Частное профессиональное образовательное учреждение
«Магнитогорский колледж современного образования»

Рассмотрено
на Педагогическом совете

Протокол № 5 от 20.04 2020

Принято
С учетом мнения родителей (законных представителей) и обучающихся
Советом колледжа

Протокол № 3 от 30.04 2020

Утверждено

Приказом № 25 от 11.05 2020

Директор ЧПОУ «Магнитогорский колледж современного образования»
_____ С.А. Кузьмина

ПОЛОЖЕНИЕ

О РЕЗЕРВИРОВАНИИ И ВОССТАНОВЛЕНИИ РАБОТОСПОСОБНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. БАЗ ДАННЫХ И СРЕДСТВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЧПОУ «МАГНИТОГОРСКИЙ КОЛЛЕДЖ СОВРЕМЕННОГО ОБРАЗОВАНИЯ»

Магнитогорск, 2020г.

1. Общие положения

1.1. Настоящее Положение разработано на основании:

- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящее Положение о резервировании и восстановлении работоспособности технических средств (далее – ТС) и программного обеспечения (далее – ПО), баз данных (далее – БД) и средств защиты персональных данных (далее – СЗПДн) определяет действия, связанные с функционированием информационных систем персональных данных образовательной организации (далее – информационная система), меры и средства поддержания непрерывности работы и восстановления работоспособности информационной системы.

1.3. Задачами настоящего Положения являются:

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

1.4. Действие настоящего Положения распространяется на всех сотрудников образовательной организации, имеющих доступ к ресурсам информационной системы, а также к основным системам обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций (далее – пользователи), в том числе к:

- системам жизнеобеспечения (включая системы пожарной сигнализации и пожаротушения, системы вентиляции и кондиционирования воздуха);
- системам обеспечения отказоустойчивости;
- системам резервного копирования и хранения данных;
- системам контроля физического доступа.

1.5. Лицо, ответственное за реагирование на инциденты, приводящие к потере защищаемой информации, назначается приказом руководителя образовательной организации.

1.6. Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов информационной системы, ТС, ПО, БД или СЗПДн, предоставляемых пользователям, а также потерей защищаемой информации.

2. Порядок реагирования на инцидент и восстановления работоспособности информационной системы

2.1. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;

- в результате нарушения правил эксплуатации ТС и ПО;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.2. Все действия в процессе реагирования на инцидент должны документироваться ответственным лицом в специальном журнале по учету мероприятий по контролю над соблюдением режима защиты персональных данных.

2.3. Реагирование на инцидент включает следующие этапы:

- выявление инцидента;
- анализ и принятие решений;
- принятие мер (технических и организационных) по устранению инцидента.

2.4. В сроки, не превышающие одного рабочего дня, ответственные лица предпринимают меры по восстановлению работоспособности ТС, ПО, СЗПДн и информационной системы.

2.5. Предпринимаемые меры согласуются с руководством образовательной организации в установленном порядке.

2.6. Восстановление работоспособности ТС, ПО, СЗПДн и информационной системы осуществляется в соответствии с эксплуатационной документацией.

2.7. В случае необходимости привлечения сторонних лиц и организаций, должна быть обеспечена невозможность их ознакомления с персональными данными.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

Технические меры:

3.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- пожарная сигнализация и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.2. Все помещения образовательной организации, в которых размещаются аппаратные элементы СЗПДн и информационной системы должны быть оборудованы средствами пожарной сигнализации и пожаротушения, системами вентиляции и кондиционирования воздуха.

3.3. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы информационной системы, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции, рабочие места пользователей должны подключаться к сети электропитания через источники бесперебойного питания.

3.4. В зависимости от необходимого времени работы ресурсов после потери питания могут быть применены такие варианты резервного электропитания как:

- 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, активное сетевое оборудование и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

3.5. К системам обеспечения отказоустойчивости относятся:

- кластеризация;
- технология RAID.

3.6. Для обеспечения отказоустойчивости могут использоваться следующие методы:

- для наиболее критичных компонентов информационной системы - территориально удаленные системы кластеров;
- для защиты отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации - технологии RAID (кроме RAID-0), которые применяют дублирование данных, хранимых на дисках.

Организационные меры.

3.7. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель.

3.8. Резервное копирование и хранение данных осуществляется на периодической основе:

- для обрабатываемых персональных данных – в соответствии с установленным порядком;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное ПО, программные СЗПДн), с которых осуществляется их установка на элементы информационной системы – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.9. Данные о проведение процедуры резервного копирования отражаются в специальном журнале учета.

3.10. Носители, на которые произведено резервное копирование, создаются, учитываются хранятся и уничтожаются в соответствии с Инструкцией по организации хранения, учета и работы с материальными носителями, содержащими конфиденциальную информацию и персональные данные.

3.11. Носители, на которые произведено резервное копирование хранятся не менее года, для сохранения возможности восстановления данных.

4. Ответственность

Пользователи и ответственные лица несут ответственность:

4.1. За неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящим Положением, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

4.2. За причинение материального ущерба работодателю – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

4.3. За правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным, гражданским законодательством Российской Федерации.

4.4. За обеспечение устойчивой работоспособности информационной системы.