|  |  |
| --- | --- |
|  | Приложение 4 к приказу комитета по культуре города Барнаулаот 29 июля 2021 г.№64 |

ОПИСАНИЕ

технологического процесса обработки информации

в информационных системах

Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

КИ – конфиденциальная информация.

ИС – информационная система.

ЛВС – локальная вычислительная сеть.

МНИ – отчуждаемые машинные носители информации.

НСД – несанкционированный доступ.

ОИ – объект информатизации.

ПДн – персональные данные.

ПО – программное обеспечение.

ПЭВМ – персональная электронно-вычислительная машина.

СЗИ – средство защиты информации.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор сети – сотрудник или группа сотрудников, который выполняет функции администратора информационной безопасности, осуществляющие непосредственную организацию и выполнение работ по созданию (модернизации), техническому обслуживанию и управлению (администрированию) информационной управляющей ЛВС, включая технические аспекты информационной безопасности.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная безопасность – состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в организации.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения различных задач подразделений. В организации используются различные типы информационных систем для решения различных задач.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий, используемая в процессах организации.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Локальная вычислительная сеть (ЛВС) – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Операционная система – системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью ЭВМ.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь ЛВС – сотрудник комитета по культуре города Барнаула (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т. п.), зарегистрированный в корпоративной сети в установленном порядке и получивший права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Сервер – выделенный компьютер, имеющий разделяемые ресурсы, выполняющий определенный перечень задач и предоставляющий пользователям ЛВС ряд сервисов.

1. Общие положения

Описание технологического процесса обработки информации в ИС, в том числе ИСПДн (далее – ИС) комитета по культуре города Барнаула (далее – комитет) разработано в соответствии с Федеральным законом от 26.07.2007 № 152-ФЗ «О персональных данных».

2. Назначение. Решаемые задачи

2.1. ИС комитета предназначены для разработки, распечатки, хранения информации в электронном виде КИ, в том числе ПДн (далее – КИ).

2.2. С документами, содержащими сведения ограниченного распространения, работают сотрудники комитета, имеющие соответствующую форму допуска и доступ к ресурсам ИС, в том числе ИСПДн.

2.3. Технологический процесс обработки информации в ИС включает в себя:

внесение КИ в базы данных, просмотр и редактирование необходимой информации, печать документов на бумажном носителе, обмен файлами на МНИ по каналам связи;

обеспечение необходимого уровня безопасности обработки, хранения и передачи КИ.

2.4. Основными задачами применения ИС являются:

работа с базами данных КИ внесение в них изменений, их хранение и уничтожение;

работа с файлами конфиденциальных документов;

подготовка и работа с МНИ для передачи их по каналам связи;

распечатка документов, содержащих КИ;

размножение необходимого числа экземпляров документов на принтере;

обеспечение необходимого уровня безопасности обработки, хранения КИ;

обеспечение в ИС разграничения доступа к КИ;

антивирусная защита программной среды и данных;

регистрация пользователей СЗИ от НСД перед началом сеанса работы на ПЭВМ, входящей в состав ИС, назначение им прав доступа к защищаемым ресурсам;

резервное копирование информации на МНИ, учтенные в установленном порядке в соответствии с требованиями Инструкции по организации работы с электронными носителями конфиденциальной информации;

восстановление информации, поврежденной или стертой при сбоях в работе ПЭВМ с резервных копий.

3. Расположение ОИ. Организация охраны и контроля доступа

3.1. ИС, обрабатывающие КИ, расположены в зданиях по адресу 656056, Алтайский край, г Барнаул пр-кт Ленина д. 6.

3.2. Помещения комитета оборудованы техническими средствами защиты (сигнализация), ведется физическая охрана помещений.

3.3. Доступ сотрудников и других лиц в помещения комитета, в которых осуществляется обработка КИ, осуществляется в соответствии с утвержденным списком лиц, имеющих доступ к КИ.

4. Состав информационной системы, обрабатывающей конфиденциальную информацию, и информационных систем персональных данных

4.1. В состав ИС комитета, обрабатывающих КИ, входят АРМ, которые функционируют в рамках локальной сети и имеют подключение к сети Интернет.

