5. **Требования к системе защиты информации ИС определяются** в зависимости от класса защищенности ИС и угроз безопасности информации, включенных в модель угроз безопасности информации.

3.6. **Основные функциональные обязанности пользователя ИС**

3.6.1. **Пользователь ИС обязан**:

- знать и выполнять требования действующих нормативных правовых актов и руководящих документов, а также Положение по обеспечению безопасности информации в администрации, регламентирующих порядок действий по обеспечению безопасности информации;
- выполнять на АРМ только те процедуры, которые определены для него его обязанностями;
- соблюдать правила при работе в сетях общего доступа и (или) международного обмена – сети «Интернет» и других;
- экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами;
- обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к лицу, ответственному за обеспечение информационной безопасности, в отношении которой установлено требование об обеспечении ее конфиденциальности (далее – администратор безопасности информации).

3.6.2. Для получения консультаций по вопросам работы и настройки элементов ИС, связанных с обеспечением безопасности, необходимо обращаться к администратору безопасности информации.

3.6.3. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован.

3.6.4. При использовании планировщика заданий состав запускаемого программного обеспечения на рабочем месте согласовывается с администратором безопасности информации.

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

3.6.6. По окончании работы в ИС выйти из системы и выключить компьютер.

3.7. **Пользователям ИС запрещается**:

3.7.1. Разглашать информацию, в отношении которой установлено требование об обеспечении ее конфиденциальности, третьим лицам;

3.7.2. Копировать информацию, в отношении которой установлено требование об обеспечении ее конфиденциальности, на внешние носители без разрешения своего руководителя;

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

3.7.4. Несанкционированно открывать общий доступ к каталогам на своем АРМ;

3.7.5. Подключать к АРМ и корпоративной информационной сети личные отчуждаемые машинные носители и мобильные устройства;

3.7.6. Отключать (блокировать) средства защиты информации;

3.7.7. Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя ИС по доступу к ИС;

3.7.8. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИС;

3.7.9. Привлекать посторонних лиц для осуществления ремонта или настройки АРМ без согласования с администратором безопасности информации;

3.7.10. Сообщать, передавать, распространять кому-либо личный пароль;

3.7.11. Производить запись паролей на бумажные и иные неучтенные носители информации.

3.8. **Организация парольной защиты**

В соответствии с Матрицей доступа системный администратор:

3.8.1. Осуществляет ведение журнала выдачи паролей доступа к АРМ администрации МО «Романовское сельское поселение» (приложение 2 к настоящему Положению) и назначает для каждого пользователя администрации уникальные имя пользователя (логин) и пароль для авторизации в операционной системе АРМ. Хранение журнала должно осуществляться в закрытом металлическом сейфе;

3.8.2. В операционной системе АРМ создает учетную запись ответственного специалиста и, в соответствии с Матрицей доступа, задает параметры доступа к информационным ресурсам;

3.8.3. Проверяет на АРМ заданные возможности доступа для каждого ответственного специалиста.

3.8.4. Полная плановая смена паролей в ИС проводится не реже одного раза в 3 месяца.

3.8.5. **Правила ввода пароля**:

- ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;
- во время ввода пароля необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.8.6. **Правила хранение пароля**:

- запрещается записывать пароль на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям ИС личный пароль и регистрировать их в системе под своим паролем;
- лица, использующие паролирование, обязаны знать и выполнять требования настоящего Положения;
- своевременно сообщать администратору безопасности информации об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

3.9. **Требования по обеспечению безопасности с использованием СКЗИ**

3.9.1. СКЗИ, находящиеся в эксплуатации, должны подвергаться контрольным тематическим исследованиям, конкретные сроки, проведения которых определяются заказчиком СКЗИ по согласованию с разработчиком СКЗИ, специализированной организацией и Федеральной службой безопасности России.

3.9.2. СКЗИ и их опытные образцы подлежат поэкземплярному учету с использованием индексов или условных наименований и регистрационных номеров.

3.9.3. Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется: обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ; собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ.

3.9.4 Эксплуатация СКЗИ должна осуществляться в соответствии с документацией на СКЗИ и требованиями, установленными в настоящем Положении, а также в соответствии с иными нормативными правовыми актами, регулирующими отношения в соответствующей области.

3.9.5. Хранение криптографических ключей должно осуществляться в закрытых сейфах (металлических шкафах).

3.9.6. Размещение, специальное оборудование, охрана и организация режима на рабочих местах сотрудников использующих СКЗИ должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

3.10. **Обязанности пользователя ИС по обеспечению антивирусной защиты**

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

3.10.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности информации, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта при необходимости привлечь администратора безопасности информации).

