Утверждено
приказом директора
средней школы №59
от 11.03.2021г. № 01-10/78

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационные системы персональных данных в средней школе №59

Общие положения

1. Целью настоящей Инструкции является обеспечение превентивной защиты элементов ИСПДн средней школы № 59 от предотвращения потери защищаемой информации.

2. Задачей данной Инструкции является:
- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

3. Действие настоящей Инструкции распространяется на всех пользователей средней школы №59, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:
- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирование и хранения данных;
- системы контроля физического доступа.

4. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается технический специалист школы.

Порядок реагирования на **инцидент**

1. В настоящей Инструкции под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляем пользователям ИСПДн, а также потерей защищаемой информации.

2. Происшествие, вызывающее инцидент, может произойти:
- В результате непреднамеренных действий пользователей.
- В результате преднамеренных действий пользователей и третьих лиц.
- В результате нарушения правил эксплуатации технических средств ИСПДн.
- В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

3. Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

4. В кратчайшие сроки, не превышающее одного рабочего дня, ответственными за реагирование сотрудники школы (Технический специалист 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 срок.

Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

1. Технические меры

1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, 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.

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

1.3. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

1.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

1.5. Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

1.5.1. Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

1.5.2. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

1.5.3. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

2. Организационные меры

2.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных — не реже раза в месяц;
- электронный журнал – один раз в год;
- для технологической информации — не реже раз в полгода.

2.2. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

2.3. Дамп АСИОУ хранится на сервере в папке Архив.