



РАСПОРЯЖЕНИЕ ТШÖКТÖМ

20 ноября 2018 г.
с. Визинга, Республика Коми

№ 363 - р

Об организации резервного копирования

В целях совершенствования существующей организации обработки и защиты персональных данных в администрации муниципального района «Сысольский», а также исполнения Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных»:

1. Утвердить Инструкцию о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации согласно приложению 1.

2. Постоянно действующей комиссии по защите персональных данных определить ресурсы информационных систем персональных данных, подлежащие резервному копированию, его способы, периодичность и время проведения, а также сроки и места хранения резервных копий в соответствии с инструкцией, указанной в п.1.

3. Утвердить План резервного копирования (архивирования) ресурсов информационных систем персональных данных согласно приложению 2.

4. Ответственному за обеспечение работоспособности программного обеспечения и технических средств информационных систем персональных данных организовать процессы резервного копирования ресурсов информационных систем персональных данных в соответствии с планом, указанным в п. 3.

5. Контроль за исполнением распоряжения оставляю за собой.

Руководитель администрации

Р. В. Носков

Приложение № 1
к распоряжению администрации
муниципального района «Сысольский»
20 ноября 2018 г. № 363-р

ИНСТРУКЦИЯ

о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации

Сокращения

АРМ	- автоматизированное рабочее место;
БД	- база данных;
ИСПДн	- информационная система персональных данных;
Комиссия	- постоянно действующая комиссия по защите персональных данных;
МНИ	- машинный носитель информации;
ПДн	- персональные данные;
ПО	- программное обеспечение;
СКЗИ	- средство криптографической защиты информации;
Учреждение	- администрация МР «Сысольский»

1. Общие положения

1.1. Назначение документа

1.1.1. Инструкция определяет действия, связанные с функционированием ИСПДн Учреждения, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.1.2. Целью инструкции является превентивная защита ИСПДн и их компонентов от изменения, повреждения или утраты ПДн.

1.1.3. Задачами инструкции является:

- определение мер защиты от изменения, повреждения или утраты ПДн;
- определение порядка восстановления ПДн в случае их утраты, потери, уничтожения и искажения.

1.2. Область действия документа

1.2.1. Инструкция является руководящим документом лица, ответственного за восстановление работоспособности технических средств и ПО, БД и средств защиты информации по предотвращению несанкционированного или случайного изменения, повреждения или утраты ПДн, поддержанию непрерывности и восстановлению работы компонентов ИСПДн.

1.2.2. Действие инструкции распространяется на всех лиц, имеющих доступ к ресурсам ИСПДн, ответственных за работоспособность ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций.

1.3. Вступление в силу документа

1.3.1. Инструкция вступает в силу с момента ее утверждения руководителем Учреждения.

1.3.2. Изменения в инструкцию вносятся распоряжением руководителя Учреждения.

1.3.3. Пересмотр инструкции осуществляется по мере необходимости, но не реже одного раза в два года Комиссией.

2. Меры обеспечения непрерывности работы элементов ИСПДн

2.1. Основные системы обеспечения непрерывности работы элементов ИСПДн

2.1.1. К основным системам обеспечения непрерывности работы и восстановления компонент ИСПДн относятся программные, аппаратные и технические средства и системы, используемые для предотвращения сбоев функционирования элементов ИСПДн, такие как:

1) системы жизнеобеспечения:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного электропитания.

2) системы обеспечения отказоустойчивости:

- кластеризации;
- технологии RAID.
- 3) системы резервного копирования и хранения данных:
 - полного копирования;
 - дифференциального копирования;
 - инкрементного копирования;
 - зеркального копирования (двухсторонней синхронизации).

4) системы контроля и управления доступом.

2.2. Основные причины сбоев функционирования элементов ИСПДн

2.2.1. Сбои функционирования элементов ИСПДн, а также утрата или повреждение ПДн могут произойти в результате:

- преднамеренных действий пользователей ИСПДн;
- непреднамеренных действий пользователей ИСПДн;
- преднамеренных действий лиц, не допущенных к работе с ИСПДн;
- нарушения правил эксплуатации технических или программных средств ИСПДн;
- возникновения нештатных или чрезвычайных ситуаций.

