«Каляты»
сикт овмöдчöминса
администрация

Администрация
сельского поселения
«Приозёрный»

ТШÖКТÖМ

РАСПОРЯЖЕНИЕ

от 26 декабря 2014 года **№ 36 -р**

(Республика Коми, Корткеросский район, п. Приозёрный)

Об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

1. Ввести в Администрацию сельского поселения «Приозёрный» режим защиты персональных данных с 26 декабря 2015 года.
2. Утвердить Перечень персональных данных, обрабатываемых в Администрации сельского поселения «Приозёрный» (Приложение 1).
3. Утвердить Перечень защищаемых ресурсов Администрации сельского поселения «Приозёрный» (Приложение 2).
4. Утвердить Правила обработки персональных данных в Администрации сельского поселения «Приозёрный» (Приложение 3).
5. Утвердить Инструкцию ответственного за организацию обработки персональных данных (Приложение 4).
6. Утвердить Инструкцию по работе пользователей информационной системы персональных данных (Приложение 5).
7. Утвердить Инструкцию об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные информационной системы персональных данных (Приложение 6).
8. Утвердить Перечень должностей (функциональных обязанностей), для которых необходим доступ к ПДн (Приложение 7).
9. Утвердить Инструкцию о порядке доступа сотрудников Администрации сельского поселения «Приозёрный» в помещения, предназначенные для обработки персональных данных, а также о порядке сдачи ключей от этих помещений (Приложение 8).
10. Утвердить Правила рассмотрения запросов субъектов персональных данных или их представителей (Приложение 9).
11. Утвердить Перечень информационных систем персональных данных Администрации сельского поселения «Приозёрный» (Приложение 10).

12. Утвердить Правила работы с обезличенными персональными данными в Администрации сельского поселения «Приозёрный» (Приложение 11).

13. Утвердить Перечень должностей Администрации сельского поселения «Приозёрный», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных (Приложение 12).

14. Утвердить списком лиц, имеющих право самостоятельного доступа в помещения, предназначенные для обработки персональных данных Администрации сельского поселения «Приозёрный» (Приложение 13).

15. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение 14).

16. Утвердить Порядок осуществления внутреннего контроля соответствия персональных данных установленным требованиям (Приложение 15).

17. Лица, допущенные к обработке персональных данных, несут персональную ответственность за обработку и хранение персональных данных.

18. Опубликовать и обеспечить возможность доступа к Политике обработки персональных данных в Администрации сельского поселения «Приозёрный» с использованием сети интернет на официальном сайте Администрации муниципального района «Корткеросский».

19. С настоящим распоряжением и его приложениями ознакомить всех сотрудников (под подпись) в части, их касающейся.

20. Контроль за исполнением распоряжения оставляю за Главой сельского поселения «Приозёрный».

И. о. руководителя администрации
сельского поселения «Приозёрный» О. А. Каракчиева

Приложение 1
к распоряжению администрации СП
«Приозёрный »
от 26.12.2014 г. № 36-р

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в Администрации сельского поселения «Приозёрный»

Настоящий Перечень разработан на основании и в соответствии с:

- Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановлением Правительства 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»;
- другими нормативными правовыми документами по вопросам обработки персональных данных и защиты информационных ресурсов.

Настоящий Перечень предназначен для работников Администрации сельского поселения «Приозёрный», выполнение должностных обязанностей которых связано с обработкой персональных данных.

Сведения, указанные в перечне, могут быть представлены органам государственной власти в объемах и пределах их компетенции в соответствии с законодательством Российской Федерации.

Таблица 1. Перечень персональных данных

№	Содержание
–	**Персональные данные**
○	**Персональные данные работников**
–	**Первичные учетные данные работника**
●	фамилия, имя, отчество;
●	пол.
–	**Сведения о занимаемой должности работника**
●	наименование организации работодателя;
●	наименование структурного подразделения;

•	наименование занимаемой должности;
•	рабочая контактная информация (адрес рабочего места, номер рабочего телефона, адрес рабочей электронной почты и т.п.).
–	**Сведения о реквизитах работника (дополнительные сведения)**
•	данные документа удостоверяющего личность (серия, номер паспорта, кем и когда выдан);
•	дата и место рождения;
•	адрес регистрации и адрес фактического проживания;
•	индивидуальный номер налогоплательщика;
•	номер страхового свидетельства (СНИЛС);
•	реквизиты полиса медицинского страхования;
•	сведения о медицинском заключении по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождение;
•	сведения о пребывании за границей;
•	сведения о наличии или отсутствии судимости;
•	домашний телефон;
•	сотовый телефон;
–	**Трудовая деятельность**
•	сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи);
•	специальность по диплому;
•	квалификация по диплому;
•	форма профессионального послевузовского образования;
•	данные об аттестации работника;
•	данные о профессиональной переподготовке или повышении квалификации;
•	сведения об учёной степени;
•	сведения о государственных наградах, знаках отличия;
•	сведения о трудовой деятельности (стаж, места работы/должности/периоды работы/причины увольнения,

	сведения о трудовой книжке (№/серия/дата выдачи/записи в ней), сведения о командировках/отпусках, поощрениях, данные о трудовом договоре (№/дата/условия/гарантии));
•	сведения о проведении служебных проверок, дисциплинированных расследований;
•	информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;
•	номер расчетного счета, номер банковской карты;
•	информация об оформленных допусках к государственной тайне;
•	личная фотография;
•	табельный номер;
•	сведения о периодах нетрудоспособности;
•	данные о суммах удержаний и перечислений заработной платы согласно заявлению или исполнительному листу.
–	**Социальное положение работника**
•	сведения о доходах, об имуществе и обязательствах имущественного характера, в т.ч. членов семьи, а также о расходах;
•	тип и сумма налогового вычета;
•	номер полиса медицинского страхования;
•	сведения об инвалидности, временной нетрудоспособности и прохождения диспансеризации;
•	сведения о составе семьи и сведения о близких родственниках;
•	реквизиты свидетельств о государственной регистрации актов гражданского состояния;
•	сведения о семейном положении;
•	сведения о воинском учете и реквизиты документов воинского учёта;
•	сведения о социальных льготах;
•	информация о владении иностранными языками (степень владения);
•	сведения о гражданстве.
○	**Граждане РФ**
–	фамилия, имя, отчество;
–	пол;

–	данные документа удостоверяющего личность (серия, номер документа, кем и когда выдан);
–	дата и место рождения;
–	адрес регистрации и адрес фактического проживания;
–	рабочая контактная информация (номер рабочего телефона, адрес рабочей электронной почты и т.п.);
–	номер страхового свидетельства (СНИЛС);
–	индивидуальный номер налогоплательщика;
–	семейное положение;
–	данные о составе семьи;
–	данные о воинском учете;
–	**Сведения об образовании**
–	наименование образовательного учреждения;
–	сведения о документах, подтверждающих образование (наименование, № документа, дата выдачи);
–	специальность по диплому, квалификация по диплому;
–	**Сведения о трудовой деятельности**
–	общий трудовой стаж;
–	сведения о местах работы (занимаемые должности, периоды работы, причины увольнения);
–	сведения о трудовой книжке (№, серия, дата выдачи, записи в ней);
–	сведения о занимаемой должности, структурном подразделении, данные о трудовом договоре (№, дата, условия, гарантии);
–	сведения о периодах нетрудоспособности.

Персональные данные могут считаться общедоступными, если таковыми их сделал (дал согласие) субъект персональных данных или в других случаях, установленных федеральным законодательством Российской Федерации.