5. Источники данных

5.1. Источниками данных для ИС комитета являются:

данные на бумажных носителях;

данные на МНИ-файлы, передаваемые из другой ИС;

вводимые сотрудниками данные – сведения, вводимые с клавиатуры операторами (пользователями).

6. Входные данные

6.1. Входными данными является информация, поступающая в ИС на различных носителях: данные на бумажных носителях, данные на МНИ, данные, вводимые операторами (пользователями) с клавиатуры.

6.2. Исходные данные поступают в ИС комитета от сотрудников, сторонних организаций и физических лиц, обращающихся в комитет.

6.3. Все носители информации регистрируются, хранятся и передаются в соответствии с требованиями Инструкции по организации работы с электронными носителями конфиденциальной информации.

7. Выходные данные ИС

7.1. Выходными данными являются подготовленные и распечатанные в ИС конфиденциальные и не конфиденциальные текстовые документы, файлы, передаваемые по каналам связи.

7.2. Используемые программные средства:

на ПЭВМ комитета установлены Windows 7 Professional 32bit, Windows 7 Professional 64bit, Windows 10 Pro 32bit, Windows 10 Pro 64bit. Дистрибутивы версий ОС хранятся у АИБа.

7.3. Функции, права и обязанности ответственных за эксплуатацию объекта информатизации регламентируются Инструкцией по техническому обслуживанию, ремонту, модернизации технических средств, входящих в состав ИС.

7.4. Разрешенное к использованию ПО указывается в перечне разрешенного к использованию в ИС ПО, который разрабатывается АИБом совместно с системным администратором. Пользователям запрещено приносить и устанавливать на рабочие станции ИС ПО без согласования с АИБом.

8. Ресурсы ИС, в том числе ИСПДн, обрабатывающих КИ

8.1. К ресурсам ИС комитета относятся файлы, каталоги, тома, диски, устройства вывода информации (СD-RW, COM и LPT порты, порты USB).

8.2. Информационные ресурсы, предназначенные для хранения и обработки КИ перечислены в утвержденном перечне защищаемых информационных ресурсов.

8.3. Разграничение доступа пользователей к портам ввода-вывода информации в ИС комитета реализовано в разрешительной системе доступа.

8.4. Если доступ пользователя к конкретному информационному ресурсу не определен, то доступа к нему они не имеют.

8.5. Запрещается хранить КИ на ресурсах, отличных от перечисленных в утвержденном перечне защищаемых ресурсов.

9. Антивирусная защита

9.1. Антивирусная защита осуществляется с применением разрешенных программных средств в соответствии с Инструкцией по проведению антивирусного контроля в информационных системах.

9.2. Используемые антивирусные средства указываются в Перечне разрешенного к использованию программного обеспечения.

10. Обеспечение безопасности информации

10.1 Оператор должен обеспечивать надлежащие условия защиты КИ, хранящихся в используемых ИС от несанкционированного доступа, использования, распространения, искажения и уничтожения. Сотрудники, уполномоченные осуществлять обработку персональных данных, несут ответственность за защиту КИ в порядке, предусмотренном действующим законодательством Российской Федерации.

10.2 Настройку СЗИ от НСД для конкретных пользователей, контроль её работы, обновление антивирусных баз, диагностику и устранение неисправностей или сбоев в работе программного или аппаратного обеспечения осуществляет АИБ с обязательным подписанием совместного протокола об установке ПО с указанием даты установки, фамилии, имени, отчества, должности получателя – ответственного лица оператора.

10.3 Функции, права, обязанности АИБа, а также порядок ремонта и модернизации регламентируются специально разработанной Инструкцией по техническому обслуживанию, ремонту, модернизации технических средств, входящих в состав ИС и должностной инструкцией АИБа.

10.4 Повседневный контроль защищенности ИС от НСД проводится АИБом. Контроль осуществляется с помощью штатных средств СЗИ от НСД. Основным средством контроля является анализ системного журнала.

