|  |  |
| --- | --- |
|  | Приложение 21  к приказу комитета  по культуре города Барнаула  от 29 июля 2021г. №64 |

РЕГЛАМЕНТ

резервного копирования информации

Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

ИБ – информационная безопасность.

НСД – несанкционированный доступ.

ОС – операционная система.

ПО – программное обеспечение.

СУБД – система управления базами данных.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ИС, в том числе ИСПДн, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

1. Общие положения

1.1. Регламент резервного копирования информации (далее – Регламент), хранящихся на серверах и рабочих станциях, обрабатывающих КИ, в том числе ПДн, комитета по культуре города Барнаула (далее – комитет) разработан с целью:

определения порядка резервирования данных для последующего восстановления работоспособности ИСПДн 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.

1.2. Регламент определяет действия при выполнении следующих мероприятий:

резервное копирование;

контроль резервного копирования;

хранение резервных копий;

полное или частичное восстановление данных и приложений.

1.3. 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);

персональные профили пользователей сети;

информация автоматизированных систем, в т.ч. баз данных.

2. Порядок резервного копирования

2.1. 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;

резервное копирование осуществляется 1 раз в месяц.

2.2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне резервируемой информации, в установленные сроки и с заданной периодичностью.

2.3. О выявленных попытках НСД к резервируемой информации, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, ответственный сотрудник сообщает АИБу.

3. Методика резервного копирования

3.1. 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.

3.2. 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.

3.3. 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.

4. Контроль результатов резервного копирования

4.1. 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 ответственной лицо сообщает АИБу 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.

5. Ротация носителей резервной копии

5.1. 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.

5.2. В качестве новых носителей информации допускается повторное использование тех, у которых срок хранения содержащейся информации истек.

5.3. Персональные данные с носителей, которые перестают использоваться в системе резервного копирования, должна.

6. Восстановление информации из резервных копий

6.1. В случае необходимости восстановление данных из резервных копий производится на основании Заявки владельца информации на имя ответственного сотрудника.

6.2. После поступления заявки восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.