

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

**СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ
ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ
ИНФОРМАЦИИ**

(СТР-К)

Москва 2001

СО Д Е Р Ж А Н И Е

1. Термины, определения и сокращения.....	
2. Общие положения.....	
3. Организация работ по защите информации.....	
4. Требования и рекомендации по защите речевой информации.....	
4.1. Общие положения.....	
4.2. Основные требования и рекомендации по защите информации, циркулирующей в защищаемых помещениях.....	
4.3. Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения кинофильмов.....	
4.4. Защита информации при проведении магнитной звукозаписи..	
4.5. Защита речевой информации при ее передаче по каналам связи	
5. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	
5.1. Общие требования и рекомендации.....	
5.2. Основные требования и рекомендации по защите служебной тайны и персональных данных.....	
5.3. Основные рекомендации по защите информации, составляющей коммерческую тайну.....	
5.4. Порядок обеспечения защиты информации при эксплуатации АС.....	
5.5. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ.....	
5.6. Защита информации при использовании съемных накопителей большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ	
5.7. Защита информации в локальных вычислительных сетях.....	
5.8. Защита информации при межсетевом взаимодействии.....	
5.9. Защита информации при работе с системами управления базами данных.....	
6. Рекомендации по обеспечению защиты информации, содержащейся в негосударственных информационных ресурсах, при взаимодействии абонентов с информационными сетями общего пользования	
6.1. Общие положения.....	
6.2. Условия подключения абонентов к Сети.....	
6.3. Порядок подключения и взаимодействия абонентских пунктов с Сетью, требования и рекомендации по обеспечению безопасности информации	
7. Приложения.....	

1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе приняты следующие основные термины, определения и сокращения:

1.1. Абонент Сети* - лицо, являющееся сотрудником учреждения (предприятия), имеющее соответствующим образом оформленное разрешение и технические возможности на подключение и взаимодействие с Сетями.

1.2. Абонентский пункт (АП) - средства вычислительной техники учреждения (предприятия), подключаемые к Сетям с помощью коммуникационного оборудования.

АП могут быть в виде автономных персональных электронно-вычислительных машин (ПЭВМ) с модемом и не иметь физических каналов связи с другими средствами вычислительной техники (СВТ) предприятия, а также в виде одной или нескольких объединенных локальных вычислительных сетей (ЛВС) с рабочими станциями и серверами, соединенных с Сетями через коммуникационное оборудование (модемы, мосты, шлюзы, маршрутизаторы-роутеры, мультиплексоры, коммуникационные серверы и т.п.).

1.3. Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

1.4. Администратор АС - лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

1.5. Администратор защиты (безопасности) информации – лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации.

1.6. Безопасность информации - состояние защищенности информации, характеризующееся способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

1.7. Вспомогательные технические средства и системы (ВТС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

К ним относятся:

- различного рода телефонные средства и системы;
- средства и системы передачи данных в системе радиосвязи;
- средства и системы охранной и пожарной сигнализации;
- средства и системы оповещения и сигнализации;
- контрольно-измерительная аппаратура;
- средства и системы кондиционирования;
- средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.д.);
- средства электронной оргтехники;
- средства и системы электрочасофикации;
- иные технические средства и системы.

1.8. Доступ к информации (доступ) - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

**Смотри также п.1.14.

1.9. Доступность (санкционированная доступность) информации - состояние информации, характеризующееся способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

1.10. Защита информации от несанкционированного доступа (защита от НСД) или воздействия - деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

11. Специальный защитный знак (СЗЗ) - сертифицированное и зарегистрированное в установленном порядке изделие, предназначенное для контроля несанкционированного доступа к объектам защиты путем определения подлинности и целостности СЗЗ, путем сравнения самого знака или композиции "СЗЗ - подложка" по критериям соответствия характерным признакам визуальными, инструментальными и другими методами.

1. Защищаемые помещения (ЗП) – помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

1.13. Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, передаваемая, хранимая или обрабатываемая в основных технических средствах и системах и обсуждаемая в ЗП.

1.14. Информационные сети общего пользования (далее-Сети) - вычислительные (информационно-телекоммуникационные сети) открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

1.15. Контролируемая зона (КЗ) - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Границей КЗ могут являться:

- периметр охраняемой территории учреждения (предприятия);
- ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

В отдельных случаях на период обработки техническими средствами конфиденциальной информации КЗ временно может устанавливаться большей, чем охраняемая территория предприятия. При этом должны приниматься организационно-режимные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

16.

Конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

1. Локальная вычислительная сеть - вычислительная сеть, поддерживающая в пределах ограниченной территории один или несколько высокоскоростных каналов передачи цифровой информации, предоставляемых подключаемым устройствам для кратковременного монопольного использования.

1.18. Межсетевой экран (МЭ) - это локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией.

1.19. Несанкционированный доступ (несанкционированные действия) (НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами

вычислительной техники или автоматизированными системами.

1.20. Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации. В контексте настоящего документа к ним относятся технические средства и системы автоматизированных систем различного уровня и назначения на базе средств вычислительной техники, средства и системы связи и передачи данных, используемые для обработки конфиденциальной информации.

1.21. Провайдер Сети - уполномоченная организация, выполняющая функции поставщика услуг Сети для абонентского пункта и непосредственно для абонентов Сети.

1.22. Система защиты информации от НСД (СЗИ НСД) - комплекс организационных мер и программно-технических (при необходимости криптографических) средств защиты от несанкционированного доступа к информации (несанкционированных действий с ней) в автоматизированной системе.

1.23. Служебная информация СЗИ НСД - информационная база АС, необходимая для функционирования СЗИ НСД (уровень полномочий эксплуатационного персонала АС, матрица доступа, ключи, пароли и т.д.).

1.24. Технический канал утечки информации – совокупность объекта технической разведки, физической среды и средства технической разведки, которыми добываются разведывательные данные.

1.25. Услуги Сети - комплекс функциональных возможностей, предоставляемых абонентам сети с помощью прикладных протоколов (протоколы электронной почты, FTP - File Transfer Protocol - прием/передача файлов, HTTP - Hiper Text Transfer Protocol - доступ к Web-серверам, IRC - Internet Relay Chat -диалог в реальном времени, Telnet - терминальный доступ в сети, WAIS - Wide Area Information Servers - система хранения и поиска документов в сети и т.д.).

1.26. Целостность информации - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

1.27. Web-сервер - общедоступный в Сети информационный сервер, использующий гипертекстовую технологию.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий документ устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты конфиденциальной информации на территории Российской Федерации и является основным руководящим документом в этой области для федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, предприятий, учреждений и организаций (далее - учреждения и предприятия) независимо от их организационно-правовой формы и формы собственности, должностных лиц и граждан Российской Федерации, взявшим на себя обязательства либо обязанными по статусу исполнять требования правовых документов Российской Федерации по защите информации.

2.2. Требования и рекомендации настоящего документа распространяются на защиту:

- конфиденциальной информации - информации с ограниченным доступом (за исключением сведений, отнесенных к государственной тайне) содержащейся в государственных (муниципальных) информационных ресурсах, накопленной за счет государственного (муниципального) бюджета и являющейся собственностью государства (к ней может быть отнесена информация, составляющая служебную тайну и другие виды тайн в соответствии с законодательством Российской Федерации, а также сведения конфиденциального характера в соответствии с “Перечнем сведений конфиденциального характера”, утвержденного Указом Президента Российской Федерации от 06.03.97 №188), защита которой осуществляется в интересах государства (далее - служебная тайна);
- информации о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющей идентифицировать его личность (персональные данные)*, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2.3. Для защиты конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, режим защиты которой определяет собственник этих ресурсов (например, информации, составляющей коммерческую, банковскую тайну и т.д.) (далее - коммерческая тайна), данный документ носит рекомендательный характер.

4. Документ разработан на основании федеральных законов “Об информации, информатизации и защите информации”, “Об участии в международном информационном обмене”, Указа Президента Российской Федерации от 06.03.97г. № 188 “Перечень сведений конфиденциального характера”, “Доктрины информационной безопасности Российской Федерации”, утвержденной Президентом Российской Федерации 09.09.2000г. № Пр.-1895, “Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти”, утвержденного постановлением Правительства Российской Федерации от 03.11.94г. № 1233, других нормативных правовых актов по защите информации (приложение № 8), а также опыта реализации мер защиты информации в министерствах и ведомствах, в учреждениях и на предприятиях.

** соответствии с Федеральным законом “Об информации, информатизации и защите информации” режим защиты персональных данных должен быть определен федеральным законом. До его введения в действие для установления режима защиты такой информации следует руководствоваться настоящим документом.

2.5. Документ определяет следующие основные вопросы защиты информации:

- организацию работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;
- состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;
- требования и рекомендации по защите речевой информации при осуществлении переговоров, в том числе с использованием технических средств;
- требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;
- порядок обеспечения защиты информации при эксплуатации объектов информатизации;
- особенности защиты информации при разработке и эксплуатации автоматизированных систем, использующих различные типы средств вычислительной техники и информационные технологии;
- порядок обеспечения защиты информации при взаимодействии абонентов с информационными сетями общего пользования.

Порядок разработки, производства, реализации и использования средств криптографической защиты информации определяется “Положением о порядке разработки, производства (изготовления), реализации, приобретения и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну” (Положение ПКЗ-99), а также “Инструкцией по организации и обеспечению безопасности хранения, обработки и передачи по техническим каналам связи конфиденциальной информации в Российской Федерации с использованием сертифицированных ФАПСИ криптографических средств”.

2.6. Защита информации, обрабатываемой с использованием технических средств, является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и должна осуществляться в установленном настоящим документом порядке в виде системы (подсистемы) защиты информации во взаимосвязи с другими мерами по защите информации.

7. Защите подлежит информация, как речевая, так и обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в АС.

Защищаемыми объектами информатизации являются:

- средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации;
- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);

- защищаемые помещения.

2.8. Защита информации должна осуществляться посредством выполнения комплекса мероприятий и применение (при необходимости) средств ЗИ по предотвращению утечки информации или воздействия на нее по техническим каналам, за счет несанкционированного доступа к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств.

2.9. При ведении переговоров и использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

- акустическое излучение информативного речевого сигнала;
- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы КЗ;
- виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;
- несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;
- воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;
- побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;
- наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;
- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;
- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации “закладок”, модулированные информативным сигналом;
- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- прослушивание ведущихся телефонных и радиопереговоров;
- просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

2.10. Перехват информации или воздействие на нее с использованием технических средств могут вестись:

- из-за границы КЗ из близлежащих строений и транспортных средств;
- из смежных помещений, принадлежащих другим учреждениям (предприятиям) и расположенным в том же здании, что и объект защиты;
- при посещении учреждения (предприятия) посторонними лицами;
- за счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через информационные сети общего пользования.

