26

Министерство образования и молодежной политики Свердловской области

государственное автономное профессиональное образовательное учреждение
Свердловской области
«Уральский горнозаводской колледж имени Демидовых»

Рассмотрено
на заседании Совета
автономного учреждения
№ протокола 3
«03» 07 2020 г.

Введено в действие приказом
№ 144-Д от «03» 07 2020г.

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ РЕЗЕРВИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ, ОБЩЕГО И ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ГАПОУ СО «УрГЗК»

Невьянск 2020

1.Общие положения

1.1. Настоящая Инструкция по организации резервирования и восстановления технических средств, общего и прикладного программного обеспечения, средств защиты информации в государственном автономном профессиональном образовательном учреждении Свердловской области «Уральский горнозаводской колледж имени Демидовых» (далее – Инструкция) определяет действия, связанные с функционированием информационных систем персональных данных (далее – ИСПДн) в государственном автономном профессиональном образовательном учреждении Свердловской области «Уральский горнозаводской колледж имени Демидовых» (далее – колледж), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью настоящей Инструкции является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

1.3. Задачами настоящей Инструкции является определение мер защиты от потери информации, определение действий восстановления в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, имеющих доступ к ресурсам ИСПДн, а также основным системам 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. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности ИСПДн.

1.6. Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается администратор безопасности ИСПДн.

2.Порядок реагирования на инцидент

2.1. Под инцидентом понимается происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. 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.

2.3 Все действия в процессе реагирования на Инцидент должны документироваться ответственным сотрудником в «Журнале по учету мероприятий по обеспечению защиты персональных данных».

2.4 В кратчайшие сроки, не превышающие одного рабочего дня, администратор безопасности и оператор ИСПДн, предпринимают меры по восстановлению работоспособности.

3. Меры обеспечения непрерывности работы и восстановления ресурсов

3.1.Технические меры.

3.1.1К 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.

3.1.2Системы жизнеобеспечения ИСПДн включают:

пожарные сигнализации и системы пожаротушения;

системы вентиляции и кондиционирования;

системы резервного питания.

3.1.3Помещения, в которых размещаются элементы ИСПДн должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.1.4Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.1.5Для 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.

3.1.6Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

3.1.7Для 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.

3.1.8Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2.Организационные меры

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

3.2.2. Данные о проведении процедуры резервного копирования, должны отражаться в журнале учета мероприятий по защите персональных данных.

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

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

3.2.5. Носители должны храниться не менее года, для возможности восстановления данных.

4. Ответственность

Ответственность за поддержание установленного в настоящей инструкции порядка по организации резервирования и восстановления программного обеспечения, баз персональных данных в информационных системах персональных данных Колледжа возлагается на администратора безопасности ИСПДн.