Приложение 2
к распоряжению администрации СП
«Приозёрный »
от 26.12.2014 г. № 36-р

ПЕРЕЧЕНЬ
защищаемых ресурсов Администрации сельского поселения «Приозёрный»

Таблица 1. Перечень защищаемых ресурсов

№	Наименование информационного ресурса	Расположение (кабинет)	Наличие информационных систем	Расположение ИС	Инвентарный номер/ HWID/IP-адрес	Ответственный за АРМ
1.	**АРМ предприятие**	Кабинет № 2	Статистика	Республика Коми, п. Приозёрный ул. Станционная, д. 3		Каракчиева Ирина Ивановна; Каракчиева Ольга Александровна; Мингалева Светлана Евлогиевна
2.	**АС «Смета»**	Кабинет № 3	АС «Смета»	Республика Коми, п. Приозёрный ул. Станционная, д. 3		Мингалева Светлана Евлогиевна

Приложение 3
к распоряжению администрации СП
«Приозёрный»
от 26.12.2014 г. № 36-р

ПРАВИЛА
обработки персональных данных
в Администрации сельского поселения «Приозёрный»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила разработаны с целью защиты информации, относящейся к личности и личной жизни работников Администрации сельского поселения «Приозёрный», граждан, обратившихся за предоставлением муниципальной услуги, а также при осуществлении муниципальных функций (далее – Граждане), в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и Федеральным законом от 27.07. 2006 г. № 152-ФЗ «О персональных данных».

1.2. Основанием для разработки настоящих Правил является Конституция Российской Федерации, Федеральный закон «О персональных данных» №152-ФЗ от 27.07.2006 г. и другие действующие нормативно-правовые акты Российской Федерации по обеспечению защиты персональных данных.

1.3. Настоящие Правила и изменения к ним утверждаются главой сельского поселения, вступают в силу с момента утверждения и действуют бессрочно, до замены новыми Правилами. Все изменения в Правила вносятся распоряжением. Все сотрудники, допущенные к обработке персональных данных должны быть ознакомлены под подпись с данными Правилами и изменениям к ним.

1.4. В настоящих Правилах используются следующие термины и определения:

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

персональные данные сотрудника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника;

персональные данные граждан – информация, необходимая работникам администрации в связи с предоставлением муниципальной услуги и (или) осуществлением муниципальной функции;

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

II. ОСНОВНЫЕ УСЛОВИЯ ПРОВЕДЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных осуществляется исключительно в целях обеспечения соблюдения законодательных и иных нормативных правовых актов, а также обеспечения личной безопасности, сохранности имущества, контроля количества и качества выполняемой работы.

2.2. Все персональные данные предоставляются гражданином. Если персональные данные гражданина возможно получить только у третьей стороны, то администрация обязана заранее уведомить об этом гражданина и получить его письменное согласие. Администрация должна сообщить гражданину о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа граждан дать письменное согласие на их получение.

2.3. Администрация не имеет права получать и обрабатывать персональные данные граждан о его политических, религиозных и иных убеждениях и частной жизни.

2.4. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, работодатель вправе получать и обрабатывать данные о частной жизни сотрудника только с его письменного согласия.

2.5. Администрация не имеет права получать и обрабатывать персональные данные граждан о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

2.6. При принятии решений, затрагивающих интересы граждан, администрация не имеет права основываться на персональных данных гражданина, полученных исключительно в результате их автоматизированной обработки или электронного получения.

III. СБОР, ОБРАБОТКА, ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Администрация определяет объем, содержание обрабатываемых персональных данных граждан, руководствуясь Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

3.2. Осуществляемая обработка персональных данных в ИСПДн предусматривает использование средств вычислительной техники.

3.3. Все персональные данные предоставляются гражданином с его письменного согласия (Приложение 1 к Правилам обработки персональных данных). Администрация обязана сообщить гражданину о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа гражданина дать письменное согласие на их получение (Приложение 2 к Правилам обработки персональных данных).

3.4. Гражданин представляет работодателю достоверные сведения о себе. Администрация проверяет достоверность сведений, сверяя данные, представленные гражданином, с имеющимися у сотрудника администрации документами.

Представление сотрудником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

Представление гражданином подложных документов или ложных сведений при подаче заявления на предоставление муниципальной услуги и (или) для осуществления муниципальной функции является основанием для отказа в предоставлении муниципальной услуги и (или) муниципальной функции.

3.5. Персональные данные хранятся в металлических хранилищах на бумажных и электронных носителях, в специально предназначенных для этого помещениях.

3.6. В процессе хранения персональных данных должны обеспечиваться:

– требования нормативных документов, устанавливающих правила хранения персональных данных;

– сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящими Правилами;

– контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

3.7. Ответственный за организацию обработки персональных данных Администрации осуществляет контроль за хранением и обработкой персональных данных в информационных системах персональных данных в соответствии с требованиями законодательства.

3.8. Сотрудники Администрации имеют право получать только те персональные данные граждан, которые необходимы им для выполнения своих должностных обязанностей.

3.9. Персональные данные подлежат уничтожению в течение 30 дней, по достижении целей обработки или в случае утраты необходимости в их достижении, если иное не установлено действующим законодательством.

3.10. Решение об уничтожении принимается руководителем Администрации на основании ходатайства ответственного за обеспечение безопасности персональных данных.

3.11. Уничтожение бумажных носителей должно осуществляться сотрудниками Администрации, допущенными к обработке персональных данных путем, не допускающим дальнейшую возможность ознакомления с данными документами (через измельчитель бумаги или путем сожжения). Уничтожение информации на автоматизированных рабочих местах должно осуществляется комиссией способами, не позволяющими осуществить восстановление данных.

3.12. При уничтожении персональных данных составляется, в обязательном порядке, акт с указанием, какие именно документы и файлы были уничтожены (Приложение 2 к Правилам обработки персональных данных).

IV. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

4. 1. При передаче персональных данных гражданами другим юридическим и физическим лицам Администрация должна соблюдать следующие требования:

– не сообщать персональные данные третьей стороне без письменного согласия граждан, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в иных случаях, установленных федеральными законами.

– не сообщать персональные данные в коммерческих целях без их письменного согласия.

4.2. Предупреждать лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные граждан, обязаны соблюдать конфиденциальность этих персональных данных. Данные Правила не распространяются на обмен персональными данными граждан в порядке, установленном федеральными законами.

4.3. Не запрашивать информацию о состоянии здоровья сотрудников, за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовых обязанностей.

4.4. Передавать персональные данные граждан представителям Администрации в порядке, установленном Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

V. ПРАВА ГРАЖДАН В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В целях обеспечения защиты персональных данных, хранящихся в Администрации, граждане имеют право:

5.2. Получения полной информации о своих персональных данных и их обработке.

5.3. Свободного бесплатного доступа к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих персональных данных возможно при личном обращении гражданина.

5.4. Определения своих представителей для защиты своих персональных данных.

5.5. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и иных нормативных правовых актов. Указанное требование должно быть оформлено письменным заявлением гражданина на имя руководителя Администрации. При отказе Администрации исключить или исправить персональные данные гражданина, он имеет право заявить в письменной форме о своем несогласии, с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера гражданин имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.6. Требовать об извещении Администрацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные гражданина, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.7. Обжаловать в суде любые неправомерные действия (бездействие) работодателя при обработке и защите его персональных данных.

VI. ОБЯЗАННОСТИ ГРАЖДАН В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ДОСТОВЕРНОСТИ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. В целях обеспечения достоверности персональных данных гражданин обязаны:

– предоставлять Администрации, в должностные обязанности которых входит работа с документами, содержащими персональные данные граждан, достоверные сведения о себе в порядке и объеме, предусмотренном нормативными правовыми актами.

– сообщать в Администрацию в случае изменения своих персональных данных в течение 5 рабочих дней с даты их изменения.

VII. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

7. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, установленных действующим законодательством Российской Федерации и настоящими Правилами, несут ответственность, предусмотренную законодательством Российской Федерации.

