

Инструкция
по порядку резервирования и восстановления работоспособности технических
средств и программного обеспечения, баз данных, средств защиты информации в
ИСПДн МБОУ ДО «Гавриловская школа искусств»

1. Общие положения

1.1. Инструкция по порядку резервирования и восстановления работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных (БД) и средств защиты информации (СЗИ) определяет действия, связанные с функционированием информационных систем персональных данных МБОУ ДО «Гавриловская школа искусств», меры и средства поддержания непрерывности работы и восстановления её работоспособности.

1.2. Целью настоящей Инструкции является превентивная защита элементов ИСПДн от утраты защищаемой информации. Задачами настоящей Инструкции является:

- определение способов и мер защиты от утраты информации;
- определение действий по восстановлению информации в случае утраты информации, восстановлению работоспособности ТС и ПО, БД и СЗИ в случае отказа их функционирования.

1.3. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн МБОУ ДО «Гавриловская школа искусств», администратора безопасности 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 копирования и хранения данных.

1.4. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к утрате защищаемой информации, является администратор безопасности ИСПДн МБОУ ДО «Гавриловская школа искусств».

1.5. Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к утрате защищаемой информации, назначается ответственный за организацию обработки персональных данных в МБОУ ДО «Гавриловская школа искусств».

2. Порядок реагирования на инциденты

2.1. В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же утратой защищаемой информации.

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.

2.2. Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале учёта нештатных ситуаций» (Приложение 1).

2.3. В сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники МБОУ ДО «Гавриловская школа искусств», предпринимают меры по восстановлению работоспособности. Предпринимаемые меры должны быть согласованы с ответственным за организацию обработки персональных данных.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Технические меры

3.1.1. К техническим мерам обеспечения непрерывной работы и восстановления могут относиться 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.

3.1.2. Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все помещения ИСПДн МБОУ ДО «Гавриловская школа искусств», в которых размещаются элементы ИСПДн и средства защиты должны быть оборудованы средствами пожарной сигнализации.

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.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные АРМ 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 и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

3.1.3. Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев могут использоваться методы кластеризации.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии, которые применяют дублирование данных, хранимых на дисках.

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

3.2. Организационные меры

3.2.1. Резервное копирование на отдельные носители и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2.2. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.2.3. Носители должны храниться в помещении оборудованном системой пожарной сигнализации.

3.2.4. Носители должны храниться не менее полугода для возможности восстановления данных.

4. Ответственность

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на администратора безопасности ИСПДн МБОУ ДО «Гавриловская школа искусств».

