

УТВЕРЖДАЮ

Директор

Муниципального учреждения

Дом культуры «Матыра»

Л.Л. Черепяхина

_____ 2025 г.



ИНСТРУКЦИЯ

по резервному копированию

Термины и определения

Автоматизированная система (АС) - Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Автоматизированное рабочее место (АРМ) - программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Безопасность информации [данных] - состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Носитель информации (НИ) - материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин ("Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)).

1. Общие положения

1.1. Настоящая инструкция разработана на основании следующих нормативных документов:

1.1.1. Федеральный закон от 27 июня 2006 № 152 «О персональных данных».

1.2. Настоящая инструкция регламентирует порядок использования систем резервного копирования, архивирования и восстановления информации.

1.3. Под резервным копированием понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационных систем (далее – ИС) в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных, обрабатываемых в ИС.

1.4. Контроль результатов всех процедур резервного копирования осуществляется Администратором информационной безопасности.

1.5. Настоящая Инструкция является дополнением к действующим регламентирующим документам в Организации и не исключает обязательного выполнения их требований.

2. Информационные ресурсы, принадлежащие резервированию

2.1. Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные каталоги) и групповая информация; информация, обрабатываемая пользователями в ИС, а также информация, необходимая для восстановления работоспособности ИС;
- рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИС;
- регистрационная информация системы информационной безопасности ИС;
- другая информация, по мнению пользователей, администратора информационной безопасности, являющаяся критичной для работоспособности ИС.

3. Порядок резервирования

3.1. Регламент резервного копирования для ИС определен следующими требованиями:

- состав и объем копируемых данных, необходимая периодичность проведения резервного копирования;
- максимальный срок хранения резервных копий;

— надежность и защищенность хранения резервных копий.

3.2. К носителям информации, содержащим резервные копии, а также к резервируемым программным средствам допускаются только работники МУ «ДК «Матыра».

3.3. О выявленных попытках несанкционированного доступа к резервируемой информации и аппаратным средствам, а также иных нарушениях информационной безопасности, произошедших в процессе архивирования (резервного копирования), сообщается администратору безопасности.

3.4. Предварительный учет съемных носителей резервных копий производится в отдельном журнале учета съемных носителей для резервного копирования, который находится у администратора безопасности.

3.5. Все съемные носители с резервными копиями маркируются, на них указывается предназначение носителя.

3.6. В случае неотделимости носителей резервной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

3.7. Хранение отдельных съемных носителей резервных копий организуется в отдельном от используемых данных помещении. Физический доступ к резервным копиям строго ограничен. Контроль за физическим доступом возлагается на администратора безопасности.

3.8. Доступ к носителям резервных копий имеют только системные администраторы ГИС, которые несут персональную ответственность за сохранность резервных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

3.9. Съемные носители для резервных копий изымаются для работы только системным администратором, непосредственно осуществляющим резервное копирование, под роспись в журнале учета носителей.

3.10. Уничтожение съемных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

3.11. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на администратора безопасности, осуществляющего резервное копирование.

3.12. Ответственность за контроль над своевременным осуществлением резервного копирования, а также за выполнением требований по хранению резервных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности.

3.13. В случае обнаружения попыток несанкционированного доступа к носителям резервной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается администратору безопасности в течение рабочего дня после обнаружения указанного события.

3.14. Резервное копирование специализированного программного обеспечения производится 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.

3.15. Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц.

4. Порядок хранения резервных копий

4.1. Информация, содержащаяся в постоянно изменяемых базах данных ИС, сохраняется в соответствии со следующим графиком:

ежедневно проводится копирование измененной и дополненной информации. Носители с ежедневной информацией должны храниться в течение недели;

— еженедельно проводится резервное копирование всей базы данных. Носители с еженедельными копиями хранятся в течение месяца;

— ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

4.2. Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.).

4.3. Контроль результатов всех процедур резервного копирования осуществляется администраторами ИС, в срок до конца рабочего дня, следующего за установленной датой выполнения этих процедур. В случае обнаружения ошибки результат сообщается администратору информационной безопасности.

4.4. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию.

4.6. Система резервного копирования обеспечивает возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивает восстановление текущей информации ИС в случае отказа любого из устройств резервного копирования.

4.7. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются администраторами ИС. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

5. Порядок восстановления персональных данных

5.1. В случае необходимости восстановление персональных данных из резервных копий производится администраторами ИС.

5.2. Восстановление персональных данных из резервных копий происходит в случае их исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев

5.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с дистрибутивных носителей в соответствии с инструкциями производителя.

5.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

5.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

5.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной копии.