Приложение 1
к Правилам обработки
персональных данных

СОГЛАСИЕ
на обработку персональных данных муниципального служащего администрации, лиц, замещающих в администрации должности, не являющиеся должностями муниципальной службы, технического персонала администрации

Я, _____
(Фамилия, Имя, Отчество)
зарегистрированный по адресу: _____
_____
(адрес по месту регистрации)
паспорт серии _____ номер _____ выдан "___" _____ _____ г.
(дата выдачи)
_____
(наименование органа выдавшего документ)

Мне известно, что обработка моих персональных данных в администрации сельского поселения «Приозёрный» (далее - администрация) осуществляется в соответствии с требованиями Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, Республики Коми, локальных актов администрации в сфере обработки и защиты персональных данных в целях оказания содействия в исполнении моих должностных обязанностей, содействия в обучении и должностном росте, в целях обеспечения моей личной безопасности и членов моей семьи, а также в целях обеспечения сохранности принадлежащего мне имущества и имущества государственного органа, учета результатов исполнения моих должностных обязанностей.

Кроме того, мне известно, что обработка моих персональных данных осуществляется в целях исполнения администрацией предусмотренных законодательством обязательств, связанных с возникновением между администрацией и мной трудовых отношений.

Подтверждаю, что мои персональные данные могут для указанных выше целей в порядке и в случаях, установленных действующим законодательством, обрабатываться администрацией смешанным способом (с использованием средств автоматизации и (или) без такового) путем их сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения.

Подтверждаю, что в создаваемые администрацией общедоступные источники персональных данных (в том числе справочники, адресные книги) могут включаться мои фамилия, имя, отчество.

Настоящее письменное согласие действует в течение срока работы мною в администрации.

Настоящее письменное согласие может быть отозвано мною в порядке и по основаниям, предусмотренным законодательством.

При этом, я не возражаю против действий администрации по обработке персональных данных, совершенных в целях, указанных в настоящем письменном согласии, до представления мною настоящего письменного согласия.

"__" _____ 20__ г. _____ _____
(подпись) (расшифровка подписи)

Приложение 2
к Правилам обработки персональных данных

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

Уважаемый(-ая), *(инициалы субъекта персональных данных)*!

В соответствии с требованиями статьи 18 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» уведомляем Вас, что в целях:

_____
_____
_____

(указать цели, для которых необходима обработка персональных данных)

оператору необходимо получить от Вас следующие персональные данные:

_____
_____
_____

(указать, какие именно персональные данные или документы, их содержащие, должны быть представлены)

Обязанность предоставления Вами указанных персональных данных установлена:

_____
_____

(реквизиты и наименование нормативных правовых актов)

В случае Вашего отказа предоставить свои персональные данные, оператор не сможет на законных основаниях осуществлять их обработку, что приведет к следующим для Вас юридическим последствиям:

_____
_____

(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных, либо имущественных прав граждан или случаи, иным образом затрагивающие его права, свободы и законные интересы)

_____

(дата) (фамилия, инициалы и подпись сотрудника оператора)

Приложение 2
к Правилам обработки персональных
данных в Администрации

АКТ (форма) № _____
уничтожении персональных данных

п. Приозёрный «___» _____ 20___ г
.

Комиссия в составе:
председателя: _____
члены комиссии: _____
_____
_____

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации данные, записанные на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего съемных носителей _____
(цифрами и прописью)
На указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)
Перечисленные носители ПДн уничтожены путем
_____.
(разрезания, сжигания, механического уничтожения и т.п.)
Председатель комиссии: _____ _____

Члены комиссии: _____ _____

_____ _____

_____ _____

Приложение 4
к распоряжению администрации сельского
поселения « Приозёрный»
от 26.12.2014 г. № 36-р

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в Администрации сельского поселения «Приозёрный»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Лицо, ответственное за организацию обработки персональных данных (далее – Ответственный), назначается и освобождается распоряжением руководителя Учреждения.

1.2. Ответственный подчиняется главе сельского поселения «Приозёрный» (далее – Администрация) или в его отсутствии лицу, исполняющему обязанности руководителя Администрации. Методическую помощь Ответственному по вопросам защиты персональных данных оказывает ГБУ Республики Коми «ЦБИ».

1.3. В своей деятельности Ответственный руководствуется:

- действующим законодательством Российской Федерации;
- уставом сельского полселения «Приозёрный»;
- документами, регламентирующими обработку персональных данных в Администрации;
- настоящей Инструкцией;
- рекомендациями ГБУ Республики Коми «ЦБИ».

II. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

2.1. Проведение инструктажа и консультации пользователей по соблюдению установленного режима защиты персональных данных.

2.2. Взаимодействие с ГБУ Республики Коми «ЦБИ» на основании Соглашения о взаимодействии в сфере обеспечения информационной безопасности по вопросам обеспечения защиты персональных данных.

2.3. Выполнение, учет и контроль изменений, вносимых:

- в списки лиц, допущенных к обработке персональных данных;
- в перечень защищаемых ресурсов Администрации;
- в списки лиц, имеющих право самостоятельного доступа в помещения, предназначенные для обработки персональных данных.

2.4. Организация и проведение периодического и внеочередного контроля работы пользователей.

2.5. Контроль выполнения пользователями установленного режима защиты персональных данных, в том числе, соблюдения данного режима при обращении с персональными идентификаторами, личными ключевыми дискетами и карточками паролей, со съемными машинными носителями

информации, в процессе создания машинных документов, при процедурах «лечения» зараженных файлов.

2.6. Участие в процедурах контроля операций по безопасному удалению личных файлов пользователя при прекращении полномочий учетной записи, по уничтожению (в установленном порядке) старых карточек паролей (при замене АБ паролей пользователям) и созданию новых карточек паролей.

2.7. Организация и участие в служебных расследованиях для выяснения причин утечки или воздействия на обрабатываемую в ИСПДн информацию, компрометации паролей с целью выяснения величины нанесенного ущерба безопасности информации и выработки новых или совершенствования принятых технических и организационных мер по защите информации от реализации угрозы в будущем.

2.8. При возникновении необходимости, организация и участие в мероприятиях, связанных с событиями вскрытия, опечатывания, модификации состава, ремонта и т.д. технических средств ИСПДн. Опечатывание корпусов технических средств ИСПДн. Составление актов о вскрытии и опечатывании корпусов технических средств.

2.9. Проведение анализа воздействия изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение безопасности персональных данных.

2.10. Проведение процедур обезличивания персональных данных в информационных системах персональных данных.

2.11. Документальное оформление изменений в конфигурации информационной системы и системы защиты персональных данных.

2.12. Анализ инцидентов, в том числе, определение источников и причин возникновения инцидентов, а так же оценка их последствий, принятие мер по устранению последствий инцидентов.

2.13. Планирование и принятие мер по предотвращению повторного возникновения инцидентов.

2.14. Обеспечение соответствия проводимых работ технике безопасности, правилам и нормам охраны труда.

2.15. Контроль за установкой программного обеспечения, запрет установки неразрешённого программного обеспечения (в том числе средств обработки и отладки);

2.16. Контроль установки обновлений программного обеспечения;

2.17. Выполнение резервного копирования машинных документов, содержащих персональные данные;

2.18. Контроль безотказного функционирования технических средств, принятие мер по восстановлению отказавших средств.

III. ПРАВА

Ответственный имеет право:

3.1. Требовать от пользователей выполнения следующих локальных документов:

- «Инструкцию пользователя по работе с персональными данными»;

- «Инструкцию об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные информационной системы персональных данных», в части их касающейся»;
- Правила обработки персональных данных в Администрации;
- Порядок доступа сотрудников Администрации в помещения, предназначенные для обработки персональных данных.

3.2. Участвовать в разработке мероприятий по совершенствованию системы защиты информации в ИСПДн.

3.3. Вносить изменения в конфигурацию информационной системы и системы защиты персональных данных.

3.4. Обращаться к руководителю Администрации с мотивированным предложением по приостановке процесса обработки информации в ИСПДн или отстранению от работы пользователя ИСПДн в случаях систематического нарушения режима защиты персональных данных, технологии обработки информации в ИСПДн.

