УТВЕРЖДЕНА
Приказом директора
МБУ ОДО «Сивинский ДТ»
от 07.09.2018 г. № 50-од

Инструкция
пользователя ИСПДн по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций

1. Назначение и область действия

1.1 Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн МБУ ОДО «Сивинский ДТ», меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

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

1.3 Задачами данной Инструкции являются:

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

1.4 Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также на 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.

1.5 Пересмотр настоящего документа осуществляется по мере необходимости.

2. Порядок реагирования на аварийную ситуацию

2.1 **Действия при возникновении аварийной ситуации**. 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 таблице «Источники угроз».

Технологические угрозы	
1.	Пожар в здании
2.	Повреждение водой (прорыв системы водоснабжения, канализационных труб)
3.	Взрыв (теракт, взрывчатые вещества)
Внешние угрозы	
4.	Массовые беспорядки
5.	Эпидемия
6.	Массовое отравление персонала
Стихийные бедствия	
7.	Удар молнии
8.	Сильный снегопад
9.	Сильные морозы
10.	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
11.	Затопление водой в период паводка
12.	Наводнение, вызванное проливным дождем
13.	Торнадо
Телекоммуникационные и ИТ угрозы	

14.	Сбой системы кондиционирования
15.	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
16.	Ошибка персонала, имеющего доступ к ИС
17.	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
18.	Отключение электроэнергии
19.	Сбой в работе интернет-провайдера
20.	Физический разрыв внешних каналов связи

2.2 В кратчайшие сроки, не превышающие одного рабочего дня, ответственный за организацию обработки ПД предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с директором. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.3 **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 ответственным за организацию обработки ПД.
- 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 ответственным за организацию обработки ПД.

К авариям относятся следующие инциденты:

1. Отказ элементов ИСПДн и средств защиты из-за:
   - повреждения водой (прорыв системы водоснабжения, канализационных труб), а также подтопления в период паводка или проливных дождей;
   - сбоя системы кондиционирования.
2. Отсутствие заместителя по безопасности более чем на сутки из-за:
   - 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 неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты: пожар в здании; взрыв; просадка грунта с частичным обрушением здания; массовые беспорядки в непосредственной близости от Объекта.

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 включает пожарную сигнализацию, систему вентиляции и кондиционирования.

Все помещения, в которых размещаются элементы ИСПДн должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Порядке резервирования и восстановления работоспособности технический систем и программного обеспечения, баз данных и средств защиты информации.

3.2 **Организационные меры.** Ответственный за организацию обработки ПДн знакомит всех сотрудников ОО с данной инструкцией, а так же в срок, не превышающий трех рабочих дней- с момента выхода нового сотрудника на работу. По окончанию ознакомления сотрудник расписывается в листе ознакомления. Должно быть проведено обучение сотрудников ОО, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Они 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.

Ответственный за организацию обработки ПД должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИСПДн.

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

Приложение 1

Лист ознакомления
с Инструкцией пользователя ИСПДн по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций

№	Ф.И.О.	должность	дата	подпись