|  |  |  |
| --- | --- | --- |
|  | Приложение № 2 | |
|  | Утверждено | |
|  | Распоряжением от 26.02.2020 | № 4-р |

**ИНСТРУКЦИЯ**

**о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в администрации Мичуринского сельского поселения Динского района**

# Назначение и область действия

## Данная Инструкция определяет действия, связанные с мерами и средствами поддержания непрерывной работы и восстановления работоспособности информационных систем в аадминистрации Мичуринского сельского поселения Динского района (далее – Администрация).

## Настоящая Инструкция регламентирует:

* меры защиты от потери информации;
* действия по восстановлению в случае потери информации.

## Действие настоящей Инструкции распространяется на Администраторов информационных систем, ответственных за резервное копирование информации.

# Меры обеспечения надежной работы и восстановления ресурсов при возникновении инцидентов

## Технические меры.

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 ИСПДн включают:

* пожарные сигнализации и системы пожаротушения;
* системы вентиляции и кондиционирования;
* системы резервного питания.

Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, 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 компьютеров;
* источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
* резервные линии электропитания в пределах комплекса зданий;

Система резервного копирования и хранения данных, должна обеспечивать хранение [защищаемой информации](file:///C:\AppData\Local\Temp\доки%20в%20рекомендации%20УИ\Мои%20рекомендации\приложения%20к%20рекомендациям\Приложение%206%20Перечень%20персональных%20данных,%20подлежащих%20защите.doc) на носитель (ленту, жесткий диск и т.п.).

## Организационные меры.

### Резервное копирование и хранение данных должно осуществлять на периодической основе:

* для обрабатываемых персональных данных – не реже раза в неделю или по требованию пользователя ИСПДн;
* для системной 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 ИСПДн каждый раз при внесении изменений в эталонные копии (выход новых версий).

### Данные о проведение процедуры резервного копирования должны отражаться в специально созданном Журнале учета.

### Носители, на которые произведено резервное копирование, должны быть пронумерованы номером носителя, датой проведения резервного копирования.

### Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

### Носители и резервные копии данных должны храниться не менее года для возможности восстановления данных.

# Порядок проведения резервирования информации

## Перед проведением процедуры резервного копирования необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

## Резервирование информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

## Все файлы, входящие в состав резервной копии, должны архивироваться в один архив с присвоением имени архива в формате время\_дата (например 18.00\_21.11.2011).

## Архивация может производиться как штатными средствами, поставляемыми в составе специализированного программного обеспечения для построения информационной системы, так и сторонним программным обеспечением (например 7zip, WinRar).

## Резервные копии должны сохраняться на носители, не входящие в состав технических средств информационной системы персональных данных (внешние жесткие диски, CD/DVD диски, flash диски).

## После завершения процедуры резервного копирования информации и записи резервной копии на носитель, необходимо поместить носитель с резервной копией в специально отведённое для хранения место и проставить соответствующую отметку в Журнале.

# Порядок проведения восстановления информации

## Перед проведением процедуры восстановления информации необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

## Восстановление информации следует проводить из наиболее актуальной резервной копии.

## В случае, если специализированное программное обеспечение для построения информационной системы не позволяет работать с заархивированными резервными копиями, то перед восстановлением информации необходимо разархивировать файлы резервной копии при помощи стороннего программного обеспечения (например 7zip, WinRar).

## Восстановление информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

## После завершения процедуры восстановления необходимо убедиться в работоспособности информационной системы персональных данных.

## В случае успешного восстановления оповестить пользователей информационной системы о возможности продолжения работы. В противном случае необходимо изучить документацию, прилагаемую к программному обеспечению либо обратиться в службу технической поддержки.

# Ответственность

## Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

**С настоящей Инструкцией ознакомлен:**

|  |  |  |
| --- | --- | --- |
| Должность | Фамилия Имя Отчество | Дата и подпись |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |