СОГЛАСОВАНО
решением педагогического Совета
ГБОУ школа № 661
Протокол № «4»
от 09.01.2018

УТВЕРЖДАЮ
Директор ГБОУ школа № 661
_____ / Е.А.Данилова
Приказ №
от 09.01.2018г.

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации

1. Назначение и область действия

1.1 Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее – Инструкция), связанные с функционированием ИСПДн ГБОУ школа № 661, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.
1.2 Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.
1.3 Задачей данной Инструкции является:
- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

1.4 Действие настоящей Инструкции распространяется на всех пользователей ГБОУ школа № 661, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:
- 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 ИСПДн.
1.6 Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор безопасности.

2. Порядок реагирования на инцидент

2.1 В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же 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 В кратчайшие сроки, не превышающие одной рабочей недели, ответственные за реагирование сотрудники ГБОУ школа № 661 (Администратор безопасности, Администратор и Оператор ИСПДн), предпринимают меры по восстановлению работоспособности ИСПДн.

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.

3.2 Все критичные помещения ГБОУ школа № 661 (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.3 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.

3.4 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 и т. д.).

3.5 Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердом носителе (оптический, жесткий диск и т.п.).

3.6 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).

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

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

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