10.5 Доступ пользователей к работе в ИС осуществляется в строгом соответствии со списком постоянных пользователей ИС, разрабатываемым АИБом и системным администратором.

10.6 Допускается наличие только пользователей ИС, указанных в списке постоянных пользователей, имеющих доступ к КИ.

10.7. При необходимости исполнителям может быть выдан персональный электронный идентификатор СЗИ, предназначенный для идентификации при входе в систему.

10.8. Программирование, учет выдачи персональных электронных идентификаторов от СЗИ и контроль за их наличием возлагается на АИБа.

10.9 Права доступа пользователей к программам, каталогам, файлам определены в списке постоянных пользователей ИС (матрица доступа к защищаемым ресурсам).

10.10. Порядок работы пользователя определены в соответствующем положении по работе пользователя в ИС комитета.

11. Пользователи

11.1. Пользователями ИС являются сотрудники комитета в строгом соответствии со списком постоянных пользователей ИС, имеющими соответствующие права допуска, и не сотрудники организации (внешние пользователи), осуществляющие доступ к системе только в рамках установленных оператором полномочий. В рамках управления доступом пользователей ИС к ресурсам ИС и в соответствии с решаемыми задачами выделены следующие категории пользователей:

11.2. АИБ обладает всей полнотой доступа к ресурсам ИС организует и контролирует работу ИС, объектов информатизации, других пользователей:

11.3. Администратор ИС и (или) АИБ осуществляет: настройку систем защиты от НСД, контроль их работы, обновление антивирусных баз, диагностику и устранение неисправностей или сбоев в работе программного или аппаратного обеспечения, также в его обязанности входит выполнение резервного копирования и восстановления информации. Функции, права и обязанности администратора ИС и АИБа регламентируются должностными инструкциями.

11.4. Пользователи ИС (операторы) непосредственно осуществляют подготовку, ввод, обработку, хранение и удаление информации в ИС, в том числе ИСПДн. В зависимости от выполняемых в ИС задач и для реализации правил разграничения доступа к ресурсам ИС, в том числе ИСПДн могут выделяться группы пользователей. Группы пользователей и права доступа различных групп к информационным ресурсам назначаются в соответствии с разрешительной системой доступа. Функции, права и обязанности пользователя ИС регламентируются соответствующими инструкциями по работе пользователя в ИС.

11.5 Внешние пользователи проходят процедуру идентификации и аутентификации для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации. Оператором должен быть установлен перечень действий внешних пользователей разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий внешних пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации.

11.5 Разрешение действий внешних пользователей до прохождения ими процедур идентификации и аутентификации осуществляется, в том числе при предоставлении внешним пользователям доступа к общедоступной информации комитета (веб-сайтам, порталам, иным общедоступным ресурсам).

11.6. После прохождения процедуры идентификации и аутентификации внешние пользователи осуществляют доступ к информационным ресурсам в соответствии с правами, установленными АИБом для внешних пользователей ИС комитета.

12. Задачи ИС

12.1. Технологический процесс обработки информации в ИС комитета включает в себя:

задачу получения исходных данных, их подготовка, оформление, регистрация и выдача пользователям ИС комитета;

задачу оформления, регистрации и передачи выходных данных;

задачу ввода, подготовки, обработки, хранения и вывода информации в ИС;

регистрации созданных текстовых файлов.

12.2. Задача получения исходных данных, их подготовка, оформление, регистрация и выдача пользователям ИС состоит из следующих этапов:

получение ПДн, на бумажных носителях и в электронном виде от сторонних организаций, клиентов и выдача пользователям ИС комитета;

распечатка электронных файлов документов, содержащих ПДн, на принтере ИС;

передача сведений на бумажных носителях и в электронном виде, обработанных пользователями ИС комитета, в сторонние организации по каналам передачи данных.

12.3. Полученные МНИ регистрируются, ставятся на учет и хранятся в соответствии с требованиями Инструкции по организации работы с электронными носителями конфиденциальной информации, а затем используются сотрудниками комитета для обработки информации.