3.10.3. В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку.

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

3.10.5. При необходимости пополнения базы ИС данными, полученными со стороны с помощью съемных носителей, контролировать отсутствие вирусного заражения информации на съемном носителе.

3.10.6. Периодически, не реже одного раза в неделю, проводить проверку антивирусом на наличие вирусного заражения.

3.10.7. Следить за тем, чтобы антивирус был все время включен, а также следить за своевременным обновлением антивирусных баз.

4. Соблюдение мер защиты информации без использования средств автоматизации

4.1. Основные требования по обеспечению информационной безопасности:

4.1.1. Шторы на оконных проемах должны быть завешаны (жалюзи

закрыты).

4.1.2. При отсутствии сотрудника на рабочем месте должны соблюдаться следующие условия:

- помещение, в котором находится рабочее место, следует плотно запирать на ключ;
- на рабочих местах не должно оставаться материальных носителей, содержащих информацию, в отношении которой установлено требование об обеспечении ее конфиденциальности.

4.1.3. Сотрудники ответственные за помещения, в которых размещается оборудование, предназначенное для обработки сведений конфиденциального характера, должны исключать возможность бесконтрольного проникновения в них посторонних лиц, а также обеспечивать сохранность оборудования, машиночитаемых носителей информации и документов.

4.1.4. Лица для проведения регламентных (наладочных), ремонтных и других работ в эти помещения во время обработки конфиденциальной сведений конфиденциального характера могут быть допущены только в экстренных случаях по согласованию с системным администратором, руководителями структурных подразделений администрации и в присутствии ответственного специалиста при условии исключения несанкционированного доступа к персональным данным и иной информации конфиденциального характера и контроля за порядком осуществления проводимых работ.

4.2. Организация обработки персональных данных и иной конфиденциальной информации, осуществляемой без использования средств автоматизации. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

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

4.2.2. Типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,

- при необходимости получения письменного согласия на обработку персональных данных.

4.2.3. Типовая форма должна быть составлена таким образом, чтобы каждый из

субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

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

5. **Порядок работы с носителями конфиденциальной информации**

5.1. Перед началом использования служебного носителя информации ответственный специалист заносит информацию о носителе в журнал учета съемных носителей информации (приложение 3 к настоящему Положению).

5.2. Учет носителей конфиденциальной информации осуществляется ответственными специалистами в журнале регистрации носителей информации, содержащих персональные данные и иную конфиденциальную информацию (приложение 4 к настоящему Положению).

5.3. Документы на бумажных носителях информации, содержащие персональные данные или иную конфиденциальную информацию, подлежат обязательному поэкземплярному учету. Учет осуществляется ответственными специалистами в журнале учета документов, имеющих конфиденциальный характер (приложение 5 к настоящему Положению).

5.4. Хранение персональных данных и иной конфиденциальной информации работников администрации осуществляется на съемном жестком диске, хранимом в сейфе, металлическом шкафу.

5.5. Передача носителей конфиденциальной информации должна сопровождаться соответствующими актами приема-передачи, в которых в обязательном порядке указывается регистрационный номер передаваемого носителя конфиденциальной информации.

5.6. Акты передачи носителей конфиденциальной информации составляются в двух экземплярах.

5.7. Для уничтожения конфиденциальной информации (носителей конфиденциальной информации) распоряжением администрации должна быть создана постоянно действующая комиссия по уничтожению персональных данных и иной конфиденциальной информации.

5.8. По факту уничтожения комиссией по уничтожению персональных данных и иной конфиденциальной информации составляется акт уничтожения персональных данных и иной конфиденциальной информации, находящейся на АРМ (приложение 6 к настоящему Положению).

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

6.1. Работа в сетях общего доступа и (или) международного обмена (сети «Интернет» и других) (далее – Сеть) на элементах ИС должна проводиться при служебной необходимости.

6.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и другие);
- передавать по Сети информацию, в отношении которой установлено требование об обеспечении ее конфиденциальности, без использования средств шифрования;
- скачивать из Сети программное обеспечение и другие файлы;
- посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение, и другие);
- нецелевое использование подключения к Сети.

7. **Порядок учета и хранения резервных копий баз данных программ, в которых осуществляется обработка персональных данных**

7.1. Работы по формированию резервных копий баз данных программ осуществляются системным администратором или ответственными специалистами.

7.2. Резервное копирование баз данных должно осуществляться только на предварительно учтенные в установленном порядке носители конфиденциальной информации.