3.5. Требовать от пользователей своевременного информирования о возникновении инцидентов в информационной системе.

IV. ОТВЕТСТВЕННОСТЬ

4.1 Ответственность за неисполнение и/или ненадлежащее исполнение обязанностей, предусмотренных настоящей Инструкцией, возлагается на Ответственного в соответствии с действующим законодательством Российской Федерации и условиями трудового договора.

Приложение 5
к распоряжению администрации сельского
поселения «Приозёрный»
от 26.12.2014 г. № 36-р

ИНСТРУКЦИЯ
пользователя по работе с персональными данными

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет общие правила работы сотрудников Администрации сельского поселения «Приозёрный» с персональными данными.

1.2. Персональные данные в электронном виде обрабатывается в информационных системах персональных данных. Также устанавливается особый порядок обработки и хранения персональных данных, содержащихся на бумажных носителях.

1.3. Пользователем является каждый сотрудник Администрации, участвующий в рамках своих функциональных обязанностей в процессах, как автоматизированной обработки, так и обработки без использования средств автоматизации персональных данных, а также имеющий доступ к аппаратным средствам, программному обеспечению, носителям информации и средствам защиты.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, Правилами обработки персональных данных, руководящими и нормативными документами ФСТЭК России и ФСБ России и другими документами Администрации, регламентирующими обработку персональных данных.

1.5. Методическое руководство по работе Пользователя осуществляет ответственный за организацию обработки персональных данных.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

2.3. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.4. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.5. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.6. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.7. Автоматизированное рабочее место (АРМ) – программно-технический комплекс, посредством которого Пользователь выполняет свои должностные обязанности (персональный компьютер, ноутбук, терминал и т.п.).

2.8. Несанкционированный доступ (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

2.9. Посторонние лица – лица, которые не имеют права самостоятельного доступа в помещение и (или) не имеют права самостоятельного доступа в ИСПДн и (или) не имеют допуска к персональным данным.

2.10. Средство защиты информации от несанкционированного доступа (СЗИ от НСД) – программное, техническое или программно-техническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа к информации.

III. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

3.1. Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей.

3.2. Не сообщать устно или письменно, не передавать в каком либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения руководителя Администрации.

3.3. Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов, регламентирующих порядок обработки персональных данных.

3.4. Выполнять на АРМ только те процедуры обработки персональных данных, которые определены должностной инструкцией.

3.5. Знать и соблюдать установленные требования обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

3.6. Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных.

3.7. Незамедлительно, в кратчайшие сроки, сообщать руководителю Администрации об утрате или недостаче носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов и о других фактах, которые могут привести к разглашению персональных данных.

3.8. При прекращении работ (трудовых отношений) все материальные носители, содержащие персональные данные (флеш-накопители, дискеты, оптические диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, модели, промышленные образцы и пр.), передать руководителю Администрации.

3.9. Соблюдать требования парольной политики (раздел 4).

3.10. Соблюдать требования антивирусной защиты (раздел 5).

3.11. Пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена (раздел 6).

3.12. Пользователи, работающие с электронной подписью или использующие шифрование, обязаны соблюдать Инструкцию по обращению со средствами криптографической защиты информации.

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

3.14. Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, а так же для получений консультаций по вопросам обработки персональных данных, необходимо обращаться к ответственному за организацию обработки персональных данных.

Пользователям запрещается:

3.14.1. Нарушать установленные в Администрации инструкции по работе с персональных данных.

3.14.2. Использовать компоненты программного и аппаратного обеспечения Администрации в неслужебных целях.

3.14.3. Оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы Windows – комбинацией клавиш [WIN] + [L] или [CTRL] + [ALT] + [DEL] с дальнейшим нажатием кнопки «Блокировка» появившегося меню, либо при помощи штатных средств защиты информации от несанкционированного доступа при их наличии).

3.14.4. Оставлять без присмотра или неубранными в хранилища (шкаф, сейф) носители или документы, содержащие персональные данные.

3.14.5. Записывать и хранить персональные данные на неучтенных носителях информации (оптических дисках, гибких магнитных дисках, флеш-накопителях и т.п.).

3.14.6. Самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.

3.14.7. Самовольно подключать АРМ или другие средства к ЛВС Администрации, изменять IP-адрес, MAC-адрес и иные настройки сети АРМ.

3.14.8. Производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, равно как и любым другим узлам ЛВС Администрации или Интернет, в том числе:

– действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);

– установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;

– действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;

– уничтожение, модификация программного обеспечения или данных без согласования с руководителем Администрации или владельцами этого ресурса;

– попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;

– умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам (как внутри Администрации так и вне), либо на нарушение целостности и работоспособности этих систем;

– действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

3.14.9. Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.

3.14.10. Самостоятельно разрабатывать или использовать нерегламентированные (без разрешения руководителя Администрации, не относящиеся к производственному процессу) программы (например: игры; IM-клиенты, такие как Google Messenger, ICQ и т.п.; P2P-клиенты: Kazaa, eMule и т.п.).

3.14.11. Разрешать посторонним лицам работать под своей учетной записью в ИСПДн.

3.14.12. Пересылать персональные данные по каналам связи в открытом виде, в том числе Интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования).

3.14.13. Получать доступ к персональным данным с рабочих мест, не оборудованными необходимыми средствами защиты информации.

3.14.14. Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

3.14.15. В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

3.14.16. Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

3.14.17. Удалять или искажать программы и файлы с персональными данными и иной важной информацией (например, системной, необходимой для функционирования ИСПДн).

3.14.18. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению внештатной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения и сотрудников, ответственных за установку и (или) сопровождение программного обеспечения (Администратора безопасности персональных данных в информационных системах персональных данных (далее - администратор безопасности)).

3.14.19. Подключать к ЛВС Администрации личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а так же личные носители и накопители информации. В случае необходимости переноса информации с личных носителей информации обращаться к ответственным.

IV. ПАРОЛЬНАЯ ПОЛИТИКА

4.1. Общие требования к паролям:

– Минимальное требование: буквенно-цифровой пароль. Желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы (например: ~ ! @ # $ % ^ & * ( ) _ - + = | \ ? / . , : ; ’] [{ } < > . и т.п.).

– Минимальная длина пароля: не менее 6 (шести) символов.

– Максимальный срок действия пароля: 90 суток.

– Запрет использования трех ранее использовавшихся паролей.

– Пароль Пользователя не должен включать в себя легко вычисляемые сочетания символов, общепринятые сокращения, имена, фамилии, должности, год рождения, номер паспорта, табельный номер, иную информацию о Пользователе, доступную другим лицам.

– Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

– Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например: 1234567, qwerty и т.п.).

4.2. Правила использования паролей:

– Хранить в тайне свой пароль, не сообщать его другим лицам.

– Не предоставлять доступ в ИСПДн другим лицам под своей учетной записью и паролем.

– Изменять свой пароль при первом требовании политики паролей операционной системы и/или ИСПДн.

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

– Запрещается записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе АРМ, на обратной стороне клавиатуры и т.д.

– Запрещается хранить пароли в записанном виде на отдельных листах бумаги.

4.3. Смена, удаление личного пароля любого Пользователя производится в следующих случаях:

– в случае подозрения на компрометацию пароля;

– по окончании срока действия;

– в случае прекращения полномочий (увольнение, переход на другую работу внутри Администрации) Пользователя после окончания последнего сеанса работы в информационных системах персональных данных;

– по указанию ответственного за организацию обработки персональных данных.

4.4. При увольнении, переходе на новую должность сотрудника, имеющего доступ помимо своей учетной записи к другим ресурсам (межсетевые экраны, маршрутизаторы, серверы, другие учетные записи и т.п.) также производится внеплановая смена паролей к таким ресурсам.

