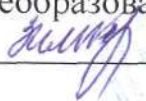


Утверждаю
Директор МБОУ «Начальная
общеобразовательная школа № 14»

Н.А. Зильберман



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 в МБОУ «Начальная общеобразовательная школа №14» 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.

Задачи, 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 два 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; сбой 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 сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Учреждения сотрудниками (Администратор безопасности, Администратор и Оператор ИСПДн) 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 сотрудники в МБОУ « Начальная общеобразовательная школа №14» 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.

3. 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 сотрудниками.

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 сотрудники знакомят всех сотрудников МБОУ « Начальная общеобразовательная школа №14», находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий трёх рабочих дней с момента выхода нового сотрудника на работу.

По окончании ознакомления сотрудник расписывается в журнале, предоставляемом Ответственным за реагирование сотрудником. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

Должно быть проведено обучение должностных лиц главного бухгалтера, секретаря, 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 сотрудниками на аварийную ситуацию; выключение оборудования, электричества, водоснабжения, газоснабжения.

Администраторы ОВТ и Администраторы безопасности информации должны быть дополнительно обучены 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:

Администратор
информации

безопасности



О.И. Шаталова