УТВЕРЖДЕНО:
Директор ОГАУ ДО ОСШ по футболу
(наименование общеобразовательной организации)

_____ /А.Ю. Фомин/
подпись расшифровка подписи

Приказ № 37 от 09.01.2024 г.

Инструкция о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных.

Обозначения и сокращения.

В настоящем документе применяются следующие обозначения и сокращения:

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

БД – база данных

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

ИБ – информационная безопасность

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированных доступ

ОС – операционная система

ПДн – персональные данные

ПК – персональный компьютер

ПО – программное обеспечение

ПП – программный продукт

ПЭМиН – побочные электромагнитные излучения и наводки

СВТ – средства вычислительной техники

СЗПДн – система защиты персональных данных

СОВ – система обнаружения вторжений

ТС – технические средства

УБПДн – угрозы безопасности персональных данных

1.Общие положения.

1.1. Настоящая инструкция о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных (далее – инструкция) определяет действия, связанные с функционированием информационных систем персональных данных ОГАУ ДО ОСШ по футболу (далее – учреждение), меры и средства поддержания непрерывности работы и восстановления работоспособности информационных систем персональных данных.

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

1.3. Задачами настоящей инструкции являются:

- определение мер защиты от потери информации;

- определение действий для восстановления в случае потери информации.

1.4. Действие настоящей инструкции распространяется на всех пользователей учреждения, имеющих доступ к ресурсам ИСПДн, а также к основным системам обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения ИСПДн;

- системы резервного копирования и хранения данных;

-системы обеспечения отказоустойчивости;

-системы контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости.

1.6. Ответственным за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, является администратор ИСПДн.

1.7. Ответственным за контролем обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере

защищаемой информации, назначается ответственный за обеспечение безопасности персональных данных.

2. Порядок реагирования на инциденты.

2.1. В настоящей инструкции 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 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 администратором ИСПДн и передаваться ответственному за обеспечение безопасности персональных данных в виде служебной записки.

2.4. В срок, не превышающий одного рабочего дня, должны быть приняты меры по восстановлению работоспособности. Предпринимаемые меры, по возможности, должны согласовываться с вышестоящим руководством.

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 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.

3.1.2. Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;

- системы вентиляции и кондиционирования;

- системы резервного питания.

3.1.3. Все помещения учреждения, в которых располагаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации.

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

3.1.5. 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);

- резервные линии электропитания в пределах комплекса зданий;

- аварийные электрогенераторы.

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

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

3.1.8. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердом носителе (жестком диске и т.п.).

3.2 Организационные меры.

3.2.1. Резервное копирование 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 возобновляемому (однократному, эталонному) резервному копированию, 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 специально отведенном месте, доступ посторонних лиц к которому ограничен. Должна быть обеспечена целостность резервных носителей.

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

4. Ответственность.

4.1. 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 ответственного за обеспечение безопасности персональных данных.