

ИНСТРУКЦИЯ

пользователи 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 МБОУ СОШ № 1, 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 сбоям 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	
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	Сбой 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 подключенных 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	Ошибка персонала, имеющего доступ к серверной
19	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
20	Отключение электроэнергии
21	Сбой в работе Интернет-провайдера
22	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 Школы (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 (прорыв 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;
 - сбоя 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.

1. 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 МБОУ СОШ № 1 (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 знакомят всех сотрудников МБОУ СОШ № 1, 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 МБОУ СОШ № 1, 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.

ИНСТРУКЦИЯ

по организации антивирусной защиты в муниципальном бюджетном общеобразовательном учреждении - средней общеобразовательной школе № 1 им. Г.К. Нестеренко муниципального образования Каневской район

1. Настоящая Инструкция определяет требования к организации защиты по организации антивирусной защиты в МБОУ СОШ № 1 (далее Школа) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников Школы за их выполнение.
2. К использованию в Школе допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.
3. Установка средств антивирусного контроля на компьютерах осуществляется уполномоченным сотрудником Школы. Настройка параметров средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.
4. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.
5. Обязательному антивирусному контролю подлежат любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).
6. Контроль входящей и исходящей информации на защищаемых серверах и персональных компьютерах (далее ПК) осуществляется непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения («монитор»). Полная проверка информации хранящейся на серверах и ПК должна осуществляться не реже одного раза в месяц.
7. Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться ежедневно.
8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка:
 - на защищаемом автоматизированном рабочем месте (АРМ) - ответственным за обеспечение информационной безопасности.
9. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник Школы самостоятельно или вместе с ответственным за антивирусную защиту Школы должен провести внеочередной антивирусный контроль своей рабочей станции.
10. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:
 - приостановить работу;
 - немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за антивирусную защиту Школы, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе;
 - совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
 - провести лечение или уничтожение зараженных файлов.
11. Ответственность за организацию антивирусного контроля в Школе, в соответствии с требованиями настоящей Инструкции возлагается на руководителя Школы.
12. Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на ответственного за антивирусную защиту Школы и всех сотрудников, являющихся пользователями ПК Школы.
13. Периодический контроль за состоянием антивирусной защиты в Школе, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений Школы осуществляется ответственным за антивирусную защиту Школы.