

УТВЕРЖДАЮ
Заведующий
МБДОУ «Васьковский детский сад»
И.С. Литке
приказ № 68-1 от 14.03.2022г.



Инструкция по организации резервирования и восстановления программного обеспечения, баз защищаемой информации в информационной системе. МБДОУ «Васьковский детский сад»

1. Общие положения

1.1. Настоящая Инструкция по организации резервирования и восстановления программного обеспечения, баз защищаемой информации информационной системы МБДОУ «Васьковский детский сад» (далее – Инструкция) устанавливает основные требования к организации резервирования (резервного копирования) программ и информации, хранящейся в информационной системе МБДОУ «Васьковский детский сад» (далее – ИС), а также требования к их восстановлению, устанавливает ответственность за выполнение резервирования и восстановления.

1.2. Инструкция разработана в целях:

- определения перечня информационных ресурсов ИС, подлежащих резервному копированию;
- определения порядка и процедуры резервирования данных для последующего восстановления работоспособности ИС при полной или частичной потере данных, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- определения порядка восстановления резервируемых данных в случае возникновения такой необходимости;
- упорядочения работы должностных лиц, ответственных за обеспечение резервного копирования и восстановления данных.

1.3. Инструкция определяет последовательность резервного копирования и восстановления информации, в том числе персональных данных (далее – ПДн) при их обработке в ИС. Резервные копии, содержащие защищаемую информацию, указываются в «Журнале восстановления, учета создания и использования резервных копий защищаемой информации» (Приложение № 1) и «Плане резервного копирования» (Приложение № 2).

1.4. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИС в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

1.5. Администратор системы резервного копирования (далее – Администратор СРК) – работник, из числа системных администраторов, назначенный ответственным лицом за организацию резервного копирования и сохранение информационных ресурсов ИС, подлежащих резервированию.

1.6. Администратор безопасности – работник, с соответствующей квалификацией, осуществляющий обеспечение устойчивой работоспособности элементов ИС и средств защиты при обработке информации.

1.7. Общее руководство организацией и проведением мероприятий по порядку резервирования и восстановления в ИС осуществляет лицо, ответственное за защиту информации в ИС. Контроль мероприятий по резервированию и восстановлению в ИС осуществляет администратор безопасности ИС.

1.8. Техническое обеспечение, сопровождение и практическое решение задач, связанных с резервированием и восстановлением, применением различных схем резервирования информации и ПО осуществляет Администратор СРК.

1.9. Обеспечение резервирования и восстановления включает:

- регулярные профилактические работы;
- резервирование защищаемой информации и ПО;
- контроль безотказного функционирования ТС, ПО, каналов передачи информации, средств обеспечения функционирования ИС;
- принятие мер по восстановлению отказавших средств и их тестирование;
- принятие мер восстановлению информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала.

1.10. Основными мероприятиями, которые регламентируются, являются:

- резервное копирование данных;
- контроль резервного копирования;
- хранение резервных копий;
- полное или частичное восстановление данных.

1.11. При возникновении ситуаций, не включенных в положения настоящей Инструкции, решение принимается Администратором СРК по согласованию с лицом, ответственным за защиту информации в ИС, а в случае его отсутствия с администратором безопасности.

2. Обязанности администратора системы резервного копирования

2.1. Осуществляет настройку системы резервного копирования в зависимости от характера и объема информации, подлежащей резервному копированию.

2.2. Вводит в эксплуатацию систему резервного копирования.

2.3. Разрабатывает графики выполнения регламентных работ.

2.4. Осуществляет техническое сопровождение системы резервного копирования, что включает в себя:

- мониторинг системы резервного копирования;
- проведение регламентных работ в соответствии с разработанными графиками выполнения указанных работ;
- проведение ремонтных работ.

2.5. Формирует и ведет реестр резервных копий, согласно Приложению № 3 к настоящей Инструкции.

2.6. Формирует и ведет журнал событий согласно Приложению № 4 к настоящей Инструкции.

2.7. Вносит изменения в настройки системы резервного копирования в соответствии с данными журнала событий и при возникновении такой необходимости.

2.8. По истечении срока хранения резервной копии на внешнем носителе информации обеспечивает уничтожение данной резервной копии и запись новой резервной копии на указанном внешнем носителе информации, осуществив предварительную проверку его исправности; в случае неисправности внешнего носителя информации такой внешний носитель информации должен быть заменен новым исправным внешним носителем информации, а неисправный - уничтожен без возможности восстановления информации, записанной на нем.

2.9. Восстанавливает информацию с резервных копий в случае изменения или утраты указанной информации.

3. Резервируемые базы защищаемой информации и программное обеспечение. Порядок резервирования и хранения резервных копий

3.1. Обязательному резервированию подлежат:

- базы защищаемой информации (текстовые и табличные файлы, а также файлы баз данных специализированных программ);
- специальное (прикладное) программное обеспечение, используемое для обработки защищаемой информации;
- программное обеспечение средств защиты информации;
- общее программное обеспечение (операционные системы и программные драйверы устройств (принтер, монитор, видеокарта и т.п.), поставляемые со средствами вычислительной техники, входящими в состав ИС).

3.2. Порядок резервного копирования информационных ресурсов ИС включает следующую схему:

- периодическое ручное создание резервной копии данных, подлежащих резервному копированию, производимое во внерабочее время
- резервирование по письменному распоряжению начальника подразделения;

резервирование по письменному распоряжению лица, ответственного за защиту информации.