V. ПРИМЕНЕНИЕ ЛИЧНЫХ ИДЕНТИФИКАТОРОВ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5. Привязку идентификатора к пользователю (учетной записи) выполняет администратор безопасности.

5.1. Пользователи ИСПДн получают свой идентификатор у администратора безопасности.

5.2. Пользователь ИСПДн обязан хранить свой личный идентификатор в недоступных для других сотрудников хранилищах.

5.3. Пользователю ИСПДн запрещается передавать свой личный идентификатор.

5.4. В случае утери личного идентификатора, пользователь ИСПДн должен немедленно доложить об этом администратору безопасности информации.

5.5. В случае прекращения полномочий учетной записи пользователя ИСПДн (увольнение, переход на другую работу, в другой отдел или помещение, а также другие обстоятельства) учетная запись должна быть удалена, а её идентификатор должен быть сдан администратору безопасности информации после окончания последнего сеанса работы данного пользователя в ИСПДн.

5.6. В случае компрометации или утери личного идентификатора пользователя администратором безопасности должны быть немедленно предприняты меры в соответствии с п. 5.7 настоящей Инструкции.

5.7. Администратор безопасности информации должен провести служебное расследование для выяснения причин компрометации идентификатора с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а

также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.

VI. АНТИВИРУСНАЯ ЗАЩИТА

6.1. В случае отсутствия штатных функций антивирусной программы, предусматривающих автоматическую проверку файлов, Пользователь обязан осуществлять проверку файлов получаемых:

- по электронной почте;
- через сеть Интернет;
- на магнитном, оптическом диске, флеш–накопителе;
- ином съемном носителе информации;
- полученные иным способом.

6.2. Перед открытием вложения (ссылок) убедиться в том, что отправитель действительно послал вам этот файл, даже если он и должен был это сделать. Позвоните ему сами. Не доверяйте имени отправителя и указанным в тексте письма номерам телефонов, а также лицам, позвонившим вам самостоятельно с просьбой открыть файлы и пройти по ссылкам.

6.3. Пользователю запрещается:

6.3.1. Осуществлять действия, направленные на выключение антивирусной программы.

6.3.2. Самостоятельно устанавливать на АРМ программное обеспечение.

6.3.3. Запускать файлы, полученные по сетям связи (электронной почте, Интернет), со съемных носителей, даже если они получены проверенного адресата, без предварительной их проверки антивирусной программой.

6.3.4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Пользователь самостоятельно или вместе с ответственным (Администратором безопасности) должен провести внеочередной антивирусный контроль своего рабочего места.

6.3.5. В случае обнаружения при проведении антивирусной проверки вирусного заражения Пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вирусного заражения ответственному (Администратору безопасности);
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

VII. ПОРЯДОК РАБОТЫ В ИСПДН И СЕТИ ИНТЕРНЕТ

7.1. Подключение к ИСПДн и сети Интернет

7.2. Целью работы Пользователя в ИСПДн и сети Интернет является сбор, обработка, хранение персональных данных, обмен электронными сообщениями в служебных целях.

7.2.1. Доступ к ИСПДн и сети Интернет предоставляется Пользователям только в том случае, если это не противоречит требованиям настоящей Инструкции и иными нормативными документами в области защиты информации.

7.2.2. Доступ пользователя к ИСПДн для обработки персональных данных производится только с рабочих мест, на которых установлены средства защиты информации.

7.2.3. Основанием для подключения сотрудника Администрации к ИСПДн и сети Интернет является мотивированная заявка ответственному за организацию обработки персональных данных от непосредственного руководителя Пользователя с указанием полномочий доступа к таким ресурсам и сервисам.

7.2.4. Ответственный за организацию обработки персональных данных, либо сотрудник, выполняющий его функции, организует подключение к ИСПДн или сети Интернет Пользователей в установленном порядке, осуществляет контроль над использованием данных ресурсов и сервисов.

7.2.5. После выполнения задания Ответственный за организацию обработки персональных данных сообщает пользователю выполнении заявки.

7.2.6. Основанием для отключения пользователя от ИСПДн и сети Интернет являются следующие события:

– нарушение инструкций и иных локальных нормативных актов в области защиты информации Администрации;

– увольнение Пользователя, либо перевод его в другое подразделение.

7.3. Порядок работы в сети Интернет

7.3.1. Использование сотрудниками Администрации сети Интернет должно осуществляться исключительно для выполнения должностных обязанностей.

7.3.2. Информация, образованная (образующаяся) в процессе трудовой деятельности работника Администрации является собственностью Администрации и не подлежит использованию (в том числе использованию в сети Интернет или с помощью сети Интернет) в личных целях и (или) в корыстных интересах других лиц (организаций).

7.3.3. При проведении технических работ, связанных с настройкой оборудования (коммуникационное оборудование, прокси-сервера, маршрутизаторы и т.п.); в случае обнаружения попыток несанкционированного доступа к Интернет-шлюзу, АРМ Пользователей может проводиться временное отключение Пользователей от сервисов сети Интернет (в случае планового отключения Пользователи уведомляются об этом заблаговременно).

7.3.4. Вся информация о ресурсах, посещаемых сотрудниками Администрации, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а так же руководству Администрации для детального изучения и принятия решения о мерах дисциплинарной ответственности.

7.3.5. При работе в сети Интернет Пользователям запрещается:

– умышленное распространение и получение материалов в/из сети Интернет, противоречащих законодательству Российской Федерации, в том числе материалов, пропагандирующих насилие или экстремизм; разжигающих расовую, национальную или религиозную вражду; разъясняющих порядок изготовления и/или применения наркотиков, взрывчатых веществ, оружия и т. п.; материалов порнографического характера; компьютерных вирусов и других вредоносных программ;

– передавать в сеть Интернет информацию, к которой в соответствии с законодательством ограничен доступ (персональные данные, служебная информация) без соответствующего разрешения;

– фальсифицировать IP-адрес, MAC-адрес, иные адреса, используемые в сетевых протоколах, а также прочую информацию при передаче данных через сеть Интернет.

– предоставлять доступ в сеть Интернет со своей рабочей станции кому-либо, в том числе программно-техническими способами через локальную вычислительную сеть Администрации (например: путем несанкционированной установки локального Интернет-шлюза на рабочее место);

– получать доступ к сети Интернет любыми способами, не предусмотренными действующими локальными документами (Инструкциями, Правилами, Регламентами Администрации);

– осуществлять несанкционированный доступ к ресурсам и сервисам сети Интернет.

1.1. выполнять действия (взлом, DoS (отказ в обслуживании), ARP-spoofing атаки, сканирование локальной вычислительной сети) направленные на нарушение функционирования элементов сети Интернет (коммуникационного оборудования, серверов, рабочих станций, программного обеспечения).

1.2. Правила работы Пользователей с электронной почтой:

7.4.1. Пользователи обязаны использовать электронную почту только для выполнения служебных обязанностей.

7.4.2. Запрещается отправлять файлы, содержащие персональные данные в открытом виде (не зашифрованные).

7.4.3. Запрещается массовая рассылка почтовых сообщений (более 100) внешним адресатам без согласования с руководством (спама).

7.4.4. Запрещается использовать не свой обратный адрес при отправке электронной почты.

7.4.5. Запрещается отправлять по электронной почте исполняемые файлы (обычно имеют расширения exe, com, bat, js, vbs и т.п.). В случае необходимости отправки таких файлов, помещать их в архив и установить пароль.

7.4.6. Присоединяемые файлы рекомендуется упаковывать в архив при помощи программ-архиваторов.

7.4.7. Корпоративные рекомендации использования электронной почты:

– Вы должны оказывать то же уважение, что и при устном общении.

– Вы должны проверять правописание, грамматику и дважды перечитывать свое сообщение перед отправлением.