2.11. В качестве аппаратуры перехвата или воздействия на информацию и технические средства могут использоваться портативные возимые и носимые устройства, размещаемые вблизи объекта защиты либо подключаемые к каналам связи или техническим средствам обработки информации, а также электронные устройства перехвата информации “закладки”, размещаемые внутри или вне защищаемых помещений.

2.12. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:

- непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем;
- случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;
- некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;
- просмотра информации с экранов дисплеев и других средств ее отображения.

2.13. Выявление и учет факторов воздействующих или могущих воздействовать на защищаемую информацию (угроз безопасности информации) в конкретных условиях, в соответствии с ГОСТ Р 51275-99, составляют основу для планирования и осуществления мероприятий, направленных на защиту информации на объекте информатизации.

Перечень необходимых мер защиты информации определяется по результатам обследования объекта информатизации с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения санкционированной доступности информации и работоспособности технических средств, обрабатывающих эту информацию, а также с учетом реальных возможностей ее перехвата и раскрытия ее содержания.

2.14. Основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности информации реализуются без применения сложных технических средств перехвата информации:

- речевой информации, циркулирующей в защищаемых помещениях;
- информации, обрабатываемой средствами вычислительной техники, от несанкционированного доступа и несанкционированных действий;
- информации, выводимой на экраны видеомониторов;
- информации, передаваемой по каналам связи, выходящим за пределы КЗ.

2.15. Разработка мер и обеспечение защиты информации осуществляются подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководством предприятия (учреждения) для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии Гостехкомиссии России и/или ФАПСИ на право оказания услуг в области защиты информации.

2.16. Для защиты информации рекомендуется использовать сертифицированные по требованиям безопасности информации технические средства обработки и передачи

информации, технические и программные средства защиты информации.

При обработке документированной конфиденциальной информации на объектах информатизации в органах государственной власти Российской Федерации и органах государственной власти субъектов Российской Федерации, других государственных органах, предприятиях и учреждениях средства защиты информационных систем подлежат обязательной сертификации.

2.17. Объекты информатизации должны быть аттестованы на соответствие требованиям по защите информации*.

2.18. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителей учреждений и предприятий, эксплуатирующих объекты информатизации.

**Здесь и далее под аттестацией понимается комиссионная приемка объекта информатизации силами предприятия с обязательным участием специалиста по защите информации.

3. ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

3.1. Организация и проведение работ по технической защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами Гостехкомиссии России.

3.2. Организация работ по защите информации возлагается на руководителей учреждений и предприятий, руководителей подразделений, осуществляющих разработку проектов объектов информатизации и их эксплуатацию, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации на руководителей подразделений по защите информации (служб безопасности) учреждения (предприятия).

3.3. Научно-техническое руководство и непосредственную организацию работ по созданию (модернизации) СЗИ объекта информатизации осуществляет его главный конструктор или другое должностное лицо, обеспечивающее научно-техническое руководство созданием объекта информатизации.

3.4. Разработка СЗИ может осуществляться как подразделением учреждения (предприятия), так и специализированным предприятием, имеющим лицензии Гостехкомиссии России и/или ФАПСИ на соответствующий вид деятельности в области защиты информации.

В случае разработки СЗИ или ее отдельных компонент специализированным предприятием, в учреждении (на предприятии), для которого осуществляется разработка (предприятие-заказчик), определяются подразделения (или отдельные специалисты), ответственные за организацию и проведение (внедрение и эксплуатацию) мероприятий по защите информации в ходе выполнения работ с использованием конфиденциальной информации.

Разработка и внедрение СЗИ осуществляется во взаимодействии разработчика со службой безопасности предприятия-заказчика, которая осуществляет методическое руководство и участвует в разработке конкретных требований по защите информации, аналитическом обосновании необходимости создания СЗИ, согласовании выбора средств вычислительной техники и связи, технических и программных средств защиты, организации работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации, в аттестации объектов информатизации.

3.5. Организация работ по созданию и эксплуатации объектов информатизации и их СЗИ определяется в разрабатываемом на предприятии “Руководстве по защите информации” или в специальном “Положении о порядке организации и проведения работ по защите информации” и должна предусматривать:

- порядок определения защищаемой информации;
- порядок привлечения подразделений предприятия, специализированных сторонних организаций к разработке и эксплуатации объектов информатизации и СЗИ, их задачи и функции на различных стадиях создания и эксплуатации объекта информатизации;
- порядок взаимодействия всех занятых в этой работе организаций, подразделений и специалистов;
- порядок разработки, ввода в действие и эксплуатацию объектов информатизации;
- ответственность должностных лиц за своевременность и качество формирования требований по технической защите информации, за качество и научно-технический уровень разработки СЗИ.

3.6. В учреждении (на предприятии) должен быть документально оформлен перечень сведений конфиденциального характера (приложение № 6), подлежащих защите в соответствии с нормативными правовыми актами, а также разработана соответствующая

разрешительная система доступа персонала к такого рода сведениям.

3.7. Устанавливаются следующие стадии создания системы защиты информации:

- предпроектная стадия, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание;
- стадия проектирования (разработки проектов) и реализации объекта информатизации, включающая разработку СЗИ в составе объекта информатизации;
- стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемосдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации.

3.8. На предпроектной стадии по обследованию объекта информатизации:

- устанавливается необходимость обработки (обсуждения) конфиденциальной информации на данном объекте информатизации;
- определяется перечень сведений конфиденциального характера, подлежащих защите от утечки по техническим каналам;
- определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования;
- определяются условия расположения объектов информатизации относительно границ КЗ;
- определяются конфигурация и топология автоматизированных систем и систем связи в целом и их отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- определяются технические средства и системы, предполагаемые к использованию в разрабатываемой АС и системах связи, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;
- определяются режимы обработки информации в АС в целом и в отдельных компонентах;
- определяется класс защищенности АС;
- определяется степень участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности;
- определяются мероприятия по обеспечению конфиденциальности информации в процессе проектирования объекта информатизации.

3.9. По результатам предпроектного обследования разрабатывается аналитическое обоснование необходимости создания СЗИ.

На основе действующих нормативных правовых актов и методических документов по защите конфиденциальной информации, в т.ч. настоящего документа, с учетом установленного класса защищенности АС задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку СЗИ.

3.10. Предпроектное обследование в части определения защищаемой информации должно базироваться на документально оформленных перечнях сведений конфиденциального характера.

Перечень сведений конфиденциального характера составляется заказчиком объекта информатизации и оформляется за подписью соответствующего руководителя.

3.11. Предпроектное обследование может быть поручено специализированному предприятию, имеющему соответствующую лицензию, но и в этом случае анализ

информационного обеспечения в части защищаемой информации целесообразно выполнять представителям предприятия-заказчика при методической помощи специализированного предприятия.

Ознакомление специалистов этого предприятия с защищаемыми сведениями осуществляется в установленном на предприятии-заказчике порядке.

3.12. Аналитическое обоснование необходимости создания СЗИ должно содержать:

- информационную характеристику и организационную структуру объекта информатизации;
- характеристику комплекса основных и вспомогательных технических средств, программного обеспечения, режимов работы, технологического процесса обработки информации;
- возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;
- перечень предлагаемых к использованию сертифицированных средств защиты информации;
- обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации;
- оценку материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;
- ориентировочные сроки разработки и внедрения СЗИ;
- перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

Аналитическое обоснование подписывается руководителем предпроектного обследования, согласовывается с главным конструктором (должностным лицом, обеспечивающим научно-техническое руководство создания объекта информатизации), руководителем службы безопасности и утверждается руководителем предприятия-заказчика.

3.13. Техническое (частное техническое) задание на разработку СЗИ должно содержать:

- обоснование разработки;
- исходные данные создаваемого (модернизируемого) объекта информатизации в техническом, программном, информационном и организационном аспектах;
- класс защищенности АС;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗИ и приниматься в эксплуатацию объект информатизации;
- конкретизацию требований к СЗИ на основе действующих нормативно-методических документов и установленного класса защищенности АС;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации, невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения;
- перечень подрядных организаций-исполнителей видов работ;
- перечень предъявляемой заказчику научно-технической продукции и документации.

3.14. Техническое (частное техническое) задание на разработку СЗИ подписывается

разработчиком, согласовывается со службой безопасности предприятия-заказчика, подрядными организациями и утверждается заказчиком.

3.15. В целях дифференцированного подхода к защите информации производится классификация АС по требованиям защищенности от НСД к информации.

Класс защищенности АС от НСД к информации устанавливается совместно заказчиком и разработчиком АС с привлечением специалистов по защите информации в соответствии с требованиями руководящего документа (РД) Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" и раздела 5 настоящего документа и оформляется актом.

Пересмотр класса защищенности АС производится в обязательном порядке, если произошло изменение хотя бы одного из критериев, на основании которых он был установлен.

3.16. На стадии проектирования и создания объекта информатизации и СЗИ в его составе на основе предъявляемых требований и заданных заказчиком ограничений на финансовые, материальные, трудовые и временные ресурсы осуществляются:

- разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) объекта информатизации в соответствии с требованиями технического (частного технического) задания на разработку СЗИ;
- разработка раздела технического проекта на объект информатизации в части защиты информации;
- строительно-монтажные работы в соответствии с проектной документацией, утвержденной заказчиком, размещением и монтажом технических средств и систем;
- разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- закупка сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации, либо их сертификация;
- закупка сертифицированных технических, программных и программно-технических (в т.ч. криптографических) средств защиты информации и их установка;
- разработка (доработка) или закупка и последующая сертификация по требованиям безопасности информации программных средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные программные средства;
- организация охраны и физической защиты помещений объекта информатизации, исключающих несанкционированный доступ к техническим средствам обработки, хранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;
- разработка и реализация разрешительной системы доступа пользователей и эксплуатационного персонала к обрабатываемой (обсуждаемой) на объекте информатизации информации;
- определение заказчиком подразделений и лиц, ответственных за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации;
- выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;
- разработка эксплуатационной документации на объект информатизации и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);

- выполнение других мероприятий, специфичных для конкретных объектов информатизации и направлений защиты информации.

3.17. Задание на проектирование оформляется отдельным документом, согласовывается с проектной организацией, службой (специалистом) безопасности предприятия-заказчика в части достаточности мер по технической защите информации и утверждается заказчиком.

Мероприятия по защите информации от утечки по техническим каналам являются основным элементом проектных решений, закладываемых в соответствующие разделы проекта, и разрабатываются одновременно с ними.

3.18. На стадии проектирования и создания объекта информатизации оформляются также технический (техно-рабочий) проект и эксплуатационная документация СЗИ, состоящие из:

- пояснительной записки с изложением решений по комплексу организационных мер и программно-техническим (в том числе криптографическим) средствам обеспечения безопасности информации, состава средств защиты информации с указанием их соответствия требованиям ТЗ;
- описания технического, программного, информационного обеспечения и технологии обработки (передачи) информации;
- плана организационно-технических мероприятий по подготовке объекта информатизации к внедрению средств и мер защиты информации;
- технического паспорта объекта информатизации (форма технического паспорта на АС приведена в приложении № 5);
- инструкций и руководств по эксплуатации технических и программных средств защиты для пользователей, администраторов системы, а также для работников службы защиты информации.

3.19. На стадии ввода в действие объекта информатизации и СЗИ осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации с оформлением приемо-сдаточного акта, подписываемого разработчиком (поставщиком) и заказчиком;
- аттестация объекта информатизации по требованиям безопасности информации.

3.20. На этой стадии оформляются:

- акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний;
- предъявительский акт к проведению аттестационных испытаний;
- заключение по результатам аттестационных испытаний.

При положительных результатах аттестации на объект информатизации оформляется “Аттестат соответствия” требованиям по безопасности информации (форма “Аттестата соответствия” для АС приведена в приложении № 2, для ЗП в приложении № 3)

3.21. Кроме вышеуказанной документации в учреждении (на предприятии) оформляются приказы, указания и решения:

- о проектировании объекта информатизации, создании соответствующих подразделений разработки и назначении ответственных исполнителей;
- о формировании группы обследования и назначении ее руководителя;
- о заключении соответствующих договоров на проведение работ;
- о назначении лиц, ответственных за эксплуатацию объекта информатизации;

- о начале обработки в АС (обсуждения в защищаемом помещении) конфиденциальной информации.

3.22. Для объектов информатизации, находящихся в эксплуатации до введения в действие настоящего документа, может быть предусмотрен по решению их заказчика (владельца) упрощенный вариант их доработки (модернизации), переоформления организационно-распорядительной, технологической и эксплуатационной документации. Программа аттестационных испытаний такого рода объектов информатизации определяется аттестационной комиссией.

Необходимым условием является их соответствие действующим требованиям по защите информации.

3.23. Эксплуатация объекта информатизации осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией, с учетом требований и положений, изложенных в разделах 4-6 настоящего документа.

3.24. С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа и предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность технических средств в учреждении (на предприятии), проводится периодический (не реже одного раза в год) контроль состояния защиты информации.

Контроль осуществляется службой безопасности учреждения (предприятия), а также отраслевыми и федеральными органами контроля (для информации, режим защиты которой определяет государство) и заключается в оценке:

- соблюдения нормативных и методических документов Гостехкомиссии России;
- работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;
- знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации.

25. Собственник или владелец конфиденциальной информации имеет право обратиться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах.

1. При необходимости по решению руководителя предприятия в ЗП и в местах размещения средств обработки информации могут проводиться работы по обнаружению и изъятию «закладок», предназначенных для скрытого перехвата защищаемой информации.
2. Такие работы могут проводиться организациями, имеющими соответствующие лицензии ФАПСИ или ФСБ России на данный вид деятельности.

4. ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ РЕЧЕВОЙ ИНФОРМАЦИИ

1. Общие положения

4.1.1. Требования и рекомендации настоящего раздела направлены на исключение (существенное затруднение) возможности перехвата конфиденциальной речевой информации, циркулирующей в ЗП, в системах звукоусиления (СЗУ) и звукового сопровождения кинофильмов (СЗСК), при осуществлении её магнитной звукозаписи и передачи по каналам связи.

4.1.2. Требования настоящего раздела, если не оговорено специально, являются обязательными на всех стадиях проектирования, строительства, оснащения, эксплуатации ЗП и размещенных в них ОТСС и ВТСС, для систем СЗУ и СЗСК.

4.1.3. При проведении мероприятий с использованием конфиденциальной речевой информации и технических средств ее обработки возможна утечка информации за счет:

- акустического излучения информативного речевого сигнала;
- виброакустических сигналов, возникающих посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические системы ЗП;
- прослушивания разговоров, ведущихся в ЗП, по информационным каналам общего пользования (городская телефонная сеть, сотовая, транкинговая и пейджинговая связь, радиотелефоны) за счет скрытного подключения оконечных устройств этих видов связи;
- электрических сигналов, возникающих в результате преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющихся по проводам и линиям передачи информации, выходящих за пределы КЗ;
- побочных электромагнитных излучений информативного сигнала от обрабатывающих конфиденциальную информацию технических средств, в т.ч. возникающих за счет паразитной генерации, и линий передачи информации;
- электрических сигналов, наводимых от обрабатывающих конфиденциальную информацию технических средств и линий ее передачи, на провода и линии, выходящих за пределы КЗ;
- радиоизлучений, модулированных информативным сигналом, возникающим при работе различных генераторов, входящих в состав технических средств, установленных в ЗП, или при наличии паразитной генерации в их узлах (элементах);
- радиоизлучений, электрических или инфракрасных сигналов, модулированных информативным сигналом, от специальных электронных устройств перехвата речевой информации “закладок”, внедренных в ЗП и установленные в них технические средства.

Также следует учитывать возможность хищения технических средств с хранящейся в них информацией или отдельных носителей информации.

4.2. Основные требования и рекомендации по защите информации, циркулирующей в защищаемых помещениях

4.2.1. В учреждении (предприятии) должен быть документально определен перечень ЗП и лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации, а также составлен технический паспорт на ЗП

(форма технического паспорта приведена в приложении № 4).

4.2.2. Защищаемые помещения должны размещаться в пределах КЗ. При этом рекомендуется размещать их на удалении от границ КЗ, обеспечивающем эффективную защиту, ограждающие конструкции (стены, полы, потолки) не должны являться смежными с помещениями других учреждений (предприятий).

Не рекомендуется располагать ЗП на первых этажах зданий.

Для исключения просмотра текстовой и графической конфиденциальной информации через окна помещения рекомендуется оборудовать их шторами (жалюзи).

4.2.3. Защищаемые помещения рекомендуется оснащать сертифицированными по требованиям безопасности информации ОТСС и ВТСС либо средствами, прошедшими специальные исследования и имеющими предписание на эксплуатацию.

Эксплуатация ОТСС, ВТСС должна осуществляться в строгом соответствии с предписаниями и эксплуатационной документацией на них.

4.2.4. Специальная проверка ЗП и установленного в нем оборудования с целью выявления возможно внедренных в них электронных устройств перехвата информации “закладок” проводится, при необходимости, по решению руководителя предприятия.

4.2.5. Во время проведения конфиденциальных мероприятий запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой, пейджинговой и транкинговой связи, переносных магнитофонов и других средств аудио и видеозаписи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком или спикерфоном, а также аппаратов с автоматическим определителем номера, следует отключать их из сети на время проведения этих мероприятий.

4.2.6. Для исключения возможности утечки информации за счет электроакустического преобразования рекомендуется использовать в ЗП в качестве оконечных устройств телефонной связи, имеющих прямой выход в городскую АТС, телефонные аппараты (ТА), прошедшие специальные исследования, либо оборудовать их сертифицированными средствами защиты информации от утечки за счет электроакустического преобразования.

4.2.7. Для исключения возможности скрытного проключения ТА и прослушивания ведущихся в ЗП разговоров не рекомендуется устанавливать в них цифровые ТА цифровых АТС, имеющих выход в городскую АТС или к которой подключены абоненты, не являющиеся сотрудниками учреждения (предприятия).

В случае необходимости, рекомендуется использовать сертифицированные по требованиям безопасности информации цифровые АТС либо устанавливать в эти помещения аналоговые аппараты.

4.2.8. Ввод системы городского радиотрансляционного вещания на территорию учреждения (предприятия) рекомендуется осуществлять через радиотрансляционный узел (буферный усилитель), размещаемый в пределах контролируемой зоны.

При вводе системы городского радиовещания без буферного усилителя в ЗП следует использовать абонентские громкоговорители в защищенном от утечки информации исполнении, а также трехпрограммные абонентские громкоговорители в режиме приема 2-й и 3-й программы (с усилителем).

В случае использования однопрограммного или трехпрограммного абонентского громкоговорителя в режиме приема первой программы (без усиления) необходимо их отключать на период проведения конфиденциальных мероприятий.

4.2.9. В случае размещения электрочасовой станции внутри КЗ использование в ЗП электровторичных часов (ЭВЧ) возможно без средств защиты информации.

При установке электрочасовой станции вне КЗ в линии ЭВЧ, имеющие выход за пределы КЗ, рекомендуется устанавливать сертифицированные средства защиты информации.

4.2.10. Системы пожарной и охранной сигнализации ЗП должны строиться только по проводной схеме сбора информации (связи с пультом) и, как правило, размещаться в пределах одной с ЗП контролируемой зоне.

В качестве оконечных устройств пожарной и охранной сигнализации в ЗП рекомендуется

использовать изделия, сертифицированные по требованиям безопасности информации, или образцы средств, прошедшие специальные исследования и имеющие предписание на эксплуатацию.

4.2.11. Звукоизоляция ограждающих конструкций ЗП, их систем вентиляции и кондиционирования должна обеспечивать отсутствие возможности прослушивания ведущихся в нем разговоров из-за пределов ЗП.

Проверка достаточности звукоизоляции осуществляется аттестационной комиссией путем подтверждения отсутствия возможности разборчивого прослушивания вне ЗП разговоров, ведущихся в нем.

При этом уровень тестового речевого сигнала должен быть не ниже используемого во время штатного режима эксплуатации помещения.

Для обеспечения необходимого уровня звукоизоляции помещений рекомендуется оборудование дверных проемов тамбурами с двойными дверями, установка дополнительных рам в оконных проемах, уплотнительных прокладок в дверных и оконных притворах и применение шумопоглотителей на выходах вентиляционных каналов.

Если предложенными выше методами не удастся обеспечить необходимую акустическую защиту, следует применять организационно-режимные меры, ограничивая на период проведения конфиденциальных мероприятий доступ посторонних лиц в места возможного прослушивания разговоров, ведущихся в ЗП.

4.2.12. Для снижения вероятности перехвата информации по виброакустическому каналу следует организационно-режимными мерами исключить возможность установки посторонних (нештатных) предметов на внешней стороне ограждающих конструкций ЗП и выходящих из них инженерных коммуникаций (систем отопления, вентиляции, кондиционирования).

Для снижения уровня виброакустического сигнала рекомендуется расположенные в ЗП элементы инженерно-технических систем отопления, вентиляции оборудовать звукоизолирующими экранами.

4.2.13. В случае, если указанные выше меры защиты информации от утечки по акустическому и виброакустическому каналам недостаточны или нецелесообразны, рекомендуется применять метод активного акустического или виброакустического маскирующего зашумления.

