

АДМИНИСТРАЦИЯ  
МАНЫЧСКОГО  
СЕЛЬСКОГО  
МУНИЦИПАЛЬНОГО  
ОБРАЗОВАНИЯ  
РЕСПУБЛИКИ КАЛМЫКИЯ



ХАЛЬМГ ТАНЬЧИН  
ЯШАЛТИНСК РАЙОНА  
МУНИЦИПАЛЬН  
БҮРДЭЦИИН  
АДМИНИСТРАЦ

---

ул.Школьная 2, пос.Манычский, Республика Калмыкия, 359013

тел/факс/84745/97253, , [manicheskoe.smo@mail.ru](mailto:manicheskoe.smo@mail.ru)

РАСПОРЯЖЕНИЕ

От 4 12.2013г

№ 36

пос.Манычский

В соответствии с Федеральным законом Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных» и Постановлением Правительства Российской Федерации от 17.11.2007 № 781 «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»:

1. утвердить:

-Инструкция пользователя по обеспечению безопасности обработки персональных данных в Администрации Манычского сельского муниципального образования Республики Калмыкия при возникновении внештатных ситуаций (приложение №1)

2. Руководителю организационно-документационного отдела администрации Манычского СМО РК Ошкаевой В.Б. довести данное распоряжение до сотрудников в части касающейся.

3. Контроль за выполнением требований настоящего распоряжения оставляю за собой.

Глава администрации  
Манычского СМО РК

А.Д.Науменко

Приложение № 1  
к распоряжению Администрации  
Манычского СМО РК  
от 4.12.2013года № 36

**Инструкция пользователя по обеспечению безопасности обработки персональных  
данных в Администрации Манычского сельского муниципального образования  
Республики Калмыкия  
при возникновении внештатных ситуаций**

**1. Назначение и область действия**

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

Задачей данной Инструкции является:

- определение мер защиты от прерывания;
- определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех пользователей администрации, 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.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

**2. Порядок реагирования на аварийную ситуацию**

**2.1. Действия при возникновении аварийной ситуации**

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении 1.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники 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**

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

**Уровень 1 – Незначительный инцидент.** 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.

**Уровень 2 – Авария.** Любой инцидент, который приводит или может привести к прерыванию работоспособности 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, систем охлаждения), а также подтопления в период паводка или проливных дождей;
  - сбоя системы кондиционирования.
- Отсутствие Администратора безопасности более чем на сутки из-за:
  - химического выброса в атмосферу;
  - сбоев общественного транспорта;
  - эпидемии;
  - массового отравления персонала;
  - сильного снегопада;
  - торнадо;
  - сильных морозов.

**Уровень 3 – 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 работоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;
- massовые беспорядки в непосредственной близости от Объекта.

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

#### **3.1Технические 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 отказ устойчивости;
- системы резервного копирования и хранения данных;

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;

Все критичные помещения (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.

### **3.2Организационные меры**

Ответственные за реагирование сотрудники ознакомливают всех сотрудников находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х 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, 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.

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 Глава МО . Сроки и порядок их обучения согласуется с Администратором безопасности.

## Приложение 1

### Источники угроз

Таблица 1 – Источники угроз

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Торнадо
16	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
Телеком и ИТ угрозы	
17	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
18	Ошибка персонала, имеющего доступ к серверной
19	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
20	Отключение электроэнергии
21	Сбой в работе интернет-провайдера
22	Физически разрыв внешних каналов связи