УТВЕРЖДЕНА

Приказом директора областного государственного бюджетного учреждения «Комплексный центр социального обслуживания Еврейской автономной области»

от 09.01 2019 г. № 19

ИНСТРУКЦИЯ
пользователя ИСПДн по обеспечению безопасности при возникновении внештатных ситуаций

1. Назначение и область действия

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием объектов вычислительной техники ОГБУ «КЦСО ЕАО» меры и средства поддержания непрерывности работы и восстановления работоспособности объектов вычислительной техники (далее – ОВТ) после аварийных ситуаций.

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

Задачами, решаемые данной Инструкцией, являются определение мер защиты от прерывания; определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех пользователей ОВТ, имеющих доступ к ее ресурсам, а также 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.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в три года.

2. Действия при возникновении аварийной ситуации

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:

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; торнадо; 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; физически разрыв внешних каналов связи

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование работником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники учреждения, имеющие доступ к ПДн и осуществляющие обработку ПДн под руководством администратора безопасности предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

Все действия в процессе реагирования на аварийные ситуации должны документироваться администратором безопасности информации в соответствующем журнале.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники ОГБУ «КЦСО ЕАО» предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

1. 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 ОВТ и средств защиты. Эти инциденты решаются ответственными за реагирование работниками.

Уровень 2 – Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ОВТ и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование работниками.

К авариям относятся следующие инциденты:

Отказ элементов ОВТ 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.

Отсутствие администратора безопасности информации более чем на сутки из-за: химического выброса в атмосферу; сбоев общественного транспорта; эпидемии; массового отравления персонала; сильного снегопада; урагана; сильных морозов.

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

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

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 ОВТ включают пожарные сигнализации и системы пожаротушения; системы вентиляции и кондиционирования; системы резервного питания.

Все критичные помещения ОГБУ «КЦСО ЕАО» (помещения, в которых размещаются элементы ОВТ и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ОВТ описан в Инструкции о порядке резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

Организационные меры

Ответственные за реагирование специалисты ознакомляют всех работников ОГБУ «КЦСО ЕАО», находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий трёх рабочих дней с момента выхода нового работника на работу.

По окончанию ознакомления работник расписывается в журнале, предоставляемом Ответственным за реагирование работником. Подпись работника должна соответствовать его подписи в документе, удостоверяющем его личность.

Должно быть проведено обучение должностных лиц ОГБУ «КЦСО ЕАО», имеющих доступ к ресурсам ОВТ, 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 работниками на аварийную ситуацию; выключение оборудования, электричества,

водоснабжения, газоснабжения.

Администратор безопасности информации должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ОВТ.

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.

Ответственность за организацию обучения должностных лиц несет Администратор безопасности информации.

Подготовил:
Специалист по технической поддержке

Согласовано:
Администратор безопасности информации