2.3. Требования к организации работы ИСПДн

2.3.1. Все выделенные помещения, должны быть оснащены средствами пожарной сигнализации и пожаротушения.

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

2.3.3. Для предотвращения повреждения или утраты ПДн при кратковременном отключении электроэнергии или при перепадах напряжения в сети электропитания, все ключевые компоненты ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные АРМ и серверы должны быть подключены к сети электропитания через системы (средства) резервного электропитания. В зависимости от необходимого времени работы компонентов ИСПДн в условиях отсутствия основного электропитания, могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компонент ИСПДн;

- источники бесперебойного питания с дополнительной функцией защиты от перепадов напряжения;

- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

- резервные линии электропитания в пределах комплекса зданий;

- аварийные электрогенераторы.

2.3.4. Система резервного копирования и хранения данных, должна обеспечивать копирование и хранение ПДн на твердом носителе.

2.3.5. Для хранения резервных копий в ИСПДн допускаются только зарегистрированные (учтенные) МНИ.

2.3.6. В качестве резервных МНИ могут использоваться:

- Жесткие магнитные диски;

- Твердотельные накопители;

- Оптические диски;

- Внешние жесткие магнитные диски;

- Flash-накопители.

2.4. Порядок организации резервного копирования

2.4.1. В соответствии с Планом проведения резервного копирования (архивирования) ресурсов ИСПДн, а также исходя из условий функционирования ИСПДн, Комиссия определяет необходимый и достаточный объем резервных МНИ и их типы.

2.4.2. В каждой ИСПДн рекомендуется использовать отдельные резервные МНИ.

2.4.3. Резервные МНИ подключаются к серверам ИСПДн или ключевым АРМ.

2.4.4. В случае отсутствия локальной вычислительной сети между АРМ ИСПДн рекомендуется использовать отдельные резервные МНИ для каждого АРМ.

2.4.5. Допускается использование съемных МНИ (flash-накопителей и др.) в качестве резервных МНИ, при условии организации их хранения, исключающего НСД.

2.4.6. При необходимости, архивы резервных копий или файловая система резервного МНИ подлежат шифрованию с помощью СКЗИ.

2.4.7. Ежедневно или с иной, установленной Планом проведения резервного копирования (архивирования) ресурсов ИСПДн периодичностью, на резервные МНИ сохраняются резервные копии ПДн.

2.4.8. Доступ к архивам резервных копий ПДн должен быть ограничен.

2.4.9. Ответственный обязан периодически, но не реже одного раза в месяц проверять корректность создаваемых резервных копий БД и отдельных файлов.

2.5. Требования к организации резервного копирования

2.5.1. Резервному копированию подлежат следующие данные:

- обрабатываемые ПДн (БД, разрабатываемые работниками документы и т.д.) – ежедневно;

- технологическая информация (конфигурационные файлы устройств и оборудования) – разово после настройки, и каждый раз при внесении изменений;

- точки восстановления операционной системы – еженедельно, хранятся локально на каждом АРМ;

- эталонные копии ПО (операционные системы, штатное и специальное ПО, программные средства защиты), с которых осуществляется установка на элементы ИСПДн – разово, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

2.5.2. Средство и метод резервного копирования определяются Комиссией на основании Отчета о результатах проведения внутренней проверки обработки ПДн, в соответствии с Частным техническим заданием на создание системы защиты ПДн, и согласуются с руководителем Учреждения и руководителями структурных подразделений (при необходимости).

2.5.3. Периодически, не реже одного раза в два месяца, Ответственный проводит актуализацию Плана проведения резервного копирования (архивирования) ресурсов ИСПДн. С этой целью он проводит опрос руководителей структурных подразделений и работников, участвующих в автоматизированной обработке ПДн на предмет выявления изменений в структуре обработки ПДн, изменения мест хранения ПДн, изменении состава ПО, обрабатывающего ПДн и т.д. Актуализированный План проведения резервного копирования (архивирования) ресурсов ИСПДн, утверждается руководителем Учреждения.