Для этой цели должны применяться сертифицированные средства активной защиты.

4.2.14. При эксплуатации ЗП необходимо предусматривать организационно-режимные меры, направленные на исключение несанкционированного доступа в помещение:

- двери ЗП в период между мероприятиями, а также в нерабочее время необходимо запирать на ключ;
- выдача ключей от ЗП должна производиться лицам, работающим в нем или ответственным за это помещение;
- установка и замена оборудования, мебели, ремонт ЗП должны производиться только по согласованию и под контролем подразделения (специалиста) по защите информации учреждения (предприятия).

4.3. Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения кинофильмов

4.3.1. В качестве оборудования систем звукоусиления, предназначенных для обслуживания проводимых в ЗП закрытых мероприятий, и систем звукового сопровождения кинофильмов, содержащих конфиденциальные сведения, необходимо использовать оборудование, удовлетворяющее требованиям стандартов по электромагнитной совместимости России, Европейских стран, США (например, ГОСТ 22505-97). В случае необходимости, для повышения уровня защищенности рекомендуется

применять оборудование, сертифицированное по требованиям безопасности информации или прошедшее специальные исследования и имеющее предписание на эксплуатацию.

4.3.2. Системы звукоусиления должны выполняться по проводной схеме передачи информации экранированными проводами и располагаться в пределах КЗ.

С целью уменьшения побочных электромагнитных излучений целесообразно использовать систему звукоусиления с рассредоточенной системой звукоизлучателей, т.е. следует отдавать предпочтение системам с большим количеством оконечных устройств малой мощности перед системами с малым количеством оконечных устройств большой мощности.

В качестве оконечных устройств рекомендуется использовать звуковые колонки, выпускаемые в защищенном исполнении.

Можно использовать выпускаемые в обычном исполнении громкоговорители с экранированными магнитными цепями (например: 0,5ГДШ-5, 0,5ГД-54, 1ГДШ-2, 1ГДШ-6, 1ГДШ-28, 2ГДШ-3, 2ГДШ-4, 3ГДШ-1) или укомплектованные ими звуковые колонки (например: 2КЗ-7, 6КЗ-8, 12КЗ-18).

В этом случае звуковые колонки (громкоговорители) следует заэкранировать по электрическому полю с помощью металлической сетки с ячейкой не более 1 мм^2 , заземляемой через экранирующую оплетку подводящего кабеля.

4.3.3. В системах звукоусиления рекомендуется применять аппаратуру с симметричными входными и выходными цепями. В случае использования аппаратуры с несимметричным выходом, линии оконечных устройств следует подключать к оконечным усилителям через симметрирующие трансформаторы, устанавливаемые в непосредственной близости от оконечных усилителей.

4.3.4. В качестве усилительного оборудования рекомендуется использовать усилители в металлических экранах с возможностью их заземления.

4.3.5. Коммутационное и распределительное оборудование (распределительные, входные и выходные щитки подключения) следует размещать в металлических шкафах (коробках). На корпусах шкафов (коробок) необходимо предусмотреть клеммы (винты) для их заземления и приспособления для опечатывания.

4.3.6. Усилительное и оконечное оборудование СЗУ, СЗСК следует размещать на возможно большем расстоянии относительно границы контролируемой зоны.

4.3.7. Система электропитания и заземления должна соответствовать требованиям “Правил устройства электроустановок (ПУЭ)”.

Рекомендуется электропитание и заземление аппаратуры СЗУ и СЗСК осуществлять от подстанции и на заземлитель, расположенные в пределах КЗ.

4.4. Защита информации при проведении звукозаписи

4.4.1. Запись и воспроизведение конфиденциальной речевой информации аппаратурой звукозаписи разрешается производить только в ЗП.

4.4.2. Для записи (воспроизведения) конфиденциальной информации должны применяться магнитофоны (диктофоны), удовлетворяющие требованиям стандартов по электромагнитной совместимости России, Европейских стран, США (например, ГОСТ 22505-97). Для повышения уровня защищенности информации рекомендуется использовать магнитофоны (диктофоны), сертифицированные по требованиям безопасности информации или прошедшие специальные исследования и имеющие предписание на эксплуатацию.

4.4.3. Носители информации (магнитные ленты, кассеты) должны учитываться и храниться в подразделениях учреждения (предприятия) в порядке, установленном для конфиденциальной информации.

В учреждении (предприятии) должно быть назначено должностное лицо, ответственное за хранение и использование аппаратуры звукозаписи конфиденциальной

информации, и обеспечено хранение и использование этой аппаратуры, исключающее несанкционированный доступ к ней.

4.5. Защита речевой информации при её передаче по каналам связи

Передача конфиденциальной речевой информации по открытым проводным каналам связи, выходящим за пределы КЗ, и радиоканалам должна быть исключена.

При необходимости передачи конфиденциальной информации следует использовать защищенные линии связи (например, защищенные волоконно-оптические), устройства скремблирования или криптографической защиты.

Используемые средства защиты информации должны быть сертифицированы по требованиям безопасности информации.

5. ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

5.1. Общие требования и рекомендации

5.1.1. Система (подсистема) защиты информации, обрабатываемой в автоматизированных системах различного уровня и назначения, должна предусматривать комплекс организационных, программных, технических и, при необходимости, криптографических средств и мер по защите информации при ее автоматизированной обработке и хранении, при ее передаче по каналам связи.

5.1.2. Основными направлениями защиты информации являются:

- обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения и подделки за счет НСД и специальных воздействий;
- обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

5.1.3. В качестве основных мер защиты информации рекомендуются:

- документальное оформление перечня сведений конфиденциального характера с учетом ведомственной и отраслевой специфики этих сведений;
- реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и связанным с ее использованием работам, документам;
- ограничение доступа персонала и посторонних лиц в защищаемые помещения и помещения, где размещены средства информатизации и коммуникации, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей АС и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;
- учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение;
- использование СЗЗ, создаваемых на основе физико-химических технологий для контроля доступа к объектам защиты и для защиты документов от подделки;
- необходимое резервирование технических средств и дублирование массивов и носителей информации;
 - использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;
 - использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;
 - использование сертифицированных средств защиты информации;
 - размещение объектов защиты на максимально возможном расстоянии относительно границы КЗ;
 - размещение понижающих трансформаторных подстанций электропитания и контуров заземления объектов защиты в пределах КЗ;
 - развязка цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
 - электромагнитная развязка между линиями связи и другими цепями ВТСС, выходящими за пределы КЗ, и информационными цепями, по которым

- циркулирует защищаемая информация;
- использование защищенных каналов связи (защищенных ВОЛС и криптографических средств ЗИ;
- размещение дисплеев и других средств отображения информации, исключающее несанкционированный просмотр информации;
- организация физической защиты помещений и собственно технических средств с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации, исключающих нахождение внутри контролируемой зоны технических средств разведки или промышленного шпионажа;
- криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи (при необходимости, определяемой особенностями функционирования конкретных АС и систем связи);
- предотвращение внедрения в автоматизированные системы программ-вирусов, программных закладок.

Обязательность тех или иных мер для защиты различных видов конфиденциальной информации конкретизирована в последующих подразделах документа.

5.1.4. В целях дифференцированного подхода к защите информации, обрабатываемой в АС различного уровня и назначения, осуществляемого в целях разработки и применения необходимых и достаточных мер и средств защиты информации, проводится классификация автоматизированных систем (форма акта классификации АС приведена в приложении № 1).

5.1.5. Классифицируются АС любого уровня и назначения. Классификация АС осуществляется на основании требований РД Гостехкомиссии России “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации” и настоящего раздела документа.

5.1.6. Классификации подлежат все действующие, но ранее не классифицированные, и разрабатываемые АС, предназначенные для обработки конфиденциальной информации.

5.1.7. Если АС, классифицированная ранее, включается в состав вычислительной сети или системы и соединяется с другими техническими средствами линиями связи различной физической природы, образуемая при этом АС более высокого уровня классифицируется в целом, а в отношении АС нижнего уровня классификация не производится.

Если объединяются АС различных классов защищенности, то интегрированная АС должна классифицироваться по высшему классу защищенности входящих в нее АС, за исключением случаев их объединения посредством межсетевого экрана, когда каждая из объединяющихся АС может сохранять свой класс защищенности. Требования к используемым при этом межсетевым экранам изложены в подразделе 5.9.

5.1.8. При рассмотрении и определении режима обработки данных в АС учитывается, что индивидуальным (монопольным) режимом обработки считается режим, при котором ко всей обрабатываемой информации, к программным средствам и носителям информации этой системы допущен только один пользователь.

Режим, при котором различные пользователи, в т.ч. обслуживающий персонал и программисты, работают в одной АС, рассматривается как коллективный. Коллективным режимом работы считается также и последовательный во времени режим работы различных пользователей и обслуживающего персонала.

5.1.9. В случае, когда признаки классифицируемой АС (п. 1.7. РД Гостехкомиссии России “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите

информации”) не совпадают с предложенными в РД (п. 1.9) группами по особенностям обработки информации в АС, то при классификации выбирается наиболее близкая группа защищенности с предъявлением к АС соответствующих дополнительных требований по защите информации. (Например, однопользовательская АС с информацией различного уровня конфиденциальности по формальным признакам не может быть отнесена к 3 группе защищенности. Однако, если дополнительно реализовать в такой системе управление потоками информации, то необходимый уровень защиты будет обеспечен).

5.1.10. Конкретные требования по защите информации и мероприятия по их выполнению определяются в зависимости от установленного для АС класса защищенности. Рекомендуемые классы защищенности АС, СЗЗ, средств защиты информации по уровню контроля отсутствия недеklarированных возможностей, а также показатели по классам защищенности СВТ и МЭ от несанкционированного доступа к информации приведены в приложении № 7.

5.1.11. Лица, допущенные к автоматизированной обработке конфиденциальной информации, несут ответственность за соблюдение ими установленного в учреждении (на предприятии) порядка обеспечения защиты этой информации.

Для получения доступа к конфиденциальной информации они должны изучить требования настоящего документа, других нормативных документов по защите информации, действующих в учреждении (на предприятии) в части их касающейся.

5.2. Основные требования и рекомендации по защите служебной тайны и персональных данных

При разработке и эксплуатации АС, предполагающих использование информации, составляющей служебную тайну, а также персональных данных должны выполняться следующие основные требования.

5.2.1. Организация, состав и содержание проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны отвечать требованиям раздела 3.

5.2.2. В учреждении (на предприятии) должны быть документально оформлены перечни сведений, составляющих служебную тайну, и персональных данных, подлежащих защите. Эти перечни могут носить как обобщающий характер в области деятельности учреждения (предприятия), так и иметь отношение к какому-либо отдельному направлению работ. Все исполнители должны быть ознакомлены с этими перечнями в части их касающейся.