12.4. Задачи оформления, регистрации и передачи выходных данных выполняются сотрудниками ответственными за ведение конфиденциального делопроизводства в подразделениях. Они регистрируют МНИ в соответствии с требованиями Инструкции по организации работы с электронными носителями конфиденциальной информации. В соответствии с указанным порядком происходит оформление МНИ.

12.5. Задачи ввода, подготовки, обработки, хранения и вывода информации в ИС выполняются сотрудниками ответственными за ведение конфиденциального делопроизводства в подразделениях. Задачи выполняются с помощью, установленного на рабочей станции ИС ПО, указанного в утвержденном перечне разрешенного к использованию в ПО. Все файлы, содержащие ПДн, хранятся и обрабатываются только в специальных каталогах, входящих в утвержденный перечень защищаемых информационных ресурсов. Права доступа назначаются АИБом в соответствии с разрешительной системой доступа.

12.6. Копирование файлов с МНИ в специальные каталоги на жестком диске ПЭВМ, а также (в случае необходимости) предварительное изменение скопированных файлов. Файлы содержат текстовую информацию (техническую документацию, электронные документы и т. д.).

12.7. Создание сотрудниками ответственными за ведение конфиденциального делопроизводства в подразделениях конфиденциальных документов, их редактирование, уничтожение, хранение в специальных каталогах на жестком диске ПЭВМ или учтенных МНИ.

12.8. Запись созданных текстовых файлов на учтенные МНИ осуществляется сотрудниками в соответствии с его функциональными обязанностями и разрешительной системой доступа.

12.9. Задача регистрации созданных текстовых файлов выполняется пользователями ИС вручную сразу после подготовки конфиденциальных файлов и сохранения их на жесткий диск ПЭВМ, копирования конфиденциальных файлов на МНИ.

12.10. Удаление файлов с жестких магнитных дисков или МНИ осуществляется специальными средствами удаления информации, несколькими циклами затирания информации. В случае, если МНИ выводится из обращения, он подлежит физическому уничтожению в соответствии с требованиями Инструкции по организации работы с электронными носителями конфиденциальной информации.

12.11. Настройка, управление и техническое сопровождение СЗИ проводится АИБом и включает следующие операции:

установка и настройка безопасной операционной среды для пользователей ИС. На этом этапе производится: установка и настройка операционной системы рабочих станций, подключение и конфигурирование устройств ввода-вывода информации в/из ИС, установка и настройка СЗИ, регистрация в СЗИ пользовательских учетных записей и настройка прав доступа для каждого пользователя в соответствии с его функциональными обязанностями (в том числе программирование, регистрация и выдача пользователям ИС персональных идентификаторов, а также учет и контроль за наличием их у пользователей), создание, предварительное наполнение информацией (не содержащей сведения, составляющие государственную тайну) и конфигурирование ресурсов ИС, реализация правил разграничения доступа к этим ресурсам в соответствии с разрешительной системой доступа, настройка парольной политики, политики затирания данных и т.д. Права доступа пользователей к программам, каталогам, файлам определены в разрешительной системе доступа к защищаемым ресурсам ИСПДн комитета;

непрерывный мониторинг безопасности в ИС с целью выявления нарушений правил разграничения доступа пользователями ИС, диагностики и последующего устранения выявленных неисправностей или ошибок в работе программно-аппаратного обеспечения операционной среды ИС. Данная задача выполняется АИБом путем регулярного анализа системных журналов операционной системы и СЗИ от НСД, регулярных проверок соответствия, реализованных в ИС правил разграничения доступа к ресурсам, требованиям разрешительной политики доступа, регулярных проверок правильности соблюдения пользователями требований по защите информации;

регулярное сопровождение подсистемы безопасности с целью обеспечения эффективности работы пользователей ИС и обеспечения защиты информации. Данная задача выполняется АИБом и ответственным за эксплуатацию ПЭВМ (в части касающейся организационных мероприятий по защите информации) регулярно (по расписанию) или при обнаружении внештатных ситуаций и регламентируется Инструкцией технического обслуживания, ремонта, модернизации технических средств, входящих в состав ИС. Задача включает следующие операции: регулярное проведение инструктажа пользователей по безопасной работе в ИС устранение выявленных неисправностей и ошибок (осуществляется АИБом), регулярные обновление прикладного ПО и обеспечение его целостности.