2.5.4. На резервных МНИ должны создаваться отдельные разделы (каталоги) для каждого структурного подразделения, АРМ или сервера: имя раздела (каталога) должно содержать название структурного подразделения, АРМ или сервера; названия резервных копий должны содержать дату проведения резервного копирования и его тип.

2.5.5. Если на одном АРМ работает несколько пользователей, то личные файлы и документы каждого из них должны храниться отдельно, а в названиях резервных копий должны содержаться имена (идентификаторы) пользователей.

2.5.6. Съёмные или заполненные резервные МНИ должны храниться в негорючем шкафу, сейфе или в помещении, оборудованном системой пожаротушения.

2.5.7. В зависимости от типа данных (БД субъектов ПДн, бухгалтерские отчеты, документы в формате Документ Word и т.д.), должно храниться от 3 до 12 актуальных полных резервных копий для возможности восстановления информации за последний квартал.

2.5.8. Срок хранения заполненных резервных МНИ составляет 5 лет. После истечения установленного срока хранения резервные МНИ подлежат очистке или уничтожению в соответствии с Регламентом учета, хранения и уничтожения МНИ.

2.5.9. По решению Комиссии для отдельных резервных МНИ может устанавливаться особый срок хранения, в зависимости от содержащейся на них информации.

2.6. Требования к организации восстановления работоспособности элементов ИСПДн

2.6.1. Все действия в процессе восстановления работоспособности технических средств и ПО, БД и средств защиты информации должны документироваться Ответственным в Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки и модификации программных и технических средств в ИСПДн.

2.6.2. В кратчайшие сроки, не превышающие одного рабочего дня, Ответственный предпринимает все необходимые меры по восстановлению работоспособности элементов ИСПДн. Предпринимаемые меры при необходимости согласуются с руководителем Учреждения.

3. Ответственность

3.1. Комиссия несет ответственность за выбор средств и методов резервного копирования.

3.2. Ответственный несет персональную ответственность, за качество и своевременность выполнения задач и функций, возложенных на него в соответствии с настоящей инструкцией.

3.3. Администратор ИСПДн несет персональную ответственность за установку и настройку средств резервного копирования.

Приложение № 2
к распоряжению администрации
муниципального района «Сысольский»
20 ноября 2018 г. № 363-р

ПЛАН

проведения резервного копирования (архивирования) ресурсов информационных систем
персональных данных

№ п / п	Наименование ресурса	Расположение ресурса	Тип резервного копирования	График проведения	Количество копий на хранении	Место хранения резервной копии	Примечание
1	2	3	4	5	6	7	8
1. Базы данных программного обеспечения обработки персональных данных							
1	АС Смета 3.1	\\server1	Полное	Ежедневно: 5:40	12	Съемный носитель информации\\backup\Smeta	
2	НалогоплательщикЮЛ	\\glbuhadm	Добавочное	Ежедневно: 12:40	9	Съемный носитель информации	
3	Документы ПУ	\\glbuhadm	Полное	Раз в 2 недели, Ср: 12:00	6	Съемный носитель информации	
2. Места хранения электронных документов							
4	Рабочий стол	АРМ ИСПДн Кадры	Полное	Ежемесячно, Пн: 12:00	3	Съемный носитель информации	Только текстовые файлы
5	Рабочий стол	АРМ ИСПДн Бухгалтерия	Добавочное	Ежедневно: 11:45	24	Съемный носитель информации	Только текстовые файлы
6	Мои документы	АРМ ИСПДн Делопроизводство	Полное	Ежемесячно, Пн: 12:00	3	Съемный носитель информации	Только текстовые файлы
7	Мои документы	АРМ ИСПДн Жилье	Добавочное	Ежедневно: 11:45	24	Съемный носитель информации	Только текстовые файлы
8	Мои документы	АРМ ИСПДн Управление имуществом	Добавочное	Ежедневно: 11:45	24	Съемный носитель информации	Только текстовые файлы
3. Точки восстановления операционных систем							
9	Microsoft Windows	АРМ ИСПДн	Точка восстановления	При изменении конфигурации	-	Локально	Системный диск