РОССИЙСКАЯ ФЕДЕРАЦИЯ

Карачаево-ЧеркесскАЯ РеспубликА

АДМИНИСТРАЦИЯ УСТЬ-ДЖЕГУТИНСКОГО Муниципального РАЙОНА

УПРАВЛЕНИЕ ТРУДА И СОЦИАЛЬНОГО РАЗВИТИЯ

**ПРИКАЗ № 45-ОД**

27.11.2015 г. г. Усть-Джегута

 «Об утверждении Инструкции

администратора информационной системы

персональных данных по обеспечению

информационной безопасности при

работе с ПДн…»

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Постановлением Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", Постановление Правительства РФ от 21.03.2012 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"

ПРИКАЗЫВАЮ:

 1. Утвердить Инструкции администратора информационной системы персональных данных по обеспечению информационной безопасности при работе с персональными данными (ПДн), согласно приложению.

 2. Контроль за выполнением настоящего приказа оставляю за собой.

**Начальник Управления труда и**

**социального развития администрации**

**Усть-Джегутинского муниципального района Б.М. Кубанов**

 Приложение к приказу от 27.11.2015г. № 45-ОД

**ИНСТРУКЦИЯ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ (ПДН)**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет обязанности должностного лица, ответственного за обеспечение безопасности информации (в том числе персональных данных (ПДн)), обрабатываемой в информационных системах ПДн (ИСПДн) территориального органа Росреестра, далее - администратора безопасности информации (администратора безопасности).

1.2. Действие настоящей Инструкции распространяется на структурные подразделения территориального органа Росреестра.

1.3. Администратор безопасности назначается приказом руководителя территориального органа Росреестра из числа подготовленных работников подразделения информационной безопасности (ИБ).

1.4. Администратор безопасности по вопросам обеспечения безопасности информации подчиняется руководителю подразделения ИБ, являющемуся структурным подразделением, назначаемым ответственным за обеспечение безопасности информации в Росреестре и территориальных органах Росреестра.

1.5. Администратор безопасности отвечает за поддержание установленного уровня безопасности защищаемой информации, в том числе ПДн, при их обработке в ИСПДн Росреестра.

1.6. Администратор безопасности осуществляет методическое руководство деятельностью пользователей ИСПДн Росреестра в вопросах обеспечения безопасности информации.

1.7. Требования администратора безопасности, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИСПДн Росреестра.

1.8. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн Росреестра, состояние и поддержание установленного уровня защиты информации, обрабатываемой в ИСПДн Росреестра.

 2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Администратор безопасности обязан:

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

- Осуществлять установку, настройку и сопровождение технических средств защиты.

- Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

- Участвовать в приемке новых программных средств.

- Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

- Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

- Вести контроль над процессом осуществления резервного копирования объектов защиты.

- Осуществлять контроль над выполнением Плана мероприятий по защите персональных данных.

- Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

- Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

- Контролировать физическую сохранность средств и оборудования ИСПДн.

- Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты.

- Контролировать исполнение пользователями парольной политики.

- Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

- Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

- Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

- Не допускать к работе на элементах ИСПДн посторонних лиц.

- Осуществлять периодические контрольные проверки АРМ и тестирование правильности функционирования средств защиты ИСПДн.

- Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

- Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

- В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

- Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.