|  |
| --- |
| Приложение 16  к распоряжению Администрации Заринского района  от \_\_\_\_\_\_\_\_\_\_\_\_ №\_\_\_\_\_\_\_\_ |

**РЕГЛАМЕНТ**

резервного копирования информации

в Администрации Заринского района Алтайского края

1. **Перечень использованных сокращений, единиц и терминов**

АИБ – администратор информационной безопасности.

ИБ – информационная безопасность.

ИС – информационная система.

НСД – несанкционированный доступ.

ОС – операционная система.

ПО – программное обеспечение.

СУБД – система управления базами данных.

1. Общие положения
   1. Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся на серверах и рабочих станциях, обрабатывающих персональные данные и защищаемую информацию, Администрации Заринского района Алтайского края (далее – Администрация района) разработан с целью:

* определения порядка резервирования данных для последующего восстановления работоспособности ИС при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения (ПО), ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
* определения порядка восстановления информации в случае возникновения такой необходимости;
* упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации.
  1. В настоящем документе регламентируются действия при выполнении следующих мероприятий:
* резервное копирование;
* контроль резервного копирования;
* хранение резервных копий;
* полное или частичное восстановление данных и приложений.

2.3. Резервному копированию подлежит информация следующих основных категорий:

* персональная информация пользователей (личные каталоги на файловых серверах);
* групповая информация пользователей (общие каталоги отделов);
* информация, необходимая для восстановления серверов и систем управления базами данных (СУБД);
* конфигурация средств защиты информации;
* персональные профили пользователей;
* информация информационных систем, в т.ч. баз данных;
* справочно-информационная система общего использования («Гарант», «Консультант+» и т.п.);
* рабочие копии установочных компонентов ПО рабочих станций.

1. **Порядок резервного копирования**
   1. Резервное копирование производится на основании следующих данных:

* состав и объем копируемых данных, периодичность проведения резервного копирования (из Перечня резервируемых данных);
* максимальный срок хранения резервных копий -3 месяца;
* минимальный срок хранения резервных копий – 1 месяц;
* хранению подлежат 3 последних резервных копии.
  1. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне резервируемой информации, в установленные сроки и с заданной периодичностью.
  2. О выявленных попытках несанкционированного доступа (НСД) к резервируемой информации, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, ответственный сотрудник сообщает администратору информационной безопасности.

1. **Методика резервного копирования**
   1. Для организации системы резервного копирования используются штатные средства ОС и используемого ПО. С целью оптимизации расходов на развёртывание системы резервного копирования, запись резервной копии осуществляется на специальный внешний носитель.
   2. С помощью указанного ПО выполняются такие действия, как задание режимов и составление расписания резервного копирования клиентов, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации.
   3. Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации проводятся в ночное время. Существуют три набора резервных копий:

* месячный набор. Записывается информация (Образ-файл, содержащий в себе полную копию содержания и структуры) на первые числа текущего месяца. Срок хранения –3 месяца. Хранится на внешнем жёстком диске и съёмном жёстком диске, который по отдельному расписанию выносится за пределы офиса;
* двухнедельная копия. Записывается данные за две недели. Срок хранения – 1 месяц. Хранится на внешнем жёстком диске и съёмном жёстком диске, который по отдельному расписанию выносится за пределы офиса;
* ежедневная копия. Записывается ежесуточно. Срок хранения – 1 месяц. Записывается на внешнем жёстком диске.

Различаются три принципиально разных источника информации, подлежащей резервированию:

* информация, хранимая непосредственно на файловом сервере;
* базы данных информационной системы;
* системные файлы серверов (Образ).
  1. Для резервирования информации, хранимой непосредственно в файловых системах и информации, хранимой в базах данных Прикладных информационных систем, используется штатные средства ПО, посредством которой формируются задания на проведение резервного копирования информации, находящейся в каталогах файлового сервера. При этом указывается срок хранения информации и периодичность выполнения резервного копирования.
  2. При создании задания на создание образа системных дисков серверов указывается срок хранения информации и периодичность выполнения резервного копирования.

1. **Контроль результатов резервного копирования**
   1. Контроль результатов всех процедур резервного копирования осуществляется ответственными должностными лицами, в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур. В случае обнаружения ошибки ответственное лицо сообщает администратору информационной безопасности до 17 часов текущего рабочего дня. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.
2. **Ротация носителей резервной копии**
   1. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации в случае отказа любого из устройств резервного копирования.
   2. В качестве новых носителей информации допускается повторное использование тех, у которых срок хранения содержащейся информации истек.
   3. Персональные данные с носителей, которые перестают использоваться в системе резервного копирования, должны стираться с составлением Акта.
3. **Восстановление информации из резервных копий**
   1. В случае необходимости восстановление данных из резервных копий производится на основании Заявки владельца информации на имя \*Должность руководителя организации (РП)\* при согласовании с АИБом.
   2. После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.