Приложение № 25
к приказу ГАУ ДПО ИРО
от 12.02.2025 № 23

Инструкция
по действиям работников во внештатных ситуациях при обработке защищаемой информации в информационных системах государственного автономного учреждения дополнительного профессионального образования Иркутской области «Институт развития образования Иркутской области»

1 Общие положения

1.1. Настоящая Инструкция по действиям работников во внештатных ситуациях при обработке защищаемой информации в информационных системах государственного автономного учреждения дополнительного профессионального образования Иркутской области «Институт развития образования Иркутской области» (далее соответственно – Инструкция, ИС ГАУ ДПО ИРО)определяет возможные аварийные ситуации, связанные с функционированием, меры и средства поддержания непрерывности работы и восстановления работоспособности ИС ГАУ ДПО ИРО после аварийных ситуаций.

1.2. Целью Инструкции является превентивная защита элементов ИС ГАУ ДПО ИРО от прерывания в случае реализации рассматриваемых угроз.

1.3. Задачами Инструкции являются определение мер защиты от прерывания, определение действий восстановления в случае прерывания.

1.4. Действие Инструкции распространяется на всех сотрудников ГАУ ДПО ИРО, имеющих доступ к ресурсам ИС ГАУ ДПО ИРО, а также к основным системам обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

1) система жизнеобеспечения;
2) система обеспечения отказоустойчивости;
3) система резервного копирования и хранения данных;
4) система контроля физического доступа.

1.5. Пересмотр положений Инструкции осуществляется по мере необходимости, но не реже одного раза в два года.

2 Порядок работников реагирования на аварийную ситуацию

2.1. В целях использования в Инструкции под аварийной ситуацией (инцидентом) понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИС ГАУ ДПО ИРО, предоставляемых пользователям. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении № 1 к Инструкции – «Источники угроз».

2.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование работником в журнале учета мероприятий по контролю обработки и защиты в ИС ГАУ ДПО ИРО.

2.3. Инцидент может возникнуть в результате преднамеренных действий злоумышленника или непреднамеренных действий пользователей, аварий, стихийных бедствий.

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники ГАУ ДПО ИРО (администратор информационной безопасности, работник, ответственный за организацию обработки персональных данных (далее – ПДн) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по

возможности согласуются с вышестоящим руководителем. По необходимости иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.5. При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента.

Критичность оценивается на основе следующей классификации:

2.5.1. уровень 1 – незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИС ГАУ ДПО ИРО и средств защиты. Эти инциденты решаются ответственными за реагирование работниками.

2.5.2. уровень 2 – авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИС ГАУ ДПО ИРО и средств защиты. Эти инциденты выходят за рамки ответственности работников.

К авариям относятся следующие инциденты:

1) отказ элементов ИС ГАУ ДПО ИРО 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 информационной безопасности более чем в течение суток из-за:

- химического выброса в атмосферу;
- сбоев общественного транспорта;
- эпидемии;
- массового отравления персонала;
- сильного снегопада;
- торнадо;
- сильных морозов;

2.5.3. уровень 3 – катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИС ГАУ ДПО ИРО и средств защиты, а также к угрозе жизни пользователей ИС ГАУ ДПО ИРО, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИС ГАУ ДПО ИРО и средств защиты на сутки и более.

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.

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

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

1) системы жизнеобеспечения, что включает:
2) пожарные сигнализации и системы пожаротушения;
3) системы вентиляции и кондиционирования;
4) системы резервного питания;
5) системы обеспечения отказоустойчивости;
6) системы резервного копирования и хранения данных;
7) системы контроля физического доступа;

8) пожарные сигнализации и системы пожаротушения;

9) системы вентиляции и кондиционирования.

3.2. Все критичные помещения ГАУ ДПО ИРО (помещения, в которых размещаются элементы ИС ГАУ ДПО ИРО и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.3. Порядок предотвращения потерь информации и организации системы жизнеобеспечения информационной системы описан в Порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

3.4. Ответственные за реагирование работники ознакомляют всех работников ГАУ ДПО ИРО, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3 (трех) рабочих дней с момента выхода нового работника на работу.

3.5. Должно быть проведено обучение должностных лиц ГАУ ДПО ИРО, имеющих доступ к ресурсам ИС ГАУ ДПО ИРО, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

1) оказание первой медицинской помощи;

2) пожаротушение;

3) эвакуация людей;

4) защита материальных и информационных ресурсов;

5) методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;

6) выключение оборудования, электричества, водоснабжения, газоснабжения.

3.6. Администратор информационной безопасности должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИС ГАУ ДПО ИРО.

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

3.8. Ответственность за организацию обучения должностных лиц ГАУ ДПО ИРО несет руководитель отдела. Сроки и порядок их обучения согласуется с администратором информационной безопасности.

Приложение
к Инструкции по действиям работников
во внештатных ситуациях при обработке
защищаемой информации в информационных системах
государственного автономного учреждения
дополнительного профессионального образования
Иркутской области «Институт развития образования
Иркутской области»

Источники угроз

1. Технологические угрозы	
1.1	Пожар в здании
1.2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
1.3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
1.4	Химический выброс в атмосферу
2. Внешние угрозы	
2.1	Массовые беспорядки
2.2	Сбои общественного транспорта
2.3	Эпидемия
2.4	Массовое отравление персонала
3. Стихийные бедствия	
3.1	Удар молнии
3.2	Сильный снегопад
3.3	Сильные морозы
3.4	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
3.5	Затопление водой в период паводка
3.6	Наводнение, вызванное проливным дождем
3.7	Торнадо
3.8	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
4. Телеком и ИТ угрозы	
4.1	Сбой системы кондиционирования
4.2	Сбой ИТ-систем
5. Угроза, связанная с человеческим фактором	
5.1	Ошибка персонала, имеющего доступ к помещению, где расположено серверное оборудование
5.2	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
6. Угрозы, связанные с внешними поставщиками	
6.1	Отключение электроэнергии
6.2	Сбой в работе интернет-провайдера
6.3	Физически разрыв внешних каналов связи