РОССИЙСКАЯ ФЕДЕРАЦИЯ

Карачаево-ЧеркесскАЯ РеспубликА

АДМИНИСТРАЦИЯ УСТЬ-ДЖЕГУТИНСКОГО Муниципального РАЙОНА

УПРАВЛЕНИЕ ТРУДА И СОЦИАЛЬНОГО РАЗВИТИЯ

**ПРИКАЗ № 32 -ОД**

23.07.2015 г. г. Усть-Джегута

«Об утверждении Положения о резервировании

и восстановлении работоспособности технических средств

и программного обеспечения, баз данных и средств защиты

персональных данных…»

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 Положение о резервировании и восстановлении работоспособности технических средств и программного обеспечения, баз данных и средств защиты персональных данных, 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 23.07.2015 № 32-ОД

ПОЛОЖЕНИЕ (ИНСТРУКЦИЯ) О РЕЗЕРВИРОВАНИИ И ВОССТАНОВЛЕНИИ РАБОТОСПОСОБНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ И СРЕДСТВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ

1.1. Настоящее положение (инструкция) о резервировании и восстановлении работоспособности технических средств и программного обеспечения, баз данных и средств защиты персональных данных (далее - Положение) определяет действия, связанные с функционированием информационных систем персональных данных (далее - ИСПДн) Управления труда и социального развития администрации Усть-Джегутинского муниципального района (далее - Управление), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью настоящего Положения является порядок резервирования и восстановление работоспособности элементов ИСПДн и меры предотвращения потери защищаемой информации.

1.3. Задачей данной Инструкции является:

- определение мер защиты от потери информации;

- определение действий восстановления в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех пользователей Управления, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения ИСПДн;

- системы резервного копирования и хранения данных.

Пересмотр настоящего документа осуществляется по мере необходимости.

Ответственным работником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор безопасности.

Ответственным работником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор безопасности.

2. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

2.1. В настоящем Положении под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;

- в результате преднамеренных действий пользователей и третьих лиц;

- в результате нарушения правил эксплуатации технических средств ИСПДн;

- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Реагирование на инцидент включает следующие этапы:

- выявление инцидента;

- анализ и принятие решений;

- принятие мер (технических и организационных) по устранению инцидента.

2.4. Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование работником в "Журнале по учету нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн".

2.5. В сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Управления (Администратор безопасности) 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.

2.6. Порядок восстановления работоспособности ИСПДн.

2.6.1. Восстановление работоспособности ИСПДн осуществляется в случаях, указанных в пункте 2.2 настоящей инструкции.

2.6.2. Восстановление работоспособности ИСПДн осуществляется Администратором безопасности в соответствии с эксплуатационной документации на программное обеспечение и технические средства обработки персональных данных

2.6.3. В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на ответственного за организацию работ по обеспечению безопасности персональных данных.

3. МЕРЫ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ РАБОТЫ И

ВОССТАНОВЛЕНИЯ РЕСУРСОВ ПРИ ВОЗНИКНОВЕНИИ ИНЦИДЕНТОВ

ТЕХНИЧЕСКИЕ МЕРЫ

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

- пожарные сигнализации и системы пожаротушения;

- системы вентиляции и кондиционирования;

- системы резервного питания.

Все критичные помещения Управления (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции, АРМ должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания применяются следующие методы резервного электропитания:

- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т.д.).

Системы обеспечения отказоустойчивости:

- кластеризация;

- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации:

- для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск).

Организационные меры

Резервное копирование и хранение данных осуществляется на периодической основе:

- для обрабатываемых персональных данных - один раз в неделю;

- для технологической информации - один раз в месяц;

- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн - один раз в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования отражаются в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, нумеруются: номером носителя, датой проведения резервного копирования.

Носители хранятся в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

Носители хранятся не менее года, для возможности восстановления данных.