Приложение 10
Утверждены
постановлением Администрации
Ребрихинского района Алтайского края

от 28.12.2018 №745

ИНСТРУКЦИЯ
по организации резервного копирования информации в информационных системах Администрации Ребрихинского района Алтайского края

1. Общие положения

1.1. Данная инструкция определяет порядок организации резервного копирования информации, обрабатываемой в информационных системах Администрации Ребрихинского района Алтайского края (далее – «ИС»), меры поддержания непрерывности работы ИС и восстановления их работоспособности.

1.2. Задачей данной инструкции является:

определение необходимых мероприятий по защите ИС от потери информации;

определение необходимых действий по восстановлению информации ИС в случае ее потери.

1.3. Действие настоящей инструкции распространяется на начальника отдела информатизации Ребрихинского района (далее - на администратора безопасности ИС), а в его отсутствие на замещающих его лиц и всех пользователей ИС.

1.4. Пересмотр настоящей инструкции осуществляется по мере необходимости руководителем подразделения или лицом, ответственным за обеспечение информационной безопасности.

1.5. Ответственность за обеспечение мероприятий по предотвращению инцидентов, приводящих к потере информации, возлагается на администратора безопасности ИС.

1.6. Контроль за реагированием на инциденты безопасности, приводящие к потере защищаемой информации, возлагается на руководителя подразделения или лицо, ответственное за обеспечение информационной безопасности.

2. Порядок резервирования информации

2.1. Система резервного копирования и хранения данных должна обеспечивать сохранность информации на носителях информации, не участвующих в ее обработке.

2.2. Резервное копирование данных должно осуществляться на периодической основе:

для обрабатываемой информации – не реже одного раза в неделю;

для технологической информации – не реже одного раза в 6 месяцев.

Процесс резервного копирования должен отражаться в журнале системы резервного копирования и хранения данных.

Администратор безопасности ИС должен контролировать наличие резервных копий не реже одного раза в месяц.

2.3. Носители, на которые произведено резервное копирование, должны быть учтены соответствующим образом.

2.4. Для обеспечения возможности восстановления данных резервные копии должны храниться не менее недели.

2.5. Для защиты от неисправностей носителей информации на ПЭВМ, осуществляющих обработку и хранение информации, могут применяться технические средства, основанные на RAID-технологии (кроме RAID-0), в которой применяется дублирование информации.

2.6. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также ПЭВМ 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 для защиты отдельных ПЭВМ;

источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

дублирующие системы электропитания.

3. Реагирование на инцидент

3.1. Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании ИС, предоставляемых пользователям ИС, а также потеря информации.

3.2. Инцидент может произойти:

в результате непреднамеренных действий пользователей ИС;

в результате преднамеренных действий пользователей ИС или третьих лиц;

в результате нарушения правил эксплуатации технических средств ИС;

в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

3.3. В сроки, не превышающие 3 рабочих дня, администратором безопасности ИС применяются меры по восстановлению работоспособности ИС. Предпринимаемые меры в случае необходимости согласуются с руководителем подразделения, ответственного за администрирование ИС.

4. Восстановление информации из резервных копий

4.1. Работы по восстановлению данных из резервных копий производятся администратором безопасности ИС.

4.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в ИС, воздействия вредоносного программного обеспечения, ошибок программного обеспечения, ошибок пользователей ИС и аппаратных сбоев.

4.3. Восстановление программного обеспечения производится с носителей, входящих в комплект поставки, или их резервных копий в соответствии с технической документацией на данное программное обеспечение.