5.2.3. В соответствии с РД Гостехкомиссии России “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации” устанавливается следующий порядок классификации АС в зависимости от вида сведений конфиденциального характера:

- АС, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Г;
- АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д.

5.2.4. Для обработки информации, составляющей служебную тайну, а также для обработки персональных данных следует использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96 СанПиН 2.2.2.542-96).

Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.

5.2.5. Для передачи информации по каналам связи, выходящим за пределы КЗ, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации. Применяемые средства защиты информации должны быть сертифицированы.

5.2.6. Носители информации на магнитной (магнитно-оптической) и бумажной основе должны учитываться, храниться и уничтожаться в подразделениях учреждений (предприятий) в порядке, установленном для служебной информации ограниченного распространения, с пометкой “Для служебного пользования”.

5.2.7. Доступ к информации исполнителей (пользователей, обслуживающего персонала) осуществляется в соответствии с разрешительной системой допуска исполнителей к документам и сведениям конфиденциального характера, действующей в учреждении (на предприятии).

5.2.8. При необходимости указанный минимальный набор рекомендуемых организационно-технических мер защиты информации по решению руководителя предприятия может быть расширен.

5.3. Основные рекомендации по защите информации, составляющей коммерческую тайну

При разработке и эксплуатации АС, предполагающих использование сведений, составляющих коммерческую тайну, рекомендуется выполнение следующих основных организационно-технических мероприятий:

5.3.1. На предприятии следует документально оформить “Перечень сведений, составляющих коммерческую тайну”. Все исполнители должны быть ознакомлены с этим “Перечнем”.

5.3.2. При организации разработки и эксплуатации АС с использованием таких сведений следует ориентироваться на порядок, приведенный в разделе 3. Оформить порядок разработки и эксплуатации таких АС документально.

5.3.3. Рекомендуется относить АС, обрабатывающие информацию, составляющую коммерческую тайну, режим защиты которой определяет ее собственник, по уровню защищенности к классам ЗБ, 2Б и не ниже 1Д (если по решению руководителя предприятия не предъявляются более высокие требования).

5.3.4. Рекомендуется для обработки информации, составляющей коммерческую тайну, использовать средства вычислительной техники, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96 СанПиН 2.2.2.542-96).

Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.

5.3.5. Для передачи информации по каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи или предназначенные для этого криптографические средства защиты информации.

5.3.6. Следует установить на предприятии порядок учета, хранения и уничтожения носителей информации на магнитной (магнитно-оптической) и бумажной основе в научных, производственных и функциональных подразделениях, а также разработать и ввести в действие разрешительную систему допуска исполнителей документам и сведениям, составляющим коммерческую тайну.

Указанный минимальный набор рекомендуемых организационно-технических мероприятий по решению руководителя предприятия может быть расширен.

Решение о составе и содержании мероприятий, а также используемых средств защиты информации принимается руководителем предприятия по результатам обследования создаваемой (модернизируемой) АС с учетом важности (ценности) защищаемой информации.

5.4. Порядок обеспечения защиты конфиденциальной информации при эксплуатации АС

5.4.1. Организация эксплуатации АС и СЗИ в ее составе осуществляется в соответствии с установленным в учреждении (на предприятии) порядком, в том числе технологическими инструкциями по эксплуатации СЗИ НСД для пользователей, администраторов АС и работников службы безопасности.

5.4.2. Для обеспечения защиты информации в процессе эксплуатации АС рекомендуется предусматривать соблюдение следующих основных положений и требований:

- допуск к защищаемой информации лиц, работающих в АС (пользователей, обслуживающего персонала), должен производиться в соответствии с установленным разрешительной системой допуска порядком;
- на период обработки защищаемой информации в помещениях, где размещаются ОТСС, могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации; допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в эти помещения только с санкции руководителя учреждения (предприятия) или руководителя службы безопасности;
- в случае размещения в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации;
- по окончании обработки защищаемой информации или при передаче управления другому лицу пользователь обязан произвести стирание временных файлов на несъёмных носителях информации и информации в оперативной памяти. Одним из способов стирания информации в оперативной памяти является перезагрузка ПЭВМ;
- изменение или ввод новых программ обработки защищаемой информации в АС должен осуществляться совместно разработчиком АС и администратором АС;
- при увольнении или перемещении администраторов АС руководителем учреждения (предприятия) по согласованию со службой безопасности должны быть приняты меры по оперативному изменению паролей, идентификаторов и ключей шифрования.

5.4.3. Все носители информации на бумажной, магнитной, оптической (магнито-оптической) основе, используемые в технологическом процессе обработки информации в АС, подлежат учету в том производственном, научном или функциональном подразделении, которое является владельцем АС, обрабатывающей эту информацию.

5.4.4. Учет съёмных носителей информации на магнитной или оптической основе (гибкие магнитные диски, съёмные накопители информации большой емкости или картриджи, съёмные пакеты дисков, иные магнитные, оптические или магнито-оптические диски, магнитные ленты и т.п.), а также распечаток текстовой, графической и иной информации на бумажной или пластиковой (прозрачной) основе осуществляется по карточкам или журналам установленной формы, в том числе автоматизировано с использованием средств вычислительной техники. Журнальная форма учета может использоваться в АС с небольшим объемом документооборота.

5.4.5. Съёмные носители информации на магнитной или оптической основе в зависимости

от характера или длительности использования допускается учитывать совместно с другими документами по установленным для этого учетным формам.

При этом перед выполнением работ сотрудником, ответственным за их учет, на этих носителях информации предварительно проставляются любым доступным способом следующие учетные реквизиты: учетный номер и дата, пометка “Для служебного пользования”, номер экземпляра, подпись этого сотрудника, а также другие возможные реквизиты, идентифицирующие этот носитель.

5.4.6. Распечатки допускается учитывать совместно с другими традиционными печатными документами по установленным для этого учетным формам.

5.4.7. Временно не используемые носители информации должны храниться пользователем в местах, недоступных для посторонних лиц.

5.5. Защита конфиденциальной информации на автоматизированных рабочих местах на базе автономных ПЭВМ

5.5.1. Автоматизированные рабочие места на базе автономных ПЭВМ являются автоматизированными системами, обладающими всеми основными признаками АС. Информационным каналом обмена между такими АС являются носители информации на магнитной (магнитно-оптической) и бумажной основе.

В связи с этим порядок разработки и эксплуатации АРМ на базе автономных ПЭВМ по составу и содержанию проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны полностью отвечать требованиям настоящего документа.

5.5.2. АС на базе автономных ПЭВМ в соответствии с требованиями РД Гостехкомиссии России “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации” должны быть классифицированы и отнесены:

- к 3 группе АС, если в ней работает только один пользователь, допущенный ко всей информации АС;
- ко 2 и 1 группе АС, если в ней последовательно работают несколько пользователей с равными или разными правами доступа (полномочиями), соответственно.

Примечание: При использовании на автономной ПЭВМ технологии обработки информации на съемных накопителях большой емкости, классификация АС производится на основании анализа режима доступа пользователей АС к информации на используемом съемном носителе (либо одновременно используемом их комплексе).

5.6. Защита информации при использовании съемных накопителей информации большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ

5.6.1. Данная информационная технология предусматривает запись на загружаемый съемный накопитель информации большой емкости одновременно общесистемного (ОС, СУБД) и прикладного программного обеспечения, а также обрабатываемой информации одного или группы пользователей.

В качестве устройств для работы по этой технологии могут быть использованы накопители на магнитном, магнитно-оптическом или лазерном дисках различной конструкции, как встроенные (съемные), так и выносные. Одновременно может быть установлено несколько съемных накопителей информации большой емкости.

Несъемные накопители должны быть исключены из конфигурации ПЭВМ.

Основной особенностью применения данной информационной технологии для АРМ на

базе автономных ПЭВМ с точки зрения защиты информации является исключение этапа хранения на ПЭВМ в нерабочее время информации, подлежащей защите.

Эта особенность может быть использована для обработки защищаемой информации без применения сертифицированных средств защиты информации от НСД и использования средств физической защиты помещений этих АРМ.

5.6.2. На этапе предпроектного обследования необходимо провести детальный анализ технологического процесса обработки информации, обращая внимание, прежде всего, на технологию обмена информацией (при использовании съемных накопителей информации большой емкости или гибких магнитных дисков (ГМД или дискет) с другими АРМ, как использующими, так и не использующими эту информационную технологию, на создание условий, исключающих попадание конфиденциальной информации на неучтенные носители информации, несанкционированное ознакомление с этой информацией, на организацию выдачи информации на печать.

5.6.3. Обмен конфиденциальной информацией между АРМ должен осуществляться только на учтенных носителях информации с учетом допуска исполнителей, работающих на АРМ, к переносимой информации.

5.6.4. На рабочих местах исполнителей, работающих по этой технологии, во время работы, как правило, не должно быть неучтенных накопителей информации.

В случае формирования конфиденциальных документов с использованием, как текстовой, так и графической информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть “закрыты на запись”.

Условия и порядок применения таких процедур должны быть отражены в технологии обработки информации, использующей съемные накопители информации большой емкости.

5.6.5. При использовании в этой технологии современных средств вычислительной техники, оснащенных энергонезависимой, управляемой извне перезаписываемой памятью, так называемых Flash-Bios (FB), необходимо обеспечить целостность записанной в FB информации. Для обеспечения целостности, как перед началом работ, с конфиденциальной информацией при загрузке ПЭВМ, так и по их окончании, необходимо выполнить процедуру проверки целостности FB. При несовпадении необходимо восстановить (записать первоначальную версию) FB, поставить об этом в известность руководителя подразделения и службу безопасности, а также выяснить причины изменения FB.

5.6.6. Должна быть разработана и по согласованию с службой безопасности утверждена руководителем учреждения (предприятия) технология обработки конфиденциальной информации, использующая съемные накопители информации большой емкости и предусматривающая вышеуказанные, а также другие вопросы защиты информации, имеющие отношение к условиям размещения, эксплуатации АРМ, учету носителей информации, а также другие требования, вытекающие из особенностей функционирования АРМ.

5.7. Защита информации в локальных вычислительных сетях

5.7.1. Характерными особенностями ЛВС являются распределенное хранение файлов, удаленная обработка данных (вычисления) и передача сообщений (электронная почта), а также сложность проведения контроля за работой пользователей и состоянием общей безопасности ЛВС.

5.7.2. Средства защиты информации от НСД должны использоваться во всех узлах ЛВС независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС и требуют постоянного квалифицированного сопровождения со стороны администратора безопасности информации.