7.3. Все факты резервного копирования баз данных на соответствующих АРМ должны фиксироваться системным администратором и/или ответственным специалистом в журнале учета резервных копий баз данных (приложение 7 к настоящему Положению).

8. **Порядок действий в случае выявления нарушений информационной безопасности**

8.1. выявление факта нарушения;

8.2. прекращение всех операций, связанных с участком, на котором произошло нарушение;

8.3. принятие экстренных мер для прекращения несанкционированного доступа или использования информации;

8.4. оповещение управляющего делами администрации, руководителей структурных подразделений и системного администратора о нарушении;

8.5. восстановление работоспособности информационной системы;

8.6. расследование причин нарушения информационной безопасности;

8.7. проверка состояния информационной безопасности по факту нарушения.

9. **Ответственность**

Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных, привлекаются к ответственности в соответствии с действующим законодательством.

Приложение 1
к Положению….

Таблица разграничения доступа к персональным данным и иной конфиденциальной информации, обрабатываемой в администрации МО «Романовское сельское поселение»

№ п / п	Подразделение	Ф.И.О. пользователя	Помещение (адрес здания, номер кабинета)	АРМ №	Имя АРМ в домене	IP адрес АРМ	Имя пользователя (логин)	Наименование информационной системы, программы	Категория доступа
1	2	3	4	5	6	7	8	9	10

Примечания:

1. Категории доступа к задачам (подзадачам) подразделяются на: – Администратор – все виды редактирования; – Оператор – только ввод и коррекция данных (запрет удаления);

2. Все пользователи допускаются к информации в объеме решаемых задач, а также к ИСП в режиме просмотра.

Составил:_____/_____/

«_____»_____20___г.

Приложение 2
к Положению ….

Журнал выдачи паролей доступа к АРМ администрации МО «Романовское сельское поселение»

№ п/п	АРМ №	Имя пользователя в операционной системе АРМ (логин)	Ф.И.О. ответственного специалиста	Должность / подразделение	Дата выдачи пароля	Пароль в операционной системе АРМ	Роспись ответственного специалиста в получении пароля	Роспись лица, производившего выдачу пароля
1	2	3	4	5	6	7	8	9

Приложение 3
к Положению ….

Журнал учета съемных носителей информации

№ п/п	Дата начала использования носителя информации	Ф.И.О. ответственного специалиста	Тип носителя информации	Номер носителя информации	Дата окончания использования носителя информации
1	2	3	4	5	6

Приложение 4

к Положению ….

Журнал регистрации носителей информации, содержащих персональные данные и иную конфиденциальную информацию

№ п / п	Дата поступления носителя	Регистрационный номер носителя	Содержание	Прием (поступление) носителя				Учетный номер носителя	Передача носителя		Дата и номер акта уничтожения	ФИО	
				Откуда поступил	Вид носителя	Количество листов	Дата и номер сопроводительного документа		Кому передан носитель	Дата и номер сопроводительного документа		передавшего	получившего
1	2	3	4	5	6	7	8	9	10	11	12	13	14

Примечания: 1. Данный журнал должен быть учтен;

2. Страницы пронумерованы, прошиты и опечатаны (опломбированы).

Приложение 5 к
Положению….

Журнал учета документов, имеющих конфиденциальный характер

№ п/п	Наименование документа	Регистрационный номер	Дата регистрации	Количество листов
1	2	3	4	5

Приложение 6
к Положению …..

АКТ
уничтожения персональных данных и иной конфиденциальной информации, находящейся на АРМ

«_____»_____20___г.

Председатель комиссии_____
(ФИО)
Член комиссии _____
(ФИО)
составили настоящий акт в том, что «_____»_____20 г. произведено уничтожение персональных данных или иной конфиденциальной информации, находящейся на:

_____
(указывается тип носителя информации)
регистрационный номер носителя информации:

_____
(указывается регистрационный номер носителя информации)
способ уничтожения информации:

_____
(указывается способ уничтожения информации)

Председатель комиссии _____
(подпись)
Член комиссии _____
(подпись)

Приложение 7
к Положению ….

Журнал учета резервных копий баз данных

№ п/п	Дата создания резервной копии	Название АРМ, путь к файлам	Тип резервной копии	Регистрационный Номер носителя конфиденциальной информации	Путь к файлам резервной копии	Ф.И.О. ответственного лица	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8	9

Приложение № 2

к постановлению
от_____2018 №___

СПИСОК
администраторов безопасности информационных систем
персональных данных в администрации МО «Романовское сельское поселение»

1.Заместитель главы администрациии.

2. Начальник финансового сектора, главный бухгалтер администрации.

