СОГЛАСОВАНО
Председатель ПК
МБДОУ д/с №12
_____
Протокол №1 от 28.08.2020

УТВЕРЖДАЮ
Заведующий
МБДОУ д/с №12
_____ Н.А. Костенко
Приказ №77 от 28.08.2020

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах

1. Общие положения.
1.1. Настоящая инструкция разработана в МБДОУ д/с № 12 с целью организации порядка резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах (далее — ИС), и разработана на основании:
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации утвержденного».
1.2. Настоящая инструкция определяет порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации, и определяет порядок действий ответственных лиц, связанных с функционированием ИС в МБДОУ д/с № 12 меры и средства поддержания непрерывности работы и восстановления работоспособности ИС.
1.3. 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.
1.4. Действие настоящей инструкции распространяется на всех пользователей в МБДОУ д/с № 12, 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.
1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.
1.6. 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.
2. Порядок реагирования на инцидент.
2.1. В настоящем документе под инцидентом понимается происшествие, связанное со сбоем в функционировании элементов информационных систем персональных данных, предоставляемых пользователям информационных систем персональных данных, а также 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. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные. работники МБДОУ д/с № 12 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.

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:
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа;
- системы жизнеобеспечения ИС.
3.2. Системы жизнеобеспечения ИС включают:
- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания
3.3. Все помещения МБДОУ д/с № 12, в которых размещаются элементы ИС, материальные
носители персональных данных и средства защиты должны быть оборудованы средствами пожарной сигнализации и пожаротушения.
3.4. 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 их защиты от скачков напряжения;
- дублированные системы электропитания в устройствах;
- резервные линии электропитания в пределах комплекса зданий,
- аварийные электрогенераторы.
3.5. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на съемный носитель.

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

4.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:
- для обрабатываемых персональных данных — не реже раза в день инкрементальным способом, и не реже одного раза в неделю для полного объема данных;
- 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 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 в помещении, оборудованном системой пожаротушения.
45 Носители должны храниться не менее года для возможности восстановления данных.

5. Ответственность

5.1. 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 МБДОУ д/с № 12.

С инструкцией ознакомлен (а)

№	ФИО	Должность	Дата	Подпись
1	Затуло И.В	Вос-ль	11.01.2021	
2.	Фернина О.Б.	Вос-ль	11.01.2021	
3	Хакимзянова Н.Н.	Вос-ль	11.01.2021	
4.	Трещук Е.В	Б-ль	11.01.2021	
5	Клименко И.В	Муз. руководит.	11.01.2021	
6.	Мамонтова Ю.А.	Вос-ль	11.01.2021г	