13.Этапы технологического процесса

13.1. Доступ пользователей к работе в ИС.

13.1.1. Доступ пользователей к информационным ресурсам определяется на основании списка постоянных пользователей ИС и перечня защищаемых информационных ресурсов, утверждённого председателем комитета. Права доступа к информационным ресурсам назначаются каждому пользователю на основании разрешительной системы доступа, разрабатываемой АИБом.

13.1.2. Разграничение прав доступа пользователей к информационным ресурсам и установление полномочий этим пользователям реализуется АИБом средствами ОС и дополнительными средствами СЗИ от НСД.

13.1.3. Вход в систему осуществляется по персональному имени (персональному идентификатору) и паролю конкретного пользователя. При успешном входе в систему пользователь получает права доступа к устройствам, каталогам, файлам и программам, установленные АИБом.

13.1.4. При увольнении пользователя или переходе в другое подразделение, АИБом или системным администратором на основании приказа, в последний день работы пользователя (или иной день, указанный в приказе), производится удаление учетной записи пользователя и всех его ресурсов (за исключением необходимых для работы других пользователей).

13.2. Начало сеанса работы.

13.2.1. Перед началом сеанса работы пользователь включает свою рабочую станцию и проходит процедуру аутентификации.

13.2.2. В процессе аутентификации пользователь использует свои личные логин и пароль. Смена личного пароля производится не реже 1 раза в три месяца. Контроль данного процесса осуществляется АИБом.

13.3. Регистрация пользователей и назначение прав доступа.

13.3.1 Регистрация пользователей и назначение прав доступа производится администратором информационной безопасности на основании заявления «На создание (продление) учетной записи пользователя».

13.3.2. Зарегистрированный пользователь устанавливает свой личный пароль.

13.3.3. Права доступа устанавливаются пользователю средствами ОС в соответствии с разрешительной системой доступа.

13.3.4. Удаление пользователя выполняется однократно при необходимости выведения сотрудника из числа пользователей ИС комитета.

13.4. Работа с файлами документов, внесение изменений, хранение:

13.4.1. Файлы документов разрабатываются на рабочем месте пользователем, зарегистрированным в ИС комитета.

13.4.2. Работа пользователя при подготовке файла документа возможна только после успешного прохождения процедуры аутентификации в ИС.

13.4.3. Пользователи имеют право постоянного хранения файлов с конфиденциальными и не конфиденциальными данными, ПДн на жестком магнитном диске только в специально выделенных АИБом каталогах.

13.4.4. Разработка и подготовка к печати документов производится с применением установленных на рабочей станции текстовых и табличных редакторов.

13.4.5. Распечатка документов производится на принтере, размещенном на ОИ и включенном в технический паспорт на этот ОИ.

13.4.6. По окончании сеанса подготовки документа производится его сохранение в виде файла в разрешенном каталоге или на закрепленный за пользователем МНИ, соответствующим образом зарегистрированный.

13.4.7. В случае отсутствия необходимости дальнейшей работы с документом, впервые набранным с клавиатуры, пользователь может отказаться от сохранения его в виде файла. Также пользователь может отказаться от сохранения внесенных в файл изменений.

13.5. Уничтожение файлов, содержащих конфиденциальные данные:

13.5.1. Удаление данных (файлов) и временных файлов производится штатными средствами ОС при включенном режиме затирания данных или СЗИ от НСД (в том числе автоматическое обнуление файла подкачки).

13.5.2. Уничтожение файла может быть произведено без распечатки документа, если в документе отпала необходимость.

13.5.3. При установке операционной системы должна быть отключена функция удаления файлов через «корзину».

13.5.4. При установке СЗИ от НСД в ней должна быть активирована функция затирания данных с применением не менее 2-х циклов затирания.

13.5.5. Факт удаления КИ с МНИ фиксируется в соответствующем акте. Формирование акта производит пользователь, уничтоживший эту информацию.

