**КУРГАНСКАЯ ОБЛАСТЬ**

**ВАРГАШИНСКИЙ РАЙОН**

**АДМИНИСТРАЦИЯ ЮЖНОГО** **СЕЛЬСОВЕТА**

**ПОСТАНОВЛЕНИЕ**

**от 14 мая 2021 года № 33**

**с. Дубровное**

Об утверждении инструкции по обеспечению безопасности

персональных данных при возникновении внештатных ситуаций

в Администрации Южного сельсовета

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований   
о защите информации, не составляющей государственную тайну, содержащейся   
в государственных информационных системах», Администрация Южного сельсовета

ПОСТАНОВЛЯЕТ:

1. Утвердить инструкцию по обеспечению безопасности персональных данных при возникновении внештатных ситуаций в Администрации Южного сельсовета**,** согласно приложению к настоящему постановлению.

2. Опубликовать настоящее постановление в Информационном бюллетене Южного сельсовета.

3. Контроль за выполнением настоящего постановления оставляю за собой.

Глава Южного сельсовета Б.И.Максимов

Приложение к постановлению

Администрации Южного сельсовета

от 14 мая 2021г № 33

«Об утверждении инструкции по обеспечению

безопасности персональных данных

при возникновении внештатных ситуаций

в Администрации Южного сельсовета»

**Инструкция**

по обеспечению безопасности персональных данных

при возникновении внештатных ситуаций

в Администрации **Южного сельсовета**

1. **Общие положения**
   1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных системах персональных данных (далее – ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций в Администрации Южного сельсовета (далее – Администрация).
   2. Целью настоящей Инструкции является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.
   3. 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.

1. **Порядок реагирования на аварийную ситуацию**

4. Действия при возникновении аварийной ситуации.

В настоящей инструкции 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, согласно Приложению к данной инструкции.

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование пользователем в «Журнале ИСПДн».

В кратчайшие сроки, не превышающие одного рабочего дня, пользователи ИСПДн Администрации предпринимают меры по восстановлению работоспособности ИСПДн. Принимаемые меры согласуются с Главой Южного сельсовета.

5. Уровни реагирования на инцидент.

При реагировании на инцидент, важно, чтобы пользователь ИСПДн 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:

1) 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;

- химического выброса в атмосферу;

- сбоев общественного транспорта;

- эпидемии;

- массового отравления персонала;

- сильного снегопада;

- 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.

К катастрофам относятся следующие инциденты:

1) пожар в здании;

2) взрыв;

3) просадка грунта с частичным обрушением здания;

4) массовые беспорядки в непосредственной близости от Объекта.

1. **Меры обеспечения непрерывности работы и восстановления ресурсов**

**при возникновении аварийных ситуаций**

6. 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:

1) системы жизнеобеспечения;

2) системы обеспечения отказоустойчивости;

3) системы резервного копирования и хранения данных;

Системы жизнеобеспечения ИСПДн включают:

1) пожарные сигнализации и системы пожаротушения;

2) системы резервного питания.

Все критичные помещения Администрации (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 Регламенте проведения резервного копирования (восстановления) технических систем и программного обеспечения, баз данных и средств защиты информации, хранящиеся на автоматизированных рабочих местах Администрации Южного сельсовета, утвержденным распоряжением № \_\_\_\_\_ от \_\_\_\_\_\_\_\_\_.

Приложение   
к инструкции по обеспечению безопасности персональных данных при возникновении внештатных ситуаций в Администрации Южного сельсовета

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 |