3.3. Максимальный срок хранения резервных копий информационных ресурсов ИС определен в Приложении № 3 настоящей Инструкции.

3.4. Резервное копирование данных в ИС осуществляется на носители информации, учтенные установленным порядком. Машинным носителям информации, содержащим резервную копию, присваивается уровень конфиденциальности в соответствии с уровнем конфиденциальности хранимой на них информации.

3.5. Резервное копирование ПО (ОС, штатное и специальное ПО) производится Администратором СРК при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

3.6. Резервное копирование ПО СЗИ производится администратором безопасности при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

4. Учет и хранение резервных копий

4.1. Учет всех носителей резервных копий осуществляется в соответствии с инструкцией об организации учета, хранения и выдачи машинных носителей информации в информационной системе МБДОУ «Васьковский детский сад»

4.2. Порядок учета резервных копий:

4.2.1. Учет резервных копий осуществляется в «Журнале восстановления, учета создания и использования резервных копий защищаемой информации» с указанием даты, времени начала и окончания операций копирования или восстановления данных, а также с приведением комментариев в случае их необходимости. Также в Журнале учитывается:

- создание копии по запросу;
- полное копирование в случае возникновения аварийных ситуаций.

4.2.2. Форма Журнала представлена в Приложении № 2 настоящей Инструкции.

4.2.3. Ответственным за ведение Журнала является Администратор СРК.

4.3. Порядок хранения резервных копий

4.3.1. Хранение носителей резервных копий, осуществляется в условиях, исключающих возможность хищения, изменения целостности или уничтожения содержащейся на них информации.

- 4.3.2. носители резервных копий краткосрочного хранения хранятся в помещениях, доступ к которым ограничен.
- 4.3.3. Срок хранения резервных копий определяется согласно Плану резервного копирования. В случае необходимости долгосрочного хранения резервных копий носители резервных копий передаются лицу, ответственному за защиту информации в ИС.
- 4.3.4. Допускается повторное использование носителей резервных копий по истечении срока хранения резервных копий.

5. Контроль результатов резервного копирования

5.1. Машинные носители, предназначенные для долгосрочного хранения информации, периодически проверяются на их пригодность и отсутствие сбойных секторов.

5.2. При появлении сбойных секторов на машинных носителях информация с этих носителей переносится на исправные. Неисправные носители уничтожаются установленным порядком.

5.3. Контроль результатов процедур резервного копирования информационных ресурсов, подлежащих резервированию, осуществляется Администратором СРК непосредственно после их окончания.

5.4. В случае обнаружения ошибки производится внеочередная попытка процедуры резервного копирования.

6. Ротация носителей резервной копии

6.1. В случае необходимости замены испорченных носителей информации новыми Администратором СРК производится оформление заявки на закупку новых носителей информации, идентичных испорченным.

6.2. Перед использованием в системе резервного копирования ИС, новые носители информации должны быть учтены установленным порядком и проверены средствами антивирусной защиты.

6.3. Испорченные носители информации передаются администратору безопасности ИС, затем уничтожаются в установленном порядке.

7. Порядок восстановления работоспособности информационной системы

7.1. Восстановление работоспособности ИС осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИС, а также ее программного обеспечения.

Восстановление работоспособности ИС осуществляется в течение одного дня.

7.2. Данные работы, в общем случае, осуществляются в следующей последовательности:

- проверка исправности и работоспособности средств обеспечения функционирования ИС;
- восстановление работоспособности (ремонт или замена) средств обеспечения функционирования ИС, при необходимости;
- проверка исправности и работоспособности средств вычислительной техники;
- восстановление работоспособности (ремонт или замена) средств вычислительной техники, при необходимости;
- проверка правильности функционирования общего программного обеспечения ИС;
- восстановление нормального функционирования общего программного обеспечения ИС с использованием дистрибутивов и обновлений к ним или резервных копий настроек, при необходимости;
- проверка правильности функционирования средств защиты информации;
- восстановление нормального функционирования средств защиты информации с использованием дистрибутивов и обновлений к ним, при необходимости;
- проверка правильности функционирования специального программного обеспечения ИС;
- восстановление нормального функционирования специального программного обеспечения ИС с использованием дистрибутивов и обновлений к ним, при необходимости;
- восстановление баз защищаемой информации с использованием резервной копии, при необходимости.

7.3. Данные работы осуществляются в соответствии с эксплуатационной документацией на технические и программные средства до полного восстановления работоспособности.

7.4. Работы по проверке правильности функционирования средств защиты информации и восстановлению нормального функционирования средств защиты информации осуществляются администратором безопасности ИС.

7.5. Восстановление защищаемой информации, созданной после ее последнего резервирования, осуществляется пользователями, осуществившими их внесение в базы защищаемой информации.

7.6. Работы по техническому обслуживанию технических и программных средств ИС осуществляются в соответствии с правилами, установленными в Инструкции о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации в ИС.

7.7. В случае необходимости привлечения для восстановления работоспособности ИС представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с защищаемой информацией, а

также несанкционированного копирования на машинные носители информации. Ответственность за выполнение данного требования возлагается на администратора безопасности ИС.

Разработчик инструкции заведующий
МБДОУ «Васьковский детский

сад»



Д.С.

Литке