Приложение № 3
к постановлению
от_____2018 №___

ИНСТРУКЦИЯ
администратора безопасности информационной системы
персональных данных в Администрации МО «Романовское сельское поселение»

1.Общие положения

1.1. Данная инструкция является руководящим документом администратора безопасности информационной системы персональных данных (далее – ИСПДн) администрации МО «Романовское сельское поселение».
1.2. Требования администратора безопасности ИСПДн администрации МО «Романовское сельское поселение» (далее Администратор), связанные с выполнением им своих функций, обязательны для исполнения всеми сотрудниками указанного отдела, допущенными к обработке персональных данных.
1.3. Работа с персональными данными (далее – ПДн) строится на следующих принципах:
- принцип персональной ответственности – в любой момент времени за каждый документ, содержащий ПДн (не зависимо от типа носителя: бумажный, электронный), должен отвечать конкретный работник
- принцип контроля и учета – все операции с документами, содержащими ПДн, должны отражаться в соответствующих журналах и карточках.

Обязанности администратора безопасности отдела администрации

2.1. В своей повседневной деятельности администратор руководствуется настоящей инструкцией и другими документами, регламентирующими защиту персональных данных от утечки по техническим каналам и несанкционированного доступа (далее – НСД), эксплуатационной документацией на установленные на объекте информатизации системы защиты информации от НСД и от утечки информации по техническим каналам.
2.2. Администратор безопасности:
- обеспечивает поддержку подсистем управления доступом, регистрации и учета информационных ресурсов;
- контролирует целостность программно-аппаратной среды, хранимой и обрабатываемой информации;
- контролирует доступность и конфиденциальность хранимой, обрабатываемой и передаваемой по каналам связи информации.
2.3. На администратора безопасности возлагаются следующие обязанности:
- следить за сохранностью наклеек с защитной и идентификационной информацией на корпусах персональных электронно-вычислительных машинах

(далее – ПЭВМ);
- знать уровень конфиденциальности обрабатываемой информации и класс ИСПДн, следить за тем, чтобы обработка информации производилась только с использованием учтенных съемных и несъемных носителей информации;
- контролировать соблюдение требований по учету и хранению носителей конфиденциальной информации и персональных данных;
- совместно с должностным лицом ответственным за организацию защиты ПДн обеспечивать доступ к защищаемой информации пользователям согласно их прав доступа;
- незамедлительно докладывать главе администрации обо всех выявленных попытках несанкционированного доступа к информации ограниченного доступа;
- контролировать правильность применения пользователями сети средств защиты информации;
- участвовать в испытаниях и проверках ИСПДн;
- не допускать к работе на ПЭВМ посторонних лиц;
- осуществлять контроль монтажа оборудования специалистами сторонних организаций;
- участвовать в приемке для нужд отдела новых программных средств;
- обобщать результаты своей деятельности и готовить предложения по ее совершенствованию;
- вести журнал учета работы с ИСПДн.
2.4. Регистрации в журнале учета работ ИСПДн подлежат:
- обновление программного обеспечения ИСПДн;
- обновление антивирусных баз;
- вскрытие системного блока с целью модернизации или ремонта с указанием цели вскрытия и проводимых работ;
- создание резервной копии базы данных и иной служебной информации;
- замена системного блока с указанием факта гарантированного удаления информации с жесткого магнитного диска;
- отклонения в нормальной работе системных и прикладных программных средств затрудняющих эксплуатацию ПЭВМ;
- выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.);
- перебои в системе электроснабжения.
2.5. При выявлении утечки информации администратор безопасности обязан немедленно прекратить работы в ИСПДн, подать служебную записку руководству и занести соответствующую запись в журнал учета работы ИСПДн с изложением факта нарушения, предпринятые и(или) рекомендуемые им действия.
2.6. Журнала регистрации работ ИСПДн хранится у администратора безопасности информационных систем персональных данных МУ «Администрации Гойтинского сельского поселения».

Ответственность

3.1. Администратор безопасности несет ответственность за качество и своевременность выполнения задач и функций, возложенных на него в соответствии с настоящей инструкцией и нормативными документами по защите информации.

Приложение № 4
к постановлению
от_____2018 №___

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Понятие информационной системы персональных данных.

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

2. Информационные системы персональных данных:

1) Программа «1С Зарплата и кадры бюджетного учреждения 8 (Расчет зарплаты)»;
2) Программа «1С: Бухгалтерия государственного учреждения 8»;
3) Федеральная информационная адресная система (ФИАС);
4) Государственная информационная система о государственных и муниципальных платежах (ГИС ГМП).