– Вы не должны участвовать в рассылке посланий, пересылаемых по цепочке (чаще всего это письма религиозно-мистического, развлекательного содержания).

– Вы не должны по собственной инициативе пересылать по произвольным адресам незатребованную информацию.

– Вы не должны рассылать сообщения, которые являются зловредными, раздражающими или содержащими угрозы другим пользователям.

– Вы не должны отправлять никаких сообщений противозаконного или неэтичного содержания.

– Вы должны помнить, что электронное послание является эквивалентом почтовой открытки и не должно использоваться для пересылки персональных данных без использования средств защиты (шифрование).

– Вы не должны использовать широковещательные возможности электронной почты за исключением выпуска уместных объявлений.

– Вы не должны использовать корпоративную электронную почту для посланий личного характера.

– Вы должны неукоснительно соблюдать правила и инструкции и помогать администраторам бороться с нарушителями правил.

VIII. ПОРЯДОК РАБОТЫ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ

8.1. Под использованием носителей информации в ИСПДн Администрации понимается их подключение к инфраструктуре ИСПДн с целью обработки, приема/передачи информации между информационными системами и носителями информации.

8.2. Допускается использование только учтенных носителей информации, которые являются собственностью Администрации и подвергаются регулярной ревизии и контролю.

8.3. Учет и выдачу съемных носителей информации осуществляет лицо, ответственное за организацию обработки персональных данных. Факт выдачи носителя фиксируется в журнале учета машинных носителей информации.

8.4. Если доступ к ИСПДн производится при помощи персональных идентификаторов (eToken, Rutoken, др.), то факт получения и сдачи данных идентификаторов обязательно фиксируется ответственным за организацию обработки персональных данных, в соответствующих журналах.

8.5. Возможность подключения носителей информации, а также получение учтенных носителей информации предоставляются Пользователям по инициативе руководителей структурных подразделений в случаях:

– необходимости выполнения вновь принятым работником своих должностных обязанностей;

– возникновения у Пользователя служебной необходимости.

8.6. При использовании носителей информации необходимо:

– использовать носители информации исключительно для выполнения своих служебных обязанностей;

– бережно относится к носителям персональных данных.

– обеспечивать физическую безопасность носителей информации всеми разумными способами;

– извещать ответственному за организацию обработки персональных данных о фактах утраты (кражи) носителей информации.

8.7. При использовании носителей персональных данных запрещено:

– использовать носители персональных данных в личных целях;

– передавать носители персональных данных другим лицам (за исключением администраторов);

– хранить съемные носители с персональными данными на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

– выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

8.8. Любое взаимодействие (обработка, прием/передача информации) инициированное Пользователем между информационной системой и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администраторами заранее). Ответственный за организацию обработки персональных данных с привлечением помощи (если необходимо) сотрудников ГБУ Республики Коми «ЦБИ» на основании Соглашения оставляет за собой право блокировать или ограничивать использование носителей информации.

8.9. Информация об использовании Пользователями носителей информации в информационных системах протоколируется и, при необходимости, может быть предоставлена руководителям структурных подразделений, а также руководителю Администрации.

8.10. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициируется служебная проверка, проводимая комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Администрации и действующему законодательству РФ.

8.11. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные.

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

8.13. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с персональными данными осуществляется комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По результатам уничтожения носителей составляется акт.

8.14. В случае увольнения или перевода работника в другое структурное

подразделение, предоставленные носители персональных данных изымаются и делаются соответствующие пометки в журнале учета машинных носителей.

IX. ПРАВА ПОЛЬЗОВАТЕЛЯ

9.1. Использовать ИСПДн Администрации для выполнения должностных обязанностей.

9.2. Обращаться к ответственному за организацию обработки персональных данных для консультаций по поводу использования программного обеспечения и АРМ, вопросам обработки персональных данных.

9.3. Направлять предложения по установке новых версий существующего программного обеспечения (с обоснованием необходимости замены старых версий на новые).

9.4. Направлять предложения по модернизации программного обеспечения, разрабатываемого в Администрации или по заказу Администрации.

9.5. Направлять предложения по установке нового (а также дополнительного) программного обеспечения (с указанием цели использования, преимуществ перед существующими аналогами).

9.6. Направлять предложения по модернизации АРМ (замены на новые аналоги), с обязательным обоснованием замены и указанием преимуществ перед существующими аналогами.

9.7. Получать консультации и разъяснения по нормативным документам, регламентирующим работу с персональными данными в Администрации.

X. ОТВЕТСТВЕННОСТЬ

10. Пользователь несет персональную ответственность за свои действия или бездействие, которые могут повлечь за собой разглашение персональных данных, а также за нарушение нормального функционирования ИСПДн или их отдельных компонентов, несанкционированный доступ к информации в соответствие с законодательством Российской Федерации и локальными нормативными актами Администрации.

Приложение 6
к распоряжению администрации СП
«Приозёрный»
от 26.12.2014 г. № 36-р

ИНСТРУКЦИЯ
об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные в информационной системе персональных данных

1. Настоящая Инструкция устанавливает организацию учета, хранения и выдачи машинных носителей, содержащих персональные данные информационных систем персональных данных (ИСПДн) Администрации сельского поселения «Приозёрный» (далее – Администрация).

2. Учет, хранение и выдачу машинных носителей персональных данных осуществляет ответственный за организацию обработки персональных данных (далее - Ответственный). При увольнении сотрудника, ответственного за учет, хранение и выдачу машинных носителей персональных данных, составляется акт приема-сдачи этих документов, который утверждается руководителем Администрации.

3. Все находящиеся на хранении и в обращении машинные носители персональных данных (далее - носители) подлежат учёту. Учет всех видов и типов носителей производится в Журнале учета машинных носителей, содержащих персональные данные.

Каждый носитель должен иметь этикетку, на которой указывается его уникальный учетный номер. На несъемной части упаковки носителя ПДн указывается:

- учетный номер;
- отметка «Персональные данные»;
- дата регистрации (день, месяц, год);
- ФИО, должность, подпись сотрудника, выполнившего учет.

4. Пользователи ИСПДн получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в Журнале учета машинных носителей, содержащих персональные данные. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в Журнале учета машинных носителей, содержащих персональные данные.

5. Хранение носителей осуществляется в условиях, исключающих несанкционированное копирование, изменение или уничтожение персональных данных, а также хищение носителей. Носители должны храниться в служебных помещениях, в металлическом хранилище (сейфе) в установленном порядке. Запрещается хранить машинные носители персональных данных вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

6. В случае утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений, немедленно ставится в известность Ответственный. Соответствующие отметки вносятся в Журнале учета машинных носителей, содержащих персональные данные.

7. Носители, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. По результатам уничтожения носителей составляется Акт уничтожения машинных носителей персональных данных.

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

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

10. Контроль выполнения пользователями установленных правил эксплуатации машинных носителей персональных данных, осуществляет Ответственный.

Приложение 7
к распоряжению администрации СП
«Приозёрный»
от 26.12.2014 г. № 36-р

ПЕРЕЧЕНЬ

должностей (функциональных обязанностей) Администрации

сельского поселения «Приозёрный» для которых необходим доступ к персональным данным

Лица, которые обрабатывают (собирают, записывают, систематизируют, хранят, уточняют (обновляют, изменяют), используют, передают (распространяют, предоставляют, имеют доступ), обезличивают, блокируют,

удаляют, уничтожают) с использованием средств автоматизации, а также без использования таких средств конфиденциальную информацию (в том числе персональные данные), должны быть ознакомлены под роспись с документами, регламентирующими порядок обработки персональных данных.

