УТВЕРЖДАЮ
Директор МАОУ СОШ № 31
_____ Е.В. Иванова
« 22 » сентября 2023г.

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных и средств защиты информации информационной системы персональных данных

Содержание

1. Назначение и область действия.

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и средств защиты информации (далее по тексту – СЗИ) определяет действия (далее по тексту – Инструкция), связанные с функционированием информационной системы персональных данных (далее по тексту – ИСПДн) в муниципальном автономном общеобразовательном учреждении города Калининграда средней общеобразовательной школы № 31 (далее – МАОУ СОШ № 31) меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей имеющих доступ к ресурсам ИСПДн МАОУ СОШ № 31, 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 год.

Ответственным сотрудником за реагирование и обеспечения мероприятий по предотвращению инцидентов безопасности, приводящие к потере защищаемой информации, назначается Администратор информационной безопасности.

2. Порядок реагирования на инцидент.

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

Все действия в процессе реагирования на Инцидент должны документироваться администратором информационной безопасности в «Журнале учета мероприятий по контролю обеспечения защиты персональных данных в ИСПДн».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование, предпринимает меры по восстановлению работоспособности.

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

3.1. Технические меры

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 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.

Все помещения, в которых размещаются элементы ИСПДн и средства защиты оборудованы средствами пожарной сигнализации.

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

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 и т. д.);

- резервные линии электропитания в пределах комплекса зданий;

- аварийные электрогенераторы.

Система резервного копирования и хранения данных, обеспечивают хранение защищаемой информации на твердый носитель (учтенный съемный носитель информации).

3.2. Организационные меры

Резервное копирование и хранение данных должно осуществлять 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).

Данные о проведение процедуры резервного копирования, отражаются в журнале по учету мероприятий по контролю обеспечения защиты персональных данных в ИСПДн.

Резервное копирование осуществляется на учтенный съемный носитель информации.

Носитель храниться в несгораемом шкафу.

Носитель хранится не менее года, 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 информационной безопасности.