5.7.3. Информация, составляющая служебную тайну, и персональные данные могут

обрабатываться только в изолированных ЛВС, расположенных в пределах контролируемой зоны, или в условиях, изложенных в пунктах 5.8.4. и 5.8.5. следующего подраздела.

5.7.4. Класс защищенности ЛВС определяется в соответствии с требованиями РД Гостехкомиссии России “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”.

5.7.5. Для управления ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, в дополнение к системным администраторам (администраторам ЛВС) могут быть назначены администраторы по безопасности информации, имеющие необходимые привилегии доступа к защищаемой информации ЛВС.

5.7.6. Состав пользователей ЛВС должен устанавливаться по письменному разрешению руководства предприятия (структурного подразделения) и строго контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.

5.7.7. Каждый администратор и пользователь должен иметь уникальные идентификаторы и пароли, а в случае использования криптографических средств защиты информации - ключи шифрования для криптографических средств, используемых для защиты информации при передаче ее по каналам связи и хранения, и для систем электронной цифровой подписи.

5.8. Защита информации при межсетевом взаимодействии

5.8.1. Положения данного подраздела относятся к взаимодействию локальных сетей, ни одна из которых не имеет выхода в сети общего пользования типа Internet.

5.8.2. Взаимодействие ЛВС с другими вычислительными сетями должно контролироваться с точки зрения защиты информации. Коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах КЗ.

5.8.3. При конфигурировании коммуникационного оборудования (маршрутизаторов, концентраторов, мостов и мультиплексоров) и прокладке кабельной системы ЛВС рекомендуется учитывать разделение трафика по отдельным сетевым фрагментам на производственной основе и видам деятельности предприятия.

5.8.4. Подключение ЛВС к другой автоматизированной системе (локальной или неоднородной вычислительной сети) иного класса защищенности должно осуществляться с использованием МЭ, требования к которому определяются РД Гостехкомиссии России “Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации”.

5.8.5. Для защиты конфиденциальной информации при ее передаче по каналам связи из одной АС в другую необходимо использовать:

- в АС класса 1Г - МЭ не ниже класса 4;
- в АС класса 1Д и 2Б, 3Б - МЭ класса 5 или выше.

Если каналы связи выходят за пределы КЗ, необходимо использовать защищенные каналы связи, защищенные волоконно-оптические линии связи либо сертифицированные криптографические средства защиты.

5.9. Защита информации при работе с системами управления базами данных

5.9.1. При работе с системами управления базами данных (СУБД) и базами данных (БД) необходимо учитывать следующие особенности защиты информации от НСД:

- в БД может накапливаться большой объем интегрированной информации

по различным тематическим направлениям, предназначенной для различных пользователей;

- БД могут быть физически распределены по различным устройствам и узлам сети;
- БД могут включать информацию различного уровня конфиденциальности;
- разграничение доступа пользователей к БД средствами операционной системы и/или СЗИ НСД может осуществляться только на уровне файлов БД;
- разграничение доступа пользователей к объектам БД: таблицам, схемам, процедурам, записям, полям записей в базах данных и т.п., может осуществляться только средствами СУБД, если таковые имеются;
- регистрация действий пользователей при работе с объектами БД может осуществляться также только средствами СУБД, если таковые имеются;
- СУБД могут обеспечивать одновременный доступ многих пользователей (клиентов) к БД с помощью сетевых протоколов, при этом запросы пользователя к БД обрабатываются на сервере и результаты обработки направляются пользователям (клиентам).

5.9.2. С учетом указанных особенностей при создании БД рекомендуется:

- при выборе СУБД ориентироваться на операционные системы и СУБД, включающие либо штатные сертифицированные средства защиты информации от НСД, либо имеющие соответствующие сертифицированные дополнения в виде СЗИ НСД;
- при использовании СУБД, не имеющих средств разграничения доступа, производить разбиение БД на отдельные файлы, разграничение доступа к которым можно проводить средствами ОС и/или СЗИ НСД;
- при использовании современных СУБД, основанных на модели клиент-сервер, использовать их штатные средства защиты информации от НСД, применять средства регистрации (аудита) и разграничение доступа к объектам БД на основе прав, привилегий, ролей, представлений (VIEW), процедур и т.п.

6. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В НЕГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСАХ, ПРИ ВЗАИМОДЕЙСТВИИ АБОНЕНТОВ С ИНФОРМАЦИОННЫМИ СЕТЯМИ ОБЩЕГО ПОЛЬЗОВАНИЯ

6.1. Общие положения

6.1.1. В настоящем разделе приведены рекомендации, определяющие условия и порядок подключения абонентов к информационным сетям общего пользования (Сетям), а также рекомендации по обеспечению безопасности конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, режим защиты которой определяет собственник этих ресурсов (коммерческая тайна - в соответствии с п.2.3. СТР-К), при подключении и взаимодействии абонентов с этими сетями.

6.1.2. Данные рекомендации определены, исходя из требований РД “Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации”, настоящего документа, а также следующих основных угроз безопасности информации, возникающих при взаимодействии с информационными сетями общего пользования:

- несанкционированного доступа к информации, хранящейся и обрабатываемой во внутренних ЛВС (серверах, рабочих станциях) или на автономных ПЭВМ, как из Сетей, так и из внутренних ЛВС;
- несанкционированного доступа к коммуникационному оборудованию (маршрутизатору, концентратору, мосту, мультиплексору, серверу, Web/Proху серверу), соединяющему внутренние ЛВС учреждения (предприятия) с Сетями;
- несанкционированного доступа к данным (сообщениям), передаваемым между внутренними ЛВС и Сетями, включая их модификацию, имитацию и уничтожение;
- заражения программного обеспечения компьютерными “вирусами” из Сети, как посредством приема “зараженных” файлов, так и посредством E-mail, апплетов языка JAVA и объектов ActiveX Control;
- внедрения программных закладок с целью получения НСД к информации, а также дезорганизации работы внутренней ЛВС и ее взаимодействия с Сетями;
- несанкционированной передачи защищаемой конфиденциальной информации ЛВС в Сеть;
- возможности перехвата информации внутренней ЛВС за счет побочных электромагнитных излучений и наводок от основных технических средств, обрабатывающих такую информацию.

6.2. Условия подключения абонентов к Сети

6.2.1. Подключение к Сети абонентского пункта (АП) осуществляется по решению руководителя учреждения (предприятия) на основании соответствующего обоснования.

6.2.2. Обоснование необходимости подключения АП к Сети должно содержать:

- наименование Сети, к которой осуществляется подключение, и реквизиты организации-владельца Сети и провайдера Сети;
- состав технических средств для оборудования АП;
- предполагаемые виды работ и используемые прикладные сервисы Сети (E-Mail, FTP, Telnet, HTTP и т.п.) для АП в целом и для каждого абонента, в частности;
- режим подключения АП и абонентов к Сети (постоянный, в т.ч. круглосуточный, временный);
- состав общего и телекоммуникационного программного обеспечения АП и абонентов (ОС, клиентские прикладные программы для сети - Browsers и

- т.п.);
- число и перечень предполагаемых абонентов (диапазон используемых IP-адресов);
- меры и средства защиты информации от НСД, которые будут применяться на АП, организация-изготовитель, сведения о сертификации, установщик, конфигурация, правила работы с ними;
- перечень сведений конфиденциального характера, обрабатываемых (храняемых) на АП, подлежащих передаче и получаемых из Сети.

6.2.3. Право подключения к Сети АП, не оборудованного средствами защиты информации от НСД, может быть предоставлено только в случае обработки на АП информации с открытым доступом, оформленной в установленном порядке как разрешенной к открытому опубликованию. В этом случае к АП, представляющим собой автономную ПЭВМ с модемом, специальные требования по защите информации от НСД не предъявляются.

6.2.4. Подключение к Сети АП, представляющих собой внутренние (локальные) вычислительные сети, на которых обрабатывается информация, не разрешенная к открытому опубликованию, разрешается только после установки на АП средств защиты информации от НСД, отвечающих требованиям и рекомендациям, изложенным в подразделе 6.3.

6.3. Порядок подключения и взаимодействия абонентских пунктов с Сетью, требования и рекомендации по обеспечению безопасности информации

6.3.1. Подключение АП к Сети должно осуществляться в установленном порядке через провайдера Сети.

6.3.2. Подключение ЛВС предприятия (учреждения) к Сети должно осуществляться через средства разграничения доступа в виде МЭ (Firewall, Брандмауэр). Не допускается подключение ЛВС к Сети в обход МЭ. МЭ должны быть сертифицированы по требованиям безопасности информации.

6.3.3. Доступ к МЭ, к средствам его конфигурирования должен осуществляться только выделенным администратором с консоли. Средства удаленного управления МЭ должны быть исключены из конфигурации.

6.3.4. АП с помощью МЭ должен обеспечивать создание сеансов связи абонентов с внешними серверами Сети и получать с этих серверов только ответы на запросы абонентов. Настройка МЭ должна обеспечивать отказ в обслуживании любых внешних запросов, которые могут направляться на АП.

6.3.5. При использовании почтового сервера и Web-сервера предприятия, последние не должны входить в состав ЛВС АП и должны подключаться к Сети по отдельному сетевому фрагменту (через маршрутизатор).

6.3.6. На технических средствах АП должно находиться программное обеспечение только в той конфигурации, которая необходима для выполнения работ, заявленных в обосновании необходимости подключения АП к Сети (обоснование может корректироваться в установленном на предприятии порядке).

Не допускается активизация не включенных в обоснование прикладных серверов (протоколов) и не требующих привязок протоколов к портам.

6.3.7. Установку программного обеспечения, обеспечивающего функционирование АП, должны выполнять уполномоченные специалисты под контролем администратора. Абоненты АП не имеют права производить самостоятельную установку и модификацию указанного программного обеспечения, однако могут обращаться к администратору для проведения его экспертизы на предмет улучшения характеристик, наличия “вирусов”, замаскированных возможностей выполнения непредусмотренных действий. Вся ответственность за использование не прошедшего экспертизу и не рекомендованного к

использованию программного обеспечения целиком ложится на абонента АП. При обнаружении фактов такого рода администратор обязан логически (а при необходимости - физически вместе с включающей подсетью) отключить рабочее место абонента от Сети и ЛВС и поставить об этом в известность руководство.

6.3.8. Устанавливаемые межсетевые экраны должны соответствовать классу защищаемого АП (АС) и отвечать требованиям РД Гостехкомиссии России “Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации”.

6.3.9. СЗИ НСД, устанавливаемая на автономную ПЭВМ, рабочие станции и серверы внутренней ЛВС предприятия при обработке на них конфиденциальной информации, должна осуществлять:

- идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;
- контроль доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;
- регистрацию доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС, включая попытки НСД;
- регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов).

При этом СЗИ НСД должна запрещать запуск абонентом произвольных программ, не включенных в состав программного обеспечения АП.