13.6. Работа с МНИ:

13.6.1. Для разработки и хранения файлов с КИ могут использоваться МНИ, учтенные в установленном порядке в соответствии с требованиями Инструкции по организации работы с электронными носителями конфиденциальной информации;

13.6.2. В качестве МНИ в ИСПДн комитета могут использоваться (разрешены к использованию) следующие накопители информации:

гибкие магнитные диски;

оптические (лазерные) диски;

USB flash накопители (накопители информации, подключаемые к USB порту ввода–вывода ПЭВМ);

USB flash накопители учитываются в установленном порядке в соответствии с требованиями Инструкции по организации работы с электронными носителями конфиденциальной информации.

МНИ при необходимости выдаются каждому пользователю из числа сотрудников, обрабатывающих конфиденциальные сведения и персональные данные. Выданный носитель предназначен только для хранения файлов подготовленных документов. Операции с МНИ для КИ могут проводиться только на ПЭВМ, входящей в состав ИС, предназначенных для работы с информацией соответствующей категории.

13.7.Подготовка МНИ. Выведение из обращения МНИ:

13.7.1. При необходимости создания нового МНИ, пользователь регистрирует его в соответствии с требованиями Инструкции по организации работы с электронными носителями конфиденциальной информации.

13.7.2. При необходимости пользователь сдает зарегистрированный МНИ АИБу с целью его подготовки для дальнейшего использования на ПЭВМ, входящей в состав ИС.

13.7.3. Выведение МНИ из обращения производится путем его физического уничтожения, при этом составляется акт соответствующей формы, предусмотренной Инструкцией по организации работы с электронными носителями конфиденциальной информации.

13.8. Создание файлов на МНИ:

13.8.1. Условиями, необходимыми для выполнения данной процедуры, являются:

пользователю разрешено самостоятельно копировать файлы на МНИ и обратно;

наличие у пользователя подготовленного и зарегистрированного соответствующим образом МНИ.

13.9. Хранение МНИ пользователя:

13.9.1. Хранение МНИ пользователя должно осуществляться в соответствии с требованиями Инструкции по организации работы с электронными носителями конфиденциальной информации.

13.9.2. Распечатка документов на печатающем устройстве компьютера (принтере).

13.9.3. Условием, необходимым для распечатки документов, является наличие у пользователя:

прав доступа к защищаемым ресурсам ИС;

подготовленных и зарегистрированных соответствующим образом листов.

13.9.4. Регистрация листов, используемых для распечатки конфиденциальных документов, осуществляется пользователем в соответствии с требованиями Инструкции по организации работы с электронными носителями конфиденциальной информации.

13.9.5. Пользователь, распечатавший конфиденциальный документ, немедленно регистрирует его у сотрудника, ответственного за ведение конфиденциального делопроизводства.

13.9.6. Оформление, распечатка, учёт и уничтожение документов производится в соответствии с требованиями технологического процесса, Инструкции по работе пользователя в ИС, Инструкции по организации работы с электронными носителями конфиденциальной информации.

13.9.7. Контроль за распечаткой документов возлагается на АИБа.

13.10. Резервное копирование:

13.10.1. Резервное копирование информационных ресурсов производится АИБом или администратором ИС в соответствии с правами доступа на МНИ, учтенные в порядке, установленным Инструкцией по резервному копированию.

13.11. Передача информации:

13.11.1. Передача файлов КИ на МНИ в другие подразделения комитета, а также организации иной ведомственной подчинённости, производится по каналам связи, в соответствии с требованиями законодательства РФ по обеспечению защиты КИ и Инструкцией по организации работы с электронными носителями конфиденциальной информации.

13.12. Завершение сеанса работы:

13.12.1. По завершении работы пользователь выполняет штатную процедуру завершения работы, выключает рабочую станцию и сдаёт имеющиеся МНИ сотруднику, ответственному за работу пользователей с МНИ.

14. Заключительные положения

14.1. Всем сотрудникам, допущенным к работе с КИ, разъясняется ответственность за нарушение правил получения, обработки, защиты КИ.

14.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту КИ, несут ответственность в соответствии с действующим законодательством.