Приложение №2
к приказу от 31.12.2019 г. № 104/08-од
«Об организации мероприятий
по защите персональных данных,
обрабатываемых в ГБОУ гимназии №1
г. Новокуйбышевска»

УТВЕРЖДЕНО
приказом ГБОУ гимназии №1
г. Новокуйбышевска
от 31.12.2019 г. № 104/08-од
Директор
Л.Г. Слепцова

Инструкция

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

1. Общие положения

1.1. Настоящая Инструкция пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций (далее – Инструкция) определяет возможные аварийные ситуации, связанные с функционированием ИСПДн в государственном бюджетном общеобразовательном учреждении Самарской области гимназии № 1 им. Н.И. Ферапонтова города Новокуйбышевска городского округа Новокуйбышевск Самарской области (далее – образовательная организация), 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. Задачей данной Инструкции является:

- 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, но не реже одного раза в два года.

2. Порядок реагирования на аварийную ситуацию

2.1. Действия при возникновении аварийной ситуации

2.1.1. 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 таблице «Источники угроз».

Таблица №1 «Источники угроз»

Технологические угрозы	
1.	Пожар в здании
2.	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3.	Взрыв (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)
Телекоммуникационные и ИТ угрозы	
17.	Сбой системы кондиционирования
18.	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
19.	Ошибка персонала, имеющего доступ к серверной
20.	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
21.	Отключение электроэнергии
22.	Сбой в работе интернет-провайдера
23.	Физически разрыв внешних каналов связи

2.1.2. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники образовательной организации (Администратор ИС, ответственный за организацию обработки ПД) предпринимают меры по восстановлению работоспособности.

2.1.3. Предпринимаемые меры по возможности согласуются с вышестоящим руководителем (директором) образовательной организации. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.2. Уровни реагирования на инцидент

2.2.1. 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 работниками (Администратор ИС, ответственный 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 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.
2. 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 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 образовательной организации.

2.2.2. При возникновении нештатной ситуации любого уровня пользователь обязан оповестить ответственного за организацию обработки персональных данных, сообщив характер аварийной ситуации, масштаб ситуации по предварительной субъективной оценке.

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

3.1. Технические меры

3.1.1. 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.

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

3.2. Организационные меры

3.2.1. Ответственные за реагирование работники знакомят всех работников образовательной организации, находящихся в их зоне ответственности, с

данной инструкцией в срок, не превышающий трех рабочих дней с момента выхода нового работника на работу.

3.2.2. По окончанию ознакомления работник расписывается в листе ознакомления. Подпись работника должна соответствовать его подписи в документе, удостоверяющем его личность.

3.2.3. 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, газоснабжения.

3.2.4. Ответственный за организацию обработки ПД и Администратор безопасности ПД должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

3.2.5. 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.

3.3. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за организацию обработки персональных данных в Журнале регистрации фактов нарушения и восстановления работоспособности.

3.4. Навыки и знания пользователей ИСПДн по реагированию на аварийные ситуации должны регулярно проверяться.

При необходимости должно проводиться дополнительное обучение пользователей ИСПДн порядку действий при возникновении аварийной ситуации.

Ответственность за организацию обучения пользователей ИСПДн несет ответственный за организацию обработки персональных данных.