Приложение 8
к приказу № 23/1 от 03.03.2017 г.

СОГЛАСОВАНО
от Представительного органа трудового коллектива БОУ «Чебоксарская общеобразовательная школа для обучающихся с ограниченными возможностями здоровья № 1» Минобразования Чувашии
_____ О.Н. Якимова
Протокол от «02» марта 2017 г. №1

УТВЕРЖДАЮ
Директор БОУ «Чебоксарская общеобразовательная школа для обучающихся с ограниченными возможностями здоровья № 1»
_____ В.Н. Тарасьев
Приказ от «03» марта 2017 г. № 23/1

ИНСТРУКЦИЯ
О ПОРЯДКЕ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ РАБОТОСПОСОБНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ В БОУ «ЧЕБОКСАРСКАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ №1» МИНОБРАЗОВАНИЯ ЧУВАШИИ

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации утвержденного».

1.2. Настоящая инструкция устанавливает основные требования к организации резервного копирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации (ТС и ПО, БД и СЗИ) и определяет порядок действий ответственных лиц, связанных с функционированием информационных систем (ИС), меры и средства поддержания непрерывности работы и восстановления работоспособности ИС.

1.3. Настоящая Инструкция разработана с целью

- определения категории информации, подлежащей обязательному резервному копированию;
- определения процедуры резервирования данных для последующего восстановления работоспособности информационных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

1.4. Целью настоящего документа является превентивная защита элементов ИС от предотвращения потери защищаемой информации.

Задачами данной инструкции являются:

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

1.5. Действие настоящей инструкции распространяется на всех пользователей БОУ «Чебоксарская общеобразовательная школа для обучающихся с ограниченными возможностями здоровья № 1» Минобразования Чувашии, имеющих доступ к ресурсам ИС, 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.

1.6. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

1.7. Ответственным сотрудником за реагирование на инциденты безопасности и контроль мероприятий по предотвращению инцидентов, приводящих к потере защищаемой информации, назначается Администратор безопасности информационных систем персональных данных (ИСПДн).

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 ИС;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником в «Журнал учета нештатных ситуаций ИС, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах ИС».

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники БОУ «Чебоксарская общеобразовательная школа для обучающихся с ограниченными возможностями здоровья № 1» Минобразования Чувашии, предпринимают меры по восстановлению работоспособности. Предпринимаемые меры, по возможности, согласуются с вышестоящим руководством.

3. Технические меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

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 обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа;
- системы жизнеобеспечения ИС.

1.2. Системы жизнеобеспечения ИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;

– системы резервного питания.

3.3. Все помещения БОУ «Чебоксарская общеобразовательная школа для обучающихся с ограниченными возможностями здоровья № 1» Минобразования Чувашии, в которых размещаются элементы ИС, материальные носители персональных данных и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, 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 рабочих станций и серверов;

– 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.

3.6. Для обеспечения отказоустойчивости критичных компонентов ИС при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИС должны использоваться территориально удаленные системы кластеров.

3.7. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на съемный носитель (ленту, жесткий диск и т.п.).

2. Организационные меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

2.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

– для обрабатываемых персональных данных – не реже одного раза в день инкрементальным способом, и не реже одного раза в неделю полный объем данных;

– для технологической информации – не реже одного раза в месяц;

– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

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

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

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

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

3. Ответственность

3.1. 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 администратора безопасности информации БОУ «Чебоксарская общеобразовательная школа для обучающихся с ограниченными возможностями здоровья № 1» Минобразования Чувашии.