|  |
| --- |
| Приложение 5 к Положению об обеспечении безопасности общедоступной информации в информационных системах комитета по финансам, налоговой и кредитной политике города Барнаула |

**РЕГЛАМЕНТ**

резервного копирования информации

в комитете по финансам, налоговой и кредитной политике города Барнаула

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

АИБ – администратор информационной безопасности.

ИБ – информационная безопасность.

ИСПДн – информационная система персональных данных.

НСД – несанкционированный доступ.

ОС – операционная система.

ПО – программное обеспечение.

СУБД – система управления базами данных.

Администратор информационной безопасности – специалист отдела внедрения автоматизированных систем финансовых расчетов, осуществляющий контроль за обеспечением защиты информации в ИС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

1. Общие положения
   1. Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся на серверах и рабочих станциях, обрабатывающих персональные данные, Комитета по финансам, налоговой и кредитной политике города Барнаула 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. В настоящем документе регламентируются действия при выполнении следующих мероприятий:
* резервное копирование;
* контроль резервного копирования;
* хранение резервных копий;
* полное или частичное восстановление данных и приложений.

1. **Порядок резервного копирования**
   1. Резервному копированию в соответствии с регламентом подлежит информация, определенная в перечне резервируемой информации (приложение 1).
   2. Резервное копирование выполняется в автоматическом режиме, с периодичностью один раз в сутки, в нерабочее время.
   3. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне резервируемой информации, в установленные сроки и с заданной периодичностью.
   4. Максимальный срок хранения резервных копий - 6 месяцев.
   5. О выявленных попытках несанкционированного доступа (НСД) к резервируемой информации, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, ответственный сотрудник сообщает ответственному за обеспечение информационной безопасности.
2. **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.
   4. 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.
   5. При создании задания на создание образа системных дисков серверов указывается срок хранения информации и периодичность выполнения резервного копирования.
3. **Контроль результатов резервного копирования**
   1. Контроль результатов всех процедур резервного копирования осуществляется сотрудниками отдела внедрения автоматизированных систем финансовых расчетов, в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур. В случае обнаружения ошибки сотрудник отдела, обнаруживший ошибку, сообщает об этом 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.
4. **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 случае необходимости замены испорченных носителей информации новыми, специалист отдела внедрения автоматизированных систем финансовых расчетов, отвечающий за системное администрирование, заблаговременно, за 10 рабочих дней согласовывает с АИБом спецификации новых носителей информации. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также перемещение их, специалист отдела внедрения автоматизированных систем финансовых расчетов, отвечающий за системное администрирование, выполняет в присутствии АИБа.
   3. В качестве новых носителей информации допускается повторное использование тех, у которых срок хранения содержащейся информации истек.
   4. Персональные данные с носителей, которые перестают использоваться в системе резервного копирования, должна стираться с составлением акта об удалении информации (остаточной), хранившейся на диске компьютера (приложение 2).
5. **Восстановление информации из резервных копий**
   1. Полное или частичное восстановление информации производится по обращению сотрудников комитета, включенных в список постоянных пользователей информационных систем персональных данных.
   2. Частичное восстановление информации производится АИБом по месту размещения резервируемой информации, указанному в перечне резервируемой информации непосредственно в момент обращения.
   3. В случае необходимости, восстановление данных из резервных копий производится в максимально сжатые сроки, ограниченные техническими возможностями системы.
   4. Полное восстановление информации, относящейся к одному информационному ресурсу, осуществляется в течении рабочего дня.
   5. Полное восстановление информации, относящейся к нескольким информационным ресурсам, осуществляется в порядке актуальности информационных ресурсов, согласованном с начальником отдела внедрения автоматизированных систем финансовых расчетов.
   6. Полное восстановление информации, относящейся к нескольким информационным ресурсам, осуществляется в течении двух рабочих дней.