

УТВЕРЖДАЮ:



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 ИСПД организации, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПД после аварийных ситуаций.

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

1.3. Задачей настоящей 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 ИСПД, 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 ИСПД, предоставляемых пользователям ИСПД. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных ниже:

Источники угрозы

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. Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)

Телекоммуникационные и ИТ угрозы

16. Сбой системы кондиционирования
17. Сбой ИТ - систем

Угроза, связанная с человеческим фактором

18. Нарушение конфиденциальности, целостности и доступности конфиденциальной информации

Угрозы, связанные с внешними поставщиками

19. Отключение электроэнергии
 20. Сбой в работе Интернет-провайдера
 21. Физический разрыв внешних каналов связи
- 2.1.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».
- 2.1.3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники организации (Администратор безопасности, Администратор и Оператор ИСПД) предпринимают меры по восстановлению работоспособности системы. Принимаемые меры по возможности согласуются с вышестоящим руководством. По мере 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 ИСПД 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 ИСПД и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

1. Отказ элементов ИСПД 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 ИСПД и Администратора безопасности более чем на сутки из-за:
 - химического выброса в атмосферу;
 - сбоя общественного транспорта;
 - эпидемии;
 - массового отравления персонала;
 - сильного снегопада;
 - сильных морозов.

Уровень 3 - Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПД и средств защиты, а также к угрозе жизни пользователей ИСП, классифицируется как катастрофа. Обычно к катастрофам относятся обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПД 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

Технические меры

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

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПД включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.1.2. Все критические помещения (помещения, в которых размещаются элементы ИСПД и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

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

3.2. Организационные меры

3.2.1. Ответственные за реагирование сотрудники знакомят всех остальных сотрудников, находящихся в их зоне ответственности, с данной Инструкцией в срок, не превышающий трех рабочих дней с момента выхода нового сотрудника на работу. По окончании ознакомления сотрудник расписывается в листе ознакомления. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

3.2.2. Должно быть проведено обучение должностных лиц учреждения, имеющих доступ к ресурсам ИСПД, 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 на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения.

3.2.3. Администраторы ИСПД и Администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПД.

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.