Приложение 5
к приказу № 460 от 15.09.2020г.

Инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский»

1. Назначение и область действия

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее - Инструкция), связанные с функционированием ИСПДн, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский» (далее - МАДОУ).

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 МАДОУ, 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.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Ответственный за обработку ИСПДн МАДОУ.

2.Порядок реагирования на инцидент.

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также 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 ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю». В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники МАДОУ (Ответственный за обработку ПД, Операторы ИСПДн), предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

2.1. 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 обеспечения отказоустойчивости;

- 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 критичные помещения МАДОУ (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и по возможности, кондиционирования 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.

Системы обеспечения отказоустойчивости:

- кластеризация;

- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-O) применяют дублирование данных, хранимых на дисках. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

2.2. Организационные меры. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных - не реже раза в год;

- для технологической информации - не реже раза в полгода;

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). Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования. Носители должны храниться у ответственного лица (делопроизводитель). Носители должны храниться не менее года, для возможности восстановления данных.

3.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 Ответственного за обработку персональных данных.