РОССИЙСКАЯ ФЕДЕРАЦИЯ

Карачаево-ЧеркесскАЯ РеспубликА

АДМИНИСТРАЦИЯ УСТЬ-ДЖЕГУТИНСКОГО Муниципального РАЙОНА

УПРАВЛЕНИЕ ТРУДА И СОЦИАЛЬНОГО РАЗВИТИЯ

**ПРИКАЗ № 29-ОД**

21.07.2015 г. г. Усть-Джегута

 «Об утверждении Инструкции

пользователя по обеспечению информационной

безопасности при работе с персональными данными

при возникновении нештатных ситуаций …»

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 пользователя по обеспечению информационной безопасности при работе с персональными данными при возникновении нештатных ситуаций, согласно приложению.
2. Ведущему специалисту Микитовой А.М ознакомить персонально под подпись с настоящим приказом всех работников Управления труда и социального развития администрации Усть-джегутинского муниципального района.

 3. 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 21.07.2015 г. № 29-ОД

**ИНСТРУКЦИИ ПОЛЬЗОВАТЕЛЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ**

**1. Назначение и область действия**

1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн управления, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.
2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.
3. Задачей данной Инструкции является:
* определение мер защиты от прерывания;
* определение действий восстановления в случае прерывания.
1. Действие настоящей Инструкции распространяется на всех пользователей Управления труда и социального развития администрации Усть-Джегутинского муниципального района (далее - Управление), имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:
* системы жизнеобеспечения;
* системы обеспечения отказоустойчивости;
* системы резервного копирования и хранения данных;
* системы контроля физического доступа.
1. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного одного раза в два года.

**2. Порядок реагирования на аварийную ситуацию**

**2.1. Действия при возникновении аварийной ситуации**

1. В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

2.1.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в "Журнале по учету мероприятий по контролю".

2.1.3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Управления предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

**2.2. Уровни реагирования на инцидент**

1. При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:
* **Незначительный инцидент -**  определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.
* **Авария -** любой инцидент, который приводит или может привести к прерыванию функционированию отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

* отказ элементов ИСПДн и средств защиты из-за:
* повреждения водой (прорыв системы водоснабжения, канализационных труб), а также подтопления в период проливных дождей;
* сбоя системы кондиционирования.
* отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за:
* химического выброса в атмосферу;
* эпидемии;
* массового отравления персонала;
* сильного снегопада;
* сильных морозов
* и др.
* **Катастрофа -** любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

* пожар в здании;
* взрыв;
* просадка грунта с частичным обрушением здания;
* и др.

**3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций**

**3.1. Технические меры**

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы жизнеобеспечения;

- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных;

- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;

- системы вентиляции и кондиционирования;

- системы резервного питания.

Все критичные помещения Управления труда и социального развития администрации Усть-Джегутинского муниципального района (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Порядке резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

**3.2. Организационные меры**

Ответственные за реагирование сотрудники ознакомляют всех сотрудников Управления труда и социального развития администрации Усть-Джегутинского муниципального района, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3-х рабочих дней с момента выхода нового сотрудника на работу.

По окончанию ознакомления сотрудник расписывается в журнале, предоставляемом Ответственным за реагирование сотрудником. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

Должно быть проведено обучение должностных лиц Управления труда и социального развития администрации Усть-Джегутинского муниципального района, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;

- пожаротушение;

- эвакуация людей;

- защита материальных и информационных ресурсов;

- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;

- выключение оборудования, электричества, водоснабжения, газоснабжения.

Администраторы ИСПДн и Администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

Ответственность за организацию обучения должностных лиц несет начальник Управления труда и социального развития администрации Усть-Джегутинского муниципального района.

**4.** **Действия при возникновении наиболее распространённых**

**нештатных ситуаций в информационных системах**

**Управления труда и социального развития**

**администрации Усть-Джегутинского муниципального района**

**- Сбой программного обеспечения.** Администратор информационной безопасности совместно с Администратором ИСПДн выясняют причину сбоя программного обеспечения (далее – ПО). Если исправить ошибку своими силами (в том числе после консультации с разработчиками ПО) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику ПО.

**- Отключение электричества.** Администратор информационной безопасности совместно с Администратором ИСПДн проводят анализ на наличие потерь и (или) разрушения данных и ПО, а так же проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии с составлением акта.

**- Сбой в локальной вычислительной сети (ЛВС).** Администратор информационной безопасности совместно с Администратором ИСПДн отдела проводят анализ на наличие потерь и (или) разрушения данных и ПО. В случае необходимости, производится восстановление ПО и данных из последней резервной копии с составлением акта.

**- Выход из строя сервера.** Сотрудник, ответственный за эксплуатацию сервера, проводит меры по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы управления. При необходимости производятся работы по восстановлению ПО и данных из резервных копий с составлением акта.

**- Потеря данных.** При обнаружении потери данных администратор информационной безопасности совместно с Администратором ИСПДн проводят мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий с составлением акта.

**- Обнаружен вирус.** При обнаружении вируса следует руководствоваться Инструкцией по организации антивирусной защиты.

**- Обнаружена утечка информации (уязвимость в системе защиты).** При обнаружении утечки информации ставится в известность администратор информационной безопасности. Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищённости системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

**- Попытка несанкционированного доступа (НСД).** При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Также рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

**- Компрометация ключей.** При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты. Проводиться служебное расследование.

**- Компрометация пароля.** При компрометации пароля необходимо руководствоваться Инструкцией по организации парольной защиты.

**- Физическое повреждение ЛВС или ПЭВМ.** Ставится в известность администратор информационной безопасности. Проводится анализ на утечку или повреждение информации. Определяется причина повреждения ЛВС или ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий с составлением акта.

С приказом № \_\_\_ от «\_\_» \_\_\_\_\_\_\_\_20\_\_ г. ознакомлен (а):