Таблица 1. Наименование должностей, которым необходим доступ к персональным данным

№	**Наименование должности (функциональных обязанностей)**
1.	Глава сельского поселения
2.	Главный бухгалтер администрации
3.	Ведущий специалист администрации
4.	Специалист администрации
5.	Лица, их замещающие

Приложение 8
к распоряжению администрации СП
«Приозёрный»
от 26.12.2014 г. № 36-р

ИНСТРУКЦИЯ
о порядке доступа сотрудников Администрации сельского поселения «Приозёрный» в помещения, предназначенные для обработки персональных данных, а также о порядке сдачи ключей от этих помещений

1. Настоящая Инструкция определяет порядок доступа сотрудников Администрации сельского поселения «Приозёрный» (далее – Администрация) в помещения, предназначенные для обработки персональных данных, а также порядок сдачи ключей от этих помещений.
2. Ответственность за обеспечение исполнения требований настоящей Инструкции несёт лицо, ответственное за организацию обработки персональных данных.
3. Контроль за исполнением требований настоящей Инструкции осуществляет заместитель руководителя Администрации.
4. Сотрудники Администрации имеют доступ в помещения, предназначенные для работы с персональными данными, в рабочее время без ограничений.
5. В помещениях, предназначенных для обработки персональных данных, должна быть исключена возможность бесконтрольного проникновения посторонних лиц и обеспечена сохранность находящихся в этих помещениях документов и средств автоматизации.
6. Присутствие других лиц в данных помещениях допускается в той мере, в какой этого требуют технологические процессы обработки персональных данных. Доступ в помещения Администрации, предназначенные для обработки персональных данных, осуществляется только в сопровождении сотрудника Администрации, имеющего доступ в данные помещения, который предварительно производит оценку целесообразности и требуемого времени нахождения лица в помещении, а также проверяет документы, удостоверяющие личность.
7. Уборка в помещениях, предназначенных для обработки персональных данных, производится только в присутствии сотрудников Администрации, работающих в этих помещениях.
8. Двери должны быть оборудованы средством контроля вскрытия (оттиском печати).
9. Допускается пребывание в помещениях, предназначенных для обработки персональных данных, сотрудников Администрации в нерабочее время с письменного разрешения Главы сельского поселения с указанием даты и времени пребывания.
10. По окончании рабочего дня сотрудник Администрации, имеющий право самостоятельного доступа в помещения, обязан:

- закрыть окна и форточки помещения, проверить надежность их закрытия;
- все документы, содержащие персональные данные, поместить в сейф, запираемый шкаф или ящик стола;
- проверить наличие всех машинных носителей информации, содержащих персональные данные, поместить их в сейф, запираемый шкаф или ящик стола;
- запереть сейфы, шкафы, ящики столов;
- выключить технические средства и электроприборы;
- выключить освещение;
- запереть дверь помещения;
- опечатать помещение.

Ключи от помещения должны быть вложены в отдельный пенал (тубус). Пенал (тубус) опечатывается личной печатью сотрудника. Сотрудник проверяет надежность закрытия помещения, четкость оттисков печатей на двери помещения и на пенале (тубусе), после чего должна быть сделана соответствующая запись в Журнале приема-выдачи ключей и сотрудник службы охраны обязан расписаться за прием ключей под охрану.

11. Перед вскрытием помещения, сотрудник, прибывший первым, должен, совместно с сотрудником охраны здания проверить целостность печати на пенале (тубусе) с ключами, сделать запись в Журнале и расписаться за вскрытие помещения и получение пенала (тубуса) с ключами, затем проверить целостность печати на двери помещения.

12. При обнаружении повреждений замков, оттисков печати или других признаков, указывающих на возможное проникновение посторонних лиц в помещения, в которых ведется обработка персональных данных, эти помещения не вскрываются, а составляется акт и о случившемся немедленно ставятся в известность Глава сельского поселения и правоохранительные органы. Одновременно принимаются меры по охране места происшествия и до прибытия работников правоохранительных органов в эти помещения никто не допускается.

13. Сотрудники Администрации, указанные в списке лиц, имеющих право самостоятельного доступа в помещения, несут персональную ответственность за выполнение требований и указаний данного документа.

14. В случае пожара или иного стихийного бедствия вне рабочего времени, вскрытие помещений должно быть произведено сотрудниками службы охраны здания с целью эвакуации имущества из помещений в безопасное место. До прибытия сотрудников ГБУ Республики Коми «ЦБИ», сотрудники службы охраны должны принять меры по охране эвакуированного имущества.

Приложение 9
к распоряжению администрации СП
«Приозёрный»
от 26.12.2014 г. № 36-р

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей

1. При поступлении письменного запроса субъекта персональных данных или их представителей, ответственное лицо за организацию обработки персональных данных Администрации сельского поселения «Приозёрный» (далее – Администрация) должно зарегистрировать данный запрос в «Журнале учета обращений субъектов персональных данных по вопросам обработки персональных данных».

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

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и способы обработки персональных данных, применяемые в Администрации;
- место нахождения Администрации, сведения о лицах (за исключением сотрудников), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании федеральных законов;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Администрации, если обработка поручена такому лицу;
- иные сведения, предусмотренные действующим законодательством.

3. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных в Администрации, подпись субъекта персональных данных или его представителя (Приложение 1). Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4. Сведения по запросу должны быть предоставлены субъекту персональных данных Администрации в доступной форме, и в них не должны

содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

5. В случае, если сведения, указанные в ответе (Приложение 2), были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе повторно обратиться или направить повторный запрос в целях получения сведений и ознакомления с персональными данными не ранее, чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральными законами, принятыми в соответствии с ними нормативными правовыми актами или договорами, стороной которых являются либо выгодоприобретатели, либо поручители.

6. Субъект персональных данных вправе повторно обратиться или направить повторный запрос в целях получения сведений, касающихся обработки его персональных данных, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 5 настоящих правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 5 настоящих правил, должен содержать обоснование направления повторного запроса.

7. Администрация вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным п.5 и п.6 настоящих правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Администрации.

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

Приложение 1
к Правилам рассмотрения запросов
субъектов персональных данных или их
представителей

Главе сельского поселения «Приозёрный»

от _____
(ФИО субъекта ПДн)
_____
(адрес регистрации субъекта ПДн)
_____
(паспортные данные субъекта ПДн)
_____

_____

З А П Р О С
(о предоставлении/ изменении / исключении персональных данных субъекта)

Мною, _____, «____» _____г.
(ФИО) (дата предоставления ПДн)

в связи с осуществлением_____
_____
_____

в Администрацию СП «Приозёрный» были предоставлены следующие персональные данные:

_____
_____
_____
_____
_____
_____
_____

(*указать, какие сведения были предоставлены, например: ФИО, паспортные данные, сведения о дате и месте рождения и т.п.*)

Указанные данные были предоставлены мною для_____
_____
_____

(*указать, для проведения какой операции были предоставлены данные*)

В настоящее время сообщаю об *изменении/исключении* следующих моих персональных данных в связи с_____
_____
_____
_____

(*указать какие данные, каким образом поменялись, например: - ФИО изменение Иванова И.И, на Петрова И.И.*)

В срок не позднее 7 (семи) рабочих дней с даты получения документального подтверждения об изменении персональных данных прошу внести изменение/ исключить персональные данные в связи с_____
_____
_____
_____
_____
_____

(*прекращением отношений с Администрации, утратой сведениями достоверности и т.д*).

Уведомить о факте изменения прошу по телефону номер _____.

приложение:

- _____
- _____

_____ _____ _____

(ФИО) (подпись) (дата)

Приложение 2
к Правилам рассмотрения запросов
субъектов персональных данных или их
представителей

ОТВЕТ НА ЗАПРОС
(о предоставлении/ изменении / исключении
персональных данных субъекта)

гр. _____
_____
_____

Уважаемый _____

В ответ на Ваш запрос № _____ от _____, Администрации СП «Приозёрный» (далее – оператор) сообщает: «___» _____ _____ г. оператор получил от
_____
_____
сведения, содержащие персональные данные:
1. ФИО:
_____,
2. паспортные данные:
_____
_____
3. дата и место рождения:
_____
4._____
5._____
6._____
7._____
8._____
9. _____
10._____

Указанные данные были получены в целях_____
_____
_____
_____

___на что предварительно было получено Ваше письменное согласие (копия прилагается).

В настоящее время, материальные носители, содержащие Ваши персональные данные – _____,

хранятся в _____ по адресу_____ _____.

