РОССИЙСКАЯ ФЕДЕРАЦИЯ

Карачаево-ЧеркесскАЯ РеспубликА

АДМИНИСТРАЦИЯ УСТЬ-ДЖЕГУТИНСКОГО Муниципального РАЙОНА

УПРАВЛЕНИЕ ТРУДА И СОЦИАЛЬНОГО РАЗВИТИЯ

**ПРИКАЗ № 28 -ОД**

20.07.2015 г. г. Усть-Джегута

«Об утверждении Инструкции

администратора информационной

безопасности при использовании ИСПДн…»

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 безопасности при использовании информационных систем персональных данных (ИСПДн), 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 20.07.2015 № 28-ОД

ИНСТРУКЦИЯ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДН)

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности ИСПДн (далее - Администратор) назначается приказом начальника Управления труда и социального развития Усть-Джегутинского муниципального района.

1.2. Администратор в своей работе руководствуется настоящей инструкцией, требованиями законов и иных нормативных актов Российской Федерации по вопросам защиты персональных данных, руководящими и нормативными документами ФСТЭК России, ФСБ России и регламентирующими документами Управления труда и социального развития Усть-Джегутинского муниципального района.

1.3. Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.4. Администратор безопасности является ответственным должностным лицом Управления труда и социального развития Усть-Джегутинского муниципального района, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.5. Администратор безопасности осуществляет методическое руководство Операторов ИСПДн, в вопросах обеспечения безопасности персональных данных.

1.6. Требования администратора информационной безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

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

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.