Прошнуровано, пронумеровано и скреплено

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 443D69C850FE3439BB58164A10FD2912
Владелец: Андреев Владимир Георгиевич
Действителен: с 29.03.2023 до 21.06.2024

УТВЕРЖДАЮ
Директор
МБУ ДО СШ "Витязь"
_____ В.Г. Андреев
"____" _____ 2024 г.

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в муниципальном бюджетном учреждении дополнительного образования спортивная школа "Витязь"

Назначение и область действия

1.1. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и системы защиты информации информационных систем персональных данных в муниципальном бюджетном учреждении дополнительного образования спортивная школа "Витязь", определяет действия, связанные с функционированием информационных систем персональных данных используемых в организации (далее соответственно – ТС, ПО, СЗИ, порядок, ИСПДн, организация), а также меры поддержания непрерывности работы и восстановления работоспособности ИСПДн.

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

1.3. Задачей настоящего порядка является:

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

1.4. Действие настоящего порядка распространения на всех пользователей организации, 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 копирования и хранения данных
- системы контроля физического доступа

1.5. Внесение изменений в настоящее положение осуществляется по мере необходимости.

1.6. В соответствии с распорядительным актом организации назначаются:

- сотрудник, ответственный за реагирование на инциденты безопасности, приводящие к потере защищаемой информации ИСПДн в организации (администратор, ответственный за систему защиты информации);
- сотрудник, ответственный за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации (администратор, информационной безопасности ИСПДн).

2. Порядок реагирования на инцидент

2.1. В настоящем порядке под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, представляемых 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 нарушений правил эксплуатации технических средств ИСПДн;
- в результате возникновения нештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником в "Журнале по учету мероприятий по контролю".

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники организации (администратор информационной безопасности, администратор и оператор ИСПДн), предпринимают меры по восстановлению работоспособности, которые согласовываются с руководителем организации.

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

3.1. Технические меры обеспечения непрерывной работы и восстановления, к которым относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, в том числе:

- системы жизнеобеспечения (пожарные сигнализации и системы пожаротушения, системы вентиляции и кондиционирования, системы резервного питания);
- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

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

3.1.2. 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.

3.1.3. 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.

3.1.4. 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 пр.)
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.
- 3.1.5. Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться следующие методы кластеризации:
- для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров;
- технология RAID.

3.1.6. 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.

3.1.7. Система 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 осуществиться на периодической основе, ответственными лицами в соответствии с распорядительным актом организации:

- 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 элименты ИСПДн – не реже раза в месяц, и каждый раз при внесении в эталонные копии (выход новых версий).

3.2.2. Данные о проведении процедуры резервного копирования должны отражаться в специально созданном журнале учета.

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 в помещении, оборудованном системой пожаротушения.

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

Администратор информационной безопасности

заместитель по директора безопасности М.В. Смирнова