УТВЕРЖДЕНО

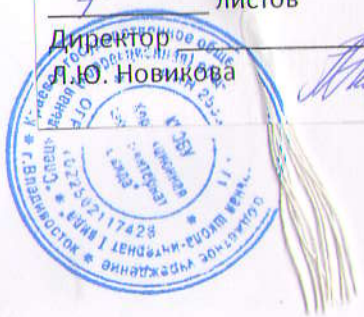
приказом директора
КГОБУ «Специальная (коррекционная)
школа – интернат I вида»

«28» 09 2016 года № 97-ОД

Порядок резервирования и восстановления ТС, ПО, СЗИ для краевого государственного общеобразовательного бюджетного учреждения «Специальная (коррекционная) школа – интернат I вида»

2016 год

Прошнуровано, пронумеровано
и скреплено печатью
7 листов
Директор
Л.Ю. Новикова



СОДЕРЖАНИЕ

Назначение и область действия

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее – Инструкция), связанные с функционированием ИСПДн краевого государственного общеобразовательного бюджетного учреждения «Специальная (коррекционная) школа – интернат I вида», (далее – Учреждение), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Задачей данного документа является:

определение мер защиты от потери информации;

определение действий восстановления в случае потери информации.

Действие настоящего документа распространяется на всех пользователей Учреждения, 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 Администратор ИСПДн _____

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор безопасности:

_____

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 ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Учреждения (Администратор безопасности, Администратор и Оператор ИСПДн), сотрудниками предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

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 критичные помещения Учреждения (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 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-0) 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.).

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).

Носители, на которые произведено резервное копирование, должны быть пронумерованы.

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

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

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