Непосредственный доступ к ним имеют следующие лица:

_____
_____
_____
_____
_____
_____,

обязанность работы с персональными данными субъектов на них предусмотрена характером выполняемых трудовых обязанностей, а также Приказом № _____ Администрации СП «Приозёрный».

Необходимость хранения Ваших персональных данных связана с текущим исполнением условий договора и/или не достижением целей обработки персональных данных.

Вы можете безвозмездно ознакомиться с указанными персональными данными в срок не позднее 30 дней с даты подачи заявления на ознакомление с персональными данными по адресу _____.

Глава СП «Приозёрный» _____

Приложение 10
к распоряжению администрации СП
«Приозёрный»
от 26.12.2014 г. № 36-р

ПЕРЕЧЕНЬ
информационных систем персональных данных Администрации сельского поселения «Приозёрный»

Перечень информационных систем приведен в таблице 1.

Таблица 1

№	Наименование информационной системы	Задачи системы	Наличие персональных данных
1.	**Автоматизированная система «Похозяйственный учет» (АС «Похозяйственный учет»)**	Обработка обращений граждан, ведение учетных дел	является ИСПДн
2.	**Автоматизированная система «Смета» (АС Смета)**	Ведение бухгалтерского учета и отчетности	является ИСПДн
3.	**Автоматизированная система «ИП Гуляева Е. И.» (АС «ИП Гуляева Е. И.»**	Ведение учетных дел по жилищно-коммунальным услугам	является ИСПДн

Приложение 11
к распоряжению администрации СП
«Приозёрный»
от 26.12.2014 г. № 36-р

ПРАВИЛА
работы с обезличенными персональными данными в Администрации сельском поселении «Приозёрный»

I.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила работы с обезличенными данными в Администрации сельского поселения «Приозёрный» (далее – Администрация) разработаны с учетом Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и Постановления Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», а также с учетом Приказа «Об утверждении требований и методов по обезличиванию персональных данных» от 05.09.2013 года №996

1.2. Настоящие Правила определяют порядок работы с обезличенными данными в Администрации.

1.3. Настоящие Правила утверждаются распоряжением Администрации.

1.4. В настоящих Правилах используются следующие термины и определения:

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

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

обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

II.УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

2.1. Обезличивание персональных данных может быть проведено с целью ведения статистического учета, снижения риска разглашения защищаемых персональных данных, а так же в иных целях, не противоречащих требованиям законодательства о защите персональных данных.

2.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- понижение точности некоторых сведений;
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

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

2.4. Для обезличивания персональных данных могут использоваться любые не противоречащие действующему законодательству способы.

2.5. В случае необходимости обезличивания персональных данных перечень должностей Администрации, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, утверждается приказом директора Администрации.

2.6. Глава сельского поселения принимает решение о необходимости обезличивания персональных данных.

2.7. Специалисты, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

2.8. Специалисты, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

III.ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ

3.1. Обезличенные данные не подлежат разглашению в случае, когда в результате такого разглашения появляется вероятность определения принадлежности персональных данных конкретному субъекту персональных данных.

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

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

- «Инструкции пользователя по работе с персональными данными»;

– «Инструкции об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные информационной системы персональных данных»;

– «Регламента резервного копирования и восстановления персональных данных»;

– «Порядка доступа сотрудников Администрации в помещения, предназначенные для обработки персональных данных».

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

– «Положения об обработке персональных данных сотрудников»;

– «Порядка доступа сотрудников Администрации в помещения, предназначенные для обработки персональных данных».

Приложение 12
к распоряжению администрации СП
«Приозёрный»
от 26.12.2014 г. № 36-р

ПЕРЕЧЕНЬ

должностей Администрации сельского поселения «Приозёрный»,

ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

Наименование должностей
Глава сельского поселения
Главный бухгалтер администрации
Специалист администрации

Приложение 13
к распоряжению администрации СП
«Приозёрный»
от 26.12.2014 г. № 36-р

Список лиц, имеющих право самостоятельного доступа в помещения, предназначенные для обработки персональных данных в Администрации сельского поселения «Приозёрный»

№ п/п	Наименование выделенного помещения	Ф.И.О. работника, имеющего право самостоятельного доступа, должность
1.	Кабинет № 1	1. Каракчиева Ирина Ивановна, глава сельского поселения; 2. Каракчиева Ольга Александровна, ведущий специалист администрации
2.	Кабинет № 2	1. Каракчиева Ирина Ивановна, глава сельского поселения; 2. Каракчиева Ольга Александровна, ведущий специалист администрации 3. Панюкова Татьяна Леонидовна, старший инспектор администрации 4. Денисова Ирина Николаевна, старший инспектор администрации
3.	Кабинет № 3	1. Мингалева Светлана Евлогиевна, главный бухгалтер администрации

Приложение 14
к распоряжению администрации
сельского поселения «Приозёрный»
от 26.12.2014 г. № 36-р

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

1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации (далее - Правила контроля) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных: основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила контроля разработаны в соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановлениями Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации", от 21 марта 2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" и другими нормативными правовыми актами в сфере обработки и защиты персональных данных.

3. В настоящих Правилах контроля используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

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

5. Проверки условий обработки персональных данных осуществляются ответственным за организацию обработки персональных данных администрации, назначенным распоряжением администрации.

В проведении проверки не может участвовать сотрудник администрации, прямо или косвенно заинтересованный в ее результатах.

6. Проверки соответствия обработки персональных данных установленным требованиям в администрации проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям (плановые проверки) или на основании поступившего в администрацию письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

7. Проведение проверки в администрации оформляется соответствующим распоряжением. Срок проведения плановой проверки составляет один месяц со дня принятия решения о ее проведении. Проведение внеплановой проверки осуществляется в течение трех рабочих дней с момента поступления соответствующего письменного заявления в администрацию.

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

- порядок и условия применения организационных и технических мер по

обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;

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

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

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

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

- осуществление мероприятий по обеспечению целостности персональных данных.

9. Ответственный за организацию обработки персональных данных в администрации имеет право:

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

- требовать от уполномоченных на обработку персональных данных должностных лиц уточнение, блокирование или уничтожение недостоверных или полученных незаконным путем персональных данных;

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

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

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

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

11. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, ответственный за организацию обработки персональных данных в администрации докладывает руководителю администрации в форме письменного заключения.

12. Контроль за своевременностью и правильностью проведения проверки соответствия обработки персональных данных в администрации возлагается на руководителя аппарата администрации.

Приложение 15
к распоряжению администрации
сельского поселения «Приозёрный»
от 26.12.2014 г. № 36-р

Порядок
осуществления внутреннего контроля соответствия персональных данных установленным требованиям

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, установленным Законом N 152-ФЗ, принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора.

2. Внутренний контроль соответствия обработки персональных данных делится на текущий и комиссионный.

3. Текущий внутренний контроль осуществляется на постоянной основе ответственным за обработку персональных данных в ходе мероприятий по обработке персональных данных.

4. Комиссионный внутренний контроль осуществляется постоянно действующей технической комиссией по вопросам защиты информации (далее - комиссия). Комиссионный внутренний контроль носит периодический характер, периодичность проверки - не реже одного раза в год.

5. Комиссия назначается постановлением администрации.

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

7. При проведении внутренней проверки соответствия обработки персональных данных установленным требованиям 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 учета 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.

8. В отношении персональных данных, ставших известными комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

9. Срок проведения проверки не может составлять более 30 (тридцати) дней со дня принятия решения о ее проведении. Результаты проверки оформляются в форме протокола.