Модификация конфигурации программного обеспечения АП должна быть доступна только со стороны администратора, ответственного за эксплуатацию АП.

Средства регистрации и регистрируемые данные должны быть недоступны для абонента.

СЗИ НСД должна быть целостной, т.е. защищенной от несанкционированной модификации и не содержащей путей обхода механизмов контроля.

Тестирование всех функций СЗИ НСД с помощью специальных программных средств должно проводиться не реже одного раза в год.

6.3.10. Технические средства АП должны быть размещены либо в отдельном помещении (при автономной ПЭВМ, подключенной к Сети), либо в рабочих помещениях абонентов с принятием организационных и технических мер, исключающих несанкционированную работу в Сети. В этих помещениях должно быть исключено ведение конфиденциальных переговоров, либо технические средства должны быть защищены с точки зрения электроакустики. В нерабочее время помещение автономной ПЭВМ либо соответствующего сервера сдается под охрану в установленном порядке.

6.3.11. При создании АП рекомендуется:

6.3.11.1. По возможности размещать МЭ для связи с внешними Сетями, Web-серверы, почтовые серверы в отдельном ЗП, доступ в которое имел бы ограниченный круг лиц (ответственные специалисты, администраторы). Периодически проверять работоспособность МЭ с помощью сканеров, имитирующих внешние атаки на внутреннюю ЛВС. Не следует устанавливать на МЭ какие-либо другие прикладные сервисы (СУБД, E-mail, прикладные серверы и т.п.).

6.3.11.2. При предоставлении абонентам прикладных сервисов исходить из принципа минимальной достаточности. Тем пользователям АП, которым не требуются услуги Сети, не предоставлять их. Пользователям, которым необходима только электронная почта (E-mail), предоставлять только доступ к ней. Максимальный перечень предоставляемых прикладных сервисов ограничивать следующими: E-mail, FTP, HTTP, Telnet.

6.3.11.3. При создании АП следует использовать операционные системы со встроенными функциями защиты информации от НСД, перечисленными в п.6.3.9, или использовать сертифицированные СЗИ НСД.

6.3.11.4. Эффективно использовать имеющиеся в маршрутизаторах средства

разграничения доступа (фильтрацию), включающие контроль по списку доступа, аутентификацию пользователей, взаимную аутентификацию маршрутизаторов.

6.3.11.5. В целях контроля за правомерностью использования АП и выявления нарушений требований по защите информации осуществлять анализ принимаемой из Сети и передаваемой в Сеть информации, в том числе на наличие “вирусов”. Копии исходящей электронной почты и отсылаемых в Сеть файлов следует направлять в адрес защищенного архива АП для последующего анализа со стороны администратора (службы безопасности).

6.3.11.6. Проводить постоянный контроль информации, помещаемой на Web-серверы предприятия. Для этого следует назначить ответственного (ответственных) за ведение информации на Web-сервере. Предусмотреть порядок размещения на Web-сервере информации, разрешенной к открытому опубликованию.

6.3.12. Приказом по учреждению (предприятию) назначаются лица (абоненты), допущенные к работам в Сети с соответствующими полномочиями, лица, ответственные за эксплуатацию указанного АП и контроль за выполнением мероприятий по обеспечению безопасности информации при работе абонентов в Сети (руководители подразделений и администраторы).

6.3.13. Вопросы обеспечения безопасности информации на АП должны быть отражены в инструкции, определяющей:

- порядок подключения и регистрации абонентов в Сети;
- порядок установки и конфигурирования на АП общесистемного, прикладного коммуникационного программного обеспечения (серверов, маршрутизаторов, шлюзов, мостов, межсетевых экранов, Browsers), их новых версий;
- порядок применения средств защиты информации от НСД на АП при взаимодействии абонентов с Сетью;
- порядок работы абонентов в Сети, в том числе с электронной почтой (E-mail), порядок выбора и доступа к внутренним и внешним серверам Сети (Web-серверам);
- порядок оформления разрешений на отправку данных в Сеть (при необходимости);
- обязанности и ответственность абонентов и администратора внутренней ЛВС по обеспечению безопасности информации при взаимодействии с Сетью;
- порядок контроля за выполнением мероприятий по обеспечению безопасности информации и работой абонентов Сети.

6.3.14. К работе в качестве абонентов Сети допускается круг пользователей, ознакомленных с требованиями по взаимодействию с другими абонентами Сети и обеспечению при этом безопасности информации и допускаемых к самостоятельной работе в Сети после сдачи соответствующего зачета.

6.3.15. Абоненты Сети обязаны:

- знать порядок регистрации и взаимодействия в Сети;
- знать инструкцию по обеспечению безопасности информации на АП;
- знать правила работы со средствами защиты информации от НСД, установленными на АП (серверах, рабочих станциях АП);
- уметь пользоваться средствами антивирусной защиты;
- после окончания работы в Сети проверить свое рабочее место на наличие “вирусов”.

6.3.16. Входящие и исходящие сообщения (файлы, документы), а также используемые при работе в Сети носители информации учитываются в журналах несекретного делопроизводства. При этом на корпусе (конверте) носителя информации наносится предупреждающая маркировка: “Допускается использование только в Сети

6.3.17. Для приемки в эксплуатацию АП, подключаемого к Сети, приказом по учреждению (предприятию) назначается аттестационная комиссия, проверяющая выполнение установленных требований и рекомендаций. Аттестационная комиссия в своей работе руководствуется требованиями и рекомендациями настоящего документа.

6.3.18. По результатам работы комиссии оформляется заключение, в котором отражаются следующие сведения:

- типы и номера выделенных технических средств АП, в т.ч. каждого абонента, их состав и конфигурация;
- состав общего и сервисного прикладного коммуникационного программного обеспечения (ОС, маршрутизаторов, серверов, межсетевых экранов, Browsers и т.п.) на АП в целом и на каждой рабочей станции абонента, в частности: логические адреса (IP-адреса), используемые для доступа в Сети;
- мероприятия по обеспечению безопасности информации, проведенные при установке технических средств и программного обеспечения, в т.ч. средств защиты информации от НСД, антивирусных средств, по защите информации от утечки по каналам ПЭМИН, наличие инструкции по обеспечению безопасности информации на АП.

6.3.19. При работе в Сети категорически запрещается:

- подключать технические средства (серверы, рабочие станции), имеющие выход в Сеть, к другим техническим средствам (сетям), не определенным в обосновании подключения к Сети;
- изменять состав и конфигурацию программных и технических средств АП без санкции администратора и аттестационной комиссии;
- производить отправку данных без соответствующего разрешения;
- использовать носители информации с маркировкой: “Допускается использование только в Сети _____” на рабочих местах других систем (в том числе и автономных ПЭВМ) без соответствующей санкции.

6.3.20. Ведение учета абонентов, подключенных к Сети, организуется в устанавливаемом в учреждении (на предприятии) порядке.

6.21. Контроль за выполнением мероприятий по обеспечению безопасности информации на АП возлагается на администраторов АП, руководителей соответствующих подразделений, определенных приказом по учреждению (предприятию), а также руководителя службы безопасности.

Приложение № 1
Для служебного пользования
Экз. № _____

Утверждаю
Руководитель предприятия

(Ф.И.О.)
“__” _____ “__” _____ г.

А К Т
классификации автоматизированной системы обработки информации

(наименование автоматизированной системы)

Комиссия в составе:

председатель: _____

члены комиссии: _____

рассмотрев исходные данные на автоматизированную систему обработки информации (АС) _____,

(наименование автоматизированной системы)

условия ее эксплуатации (многопользовательский, однопользовательский; с равными или разными правами доступа к информации), с учетом характера обрабатываемой информации (служебная тайна, коммерческая тайна, персональные данные и т.д.) и в соответствии с руководящими документами Гостехкомиссии России “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации” и “Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)”,

РЕШИЛА:

Установить АС _____

(наименование автоматизированной системы)

класс защищенности _____.

Председатель

Члены комиссии

АТТЕСТАТ СООТВЕТСТВИЯ

№ _____

(указывается полное наименование автоматизированной системы)

требованиям по безопасности информации**Выдан** “_____” _____ “_____” _____ Г.

1. Настоящим АТТЕСТАТОМ удостоверяется, что:

(приводится полное наименование автоматизированной системы)
 класса защищенности _____ соответствует требованиям нормативной документации по безопасности информации.

Состав комплекса технических средств автоматизированной системы (АС), с указанием заводских номеров, модели, изготовителя, номеров сертификатов соответствия, схема размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств, а также средств защиты (с указанием изготовителя и номеров сертификатов соответствия) указаны в техническом паспорте на АС.

2. Организационная структура, уровень подготовки специалистов, нормативно-методическое обеспечение обеспечивают поддержание уровня защищенности АС в процессе эксплуатации в соответствии с установленными требованиями.

3. Аттестация АС выполнена в соответствии с программой и методиками аттестационных испытаний, утвержденными руководителем предприятия (указываются номера документов).

4. С учетом результатов аттестационных испытаний в АС разрешается обработка конфиденциальной информации.

5. При эксплуатации АС запрещается:

- вносить изменения в комплектность АС, которые могут снизить уровень защищенности информации;
- проводить обработку защищаемой информации без выполнения всех мероприятий по защите информации;
- подключать к основным техническим средствам нештатные блоки и устройства;
- вносить изменения в состав, конструкцию, конфигурацию, размещение средств вычислительной техники;
- при обработке на ПЭВМ защищаемой информации подключать измерительную аппаратуру;
- допускать к обработке защищаемой информации лиц, не оформленных в установленном порядке;
- производить копирование защищаемой информации на неучтенные магнитные носители информации, в том числе для временного хранения информации;
- работать при отключенном заземлении;
- обрабатывать на ПЭВМ защищаемую информацию при обнаружении каких либо неисправностей.

6. Контроль за эффективностью реализованных мер и средств защиты возлагается

(наименование специалиста, подразделения по защите информации)

7. Подробные результаты аттестационных испытаний приведены в заключении аттестационной комиссии (№ ____ от ____) и протоколах испытаний.

8. “Аттестат соответствия” выдан на ____ года (лет), в течение которых должна быть обеспечена неизменность условий функционирования АС и технологии обработки защищаемой информации, могущих повлиять на характеристики защищенности АС

Руководитель аттестационной комиссии

(должность с указанием наименования предприятия) Ф.И.О.

“ ____ ” ____ ” ____ Г.

=====

Отметки органа надзора:

АТТЕСТАТ СООТВЕТСТВИЯ

№ _____

(указывается наименование защищаемого помещения)

требованиям по безопасности информации**Выдан “ _____ ” _____ ” _____ г.**

1. Настоящим АТТЕСТАТОМ удостоверяется, что

(полное наименование защищаемого помещения)

и установленное в нем оборудование соответствуют требованиям нормативных документов по безопасности информации (Заключение по результатам аттестации № _____ от _____) и в нем разрешается проведение конфиденциальных мероприятий.

