



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 организации, 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 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 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».

Источники угроз:

Технологические угрозы

-Пожар в здании

-Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)

-Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)

-Химический выброс в атмосферу

Внешние угрозы

Массовые беспорядки

Сбои общественного транспорта

Эпидемия
Массовое отравление персонала
Стихийные бедствия
Удар молнии
Сильный снегопад
Сильные морозы
Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
Затопление водой в период паводка
Наводнение, вызванное проливным дождем
Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)

Телекоммуникационные и ИТ угрозы
Сбой системы кондиционирования
Сбой ИТ - систем Угроза,
связанная с человеческим фактором
Ошибка персонала, имеющего доступ к серверной |
Нарушение конфиденциальности, целостности и доступности конфиденциальной информации

Угрозы, связанные с внешними поставщиками
Отключение электроэнергии
Сбой в работе Интернет-провайдера |
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 ИСПДн) 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 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 (провывы системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей; сбоя системы кондиционирования.
2. Отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за: 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. Обычно к катастрофам относятся 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

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 ИСПДн включают: • пожарные сигнализации и системы пожаротушения; • системы вентиляции и кондиционирования; • системы резервного питания.

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

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

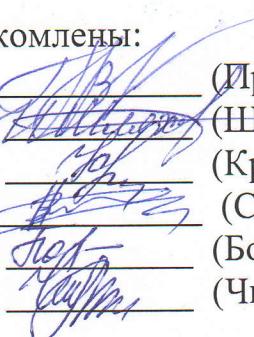
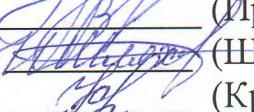
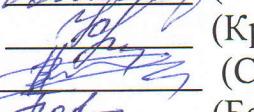
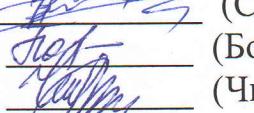
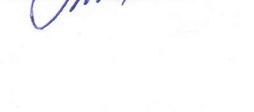
3.2. Организационные меры

3.2.1. Ответственные за реагирование сотрудники ознакомляют 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.

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 на аварийную ситуацию; выключение оборудования, электричества, водоснабжения.

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

С инструкцией ознакомлены:

- «26 » 08 2019 г.  (Прусова Н.В.)
«26 » 08 2019 г.  (Шляхова И.И.)
«26 » 08 2019 г.  (Крыловская Е.И.)
«26 » 08 2019 г.  (Стручкова Н.В.)
«26 » 08 2019 г.  (Бондаренко Г.В.)
«26 » 08 2019 г.  (Чикишева К.А.)