Схема размещения помещения относительно границ контролируемой зоны, перечень установленного в нем оборудования, используемых средств защиты информации указаны в техническом паспорте на защищаемое помещение (ЗП).

2. Установленный порядок пользования ЗП позволяет осуществлять его эксплуатацию, расположенного в нем оборудования и средств защиты в соответствии с требованиями по защите конфиденциальной информации.

3. Повседневный контроль за выполнением установленных правил эксплуатации ЗП осуществляется

(наименование подразделения или должностного лица, осуществляющего контроль)

4. В ЗП запрещается проводить ремонтно-строительные работы, замену (установку новых) элементов интерьера, вносить изменения в состав оборудования и средства защиты информации, без согласования с

(наименование подразделения или должностного лица, осуществляющего контроль)

5. Лицо, ответственное за эксплуатацию защищаемого помещения, обязано незамедлительно извещать _____:

(наименование подразделения или должностного лица, осуществляющего контроль)

- о предполагаемых ремонтно-строительных работах и изменениях в размещении и монтаже установленного оборудования, технических средств и систем, средств защиты информации, в интерьере помещения;
 - о нарушениях в работе средств защиты информации;
 - о фактах несанкционированного доступа в помещение.

Руководитель аттестационной комиссии

(должность с указанием наименования предприятия) Ф.И.О.

“ _____ ” _____ ” _____ Г.

Отметки органа надзора:

Форма технического паспорта на защищаемое помещение

ТЕХНИЧЕСКИЙ ПАСПОРТ
на защищаемое помещение № _____

Составил

(Подпись специалиста подразделения по защите информации)

Ознакомлен

(Подпись лица, ответственного за помещение)

(Год)

ПАМЯТКА

по обеспечению режима безопасности и эксплуатации оборудования, установленного в защищаемом помещении № _____

(Примерный текст)

1. Ответственность за режим безопасности в защищаемом помещении (ЗП) и правильность использования установленных в нем технических средств несет лицо, которое постоянно в нем работает, или лицо, специально на то уполномоченное.
2. Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с подразделением (специалистом) по защите информации предприятия.
3. В нерабочее время помещение должно закрываться на ключ.
4. В рабочее время, в случае ухода руководителя, помещение должно закрываться на ключ или оставаться под ответственность лиц назначенных руководителем подразделения.
5. При проведении конфиденциальных мероприятий бытовая радиоаппаратура, установленная в помещении (телевизоры, радиоприемники и т.п.), должна отключаться от сети электропитания.
6. Должны выполняться предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и др. оборудования, установленного в помещении.
7. Запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой, пейджинговой и транкинговой связи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком, спикерфоном и имеющих выход в городскую АТС, следует отключать эти аппараты на время проведения конфиденциальных мероприятий.
8. Повседневный контроль за выполнением требований по защите помещения осуществляют лица, ответственные за помещение, и служба безопасности предприятия.
9. Периодический контроль эффективности мер защиты помещения осуществляется специалистами по защите информации.

Примечание: В памятку целесообразно включать и другие сведения, учитывающие особенности установленного в ЗП оборудования; действия персонала в случае срабатывания установленной в помещении сигнализации, порядок включения средств защиты, организационные меры защиты и т.п.

ПЕРЕЧЕНЬ ОБОРУДОВАНИЯ, УСТАНОВЛЕННОГО В ПОМЕЩЕНИИ

Вид оборудования	Тип	Учетный (зав.) номер	Дата установки	Класс ТС (ОТСС или ВТСС)	Сведения по сертификации, специследованиям и спецпроверкам

МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

(пример)

1. Телефонный аппарат коммутатора директора (инв.№ 15).
Выполнены требования предписания на эксплуатацию:
(Перечень предусмотренных мер защиты согласно предписанию).
2. Телефонный аппарат № 6-56.
На линию установлено защитное устройство "Сигнал-5", зав.№ 01530.
3. Пульт коммутатора.
Выполнены требования предписания на эксплуатацию:
(Перечень предусмотренных мер защиты согласно предписанию).
4. Часы электронные.
Выполнены требования предписания на эксплуатацию:
(Перечень предусмотренных мер защиты согласно предписанию).
5. Вход в помещение оборудован тамбуром, двери двойные, обшиты слоем ваты и дерматина. Дверные притворы имеют резиновые уплотнения.
6. Доступ к вентиляционным каналам, выходящим на чердак здания, посторонних лиц исключен (приводятся предусмотренные для этого меры).

Отметка о проверке средств защиты

Вид оборудования	Учетный номер	Дата проверки	Результаты проверки и № отчетного документа

Результаты аттестационного и периодического контроля помещения

Дата проведения	Результаты аттестации или периодического контроля, № отчетного документа	Подпись проверяющего

Форма технического паспорта на автоматизированную систему

УТВЕРЖДАЮ

Руководитель
автоматизированной системы_____
" ____ " _____ Г.

ТЕХНИЧЕСКИЙ ПАСПОРТ

(указывается полное наименование автоматизированной системы)

СОГЛАСОВАНО

РАЗРАБОТАЛ

(Представитель подразделения
по защите информации)
" ____ " _____ Г.

(Год)

1. Общие сведения об АС

1.1. Наименование АС: _____
(полное наименование АС)

1.2. Расположение АС:

(адрес, здание, строение, этаж, комнаты)

1.3. Класс АС:

(номер и дата акта классификации АС, класс АС)

2. Состав оборудования АС

2.1. Состав ОТСС:

Таблица 1

П Е Р Е Ч Е Н Ь
основных технических средств и систем,
входящих в состав АС _____

№ п/п	Тип ОТСС	Заводской номер	Сведения по сертификации, специсследованиям и спецпроверкам

2.2. Состав ВТСС объекта:

Таблица 2

П Е Р Е Ч Е Н Ь
вспомогательных технических средств, входящих в состав АС _____
(средств вычислительной техники, не участвующих в
обработке конфиденциальной информации)

№ п/п	Тип ВТСС	Заводской номер	Примечание

2.3. Структура, топология и размещение ОТСС относительно границ контролируемой зоны объекта:

структурная (топологическая) схема с указанием информационных связей между устройствами; схема размещения и расположения ОТСС на объекте с привязкой к границам контролируемой зоны, схема прокладки линий передачи конфиденциальной информации с привязкой к границам контролируемой зоны объекта.

2.4. Системы электропитания и заземления:

схемы электропитания и заземления ОТСС объекта. Схемы прокладки кабелей и шины заземления. Схемы расположения трансформаторной подстанции и заземляющих устройств с привязкой к границам контролируемой зоны объекта. Схемы электропитания

розеточной и осветительной сети объекта. Сведения о величине сопротивления заземляющего устройства.

2.5. Состав средств защиты информации:

Таблица 3

ПЕРЕЧЕНЬ средств защиты информации, установленных на АС _____

№ п/п	Наименование и тип и технического средства	Заводской номер	Сведения о сертификате	Место и дата установки

3. Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации:

инвентарные номера аттестата соответствия, заключения по результатам аттестационных испытаний, протоколов испытаний и даты их регистрации.

4. Результаты периодического контроля.

Таблица 4

Дата проведения	Наименование организации, проводившей проверку	Результаты проверки, номер отчетного документа

Лист регистрации изменений

Пример документального оформления перечня сведений конфиденциального характера

Для служебного пользования

Экз. №

Утверждаю
Руководитель предприятия

(Ф. И. О.)

“ ” _____ г.

ПЕРЕЧЕНЬ

сведений конфиденциального характера

№ п/п	Наименование сведений	Типы документов, где возможно появление сведений конфиденциального характера
1.	Сведения раскрывающие систему, средства защиты информации ЛВС предприятия от НСД, а также значения действующих кодов и паролей.	Руководство по защите конфиденциальной информации предприятия (учреждения).
2.	Сводный перечень работ предприятия на перспективу, на год (квартал).	План работ предприятия на перспективу.
3.	Сведения, содержащиеся в лицевых счетах пайщиков страховых взносов.	ст. 6, п. 2 ФЗ РФ “Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования”.
4.	Сведения, содержащиеся в индивидуальном лицевом счете застрахованного лица.	ст. 6, п. 2 ФЗ РФ “Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования”.
5.	Основные показатели задания на проектирование комплекса (установки). НОУ-ХАУ технологии - различные технические, коммерческие и другие сведения, оформленные в виде технической документации.	ТТЗ и ТЭО. Техническая документация с пометкой “Для служебного пользования”.
6.	Методические материалы, типовые технологические и конструктивные решения, разработанные на предприятии и используемые при проектировании.	Методики, проектная и конструкторская документация.
7.	Требования по обеспечению сохранения служебной тайны при выполнении работ на предприятии.	План работ предприятия на перспективу. Раздел ТТЗ на НИР (НИОКР).
8.	Порядок передачи служебной информации ограниченного распространения другим организациям.	Руководство по защите конфиденциальной информации предприятия (учреждения).

Приложение № 7
(справочное)

Классы защищенности от несанкционированного доступа к информации

Руководящий документ		Классы защищенности																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	Автоматизированные системы	1А	1Б	1В	1Г	1Д	2А	2Б	3А	3Б									
		1-я группа					2-я группа		3-я группа										
					*	*		*		*									
2	Средства вычислительной техники	4-я гр.	3-я группа			2-я группа		1-я гр.											
						*													
3	Межсетевые экраны				*														
4	Специальные защитные знаки													*					
5	Недекларированные возможности				*														

Примечания:

* – рекомендуемые классы защищенности от НСД к конфиденциальной информации.

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

2. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

3. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

4. Защита информации. Специальные защитные знаки. Классификация и общие требования.

5. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

Основные нормативные правовые акты и методические документы по защите
конфиденциальной информации.

1. Федеральный закон от 20.02. 95 г. №24-ФЗ “Об информации, информатизации и защите информации”.
2. Федеральный закон от 04.07.96 г. №85-ФЗ “Об участии в международном информационном обмене”.
3. Федеральный закон от 16.02.95 г. №15-ФЗ “О связи”.
4. Федеральный закон от 26.11.98 г. № 178-ФЗ “О лицензировании отдельных видов деятельности”.
5. Указ Президента Российской Федерации от 19.02.99 г. № 212 “Вопросы Государственной технической комиссии при Президенте Российской Федерации”.
6. “Доктрина информационной безопасности Российской Федерации”, утверждена Президентом Российской Федерации 9.09.2000 г. № Пр.-1895.
7. Указ Президента Российской Федерации от 17.12.97 г. № 1300 “Концепция национальной безопасности Российской Федерации” в редакции указа Президента Российской Федерации от 10.01.2000 г. №24.
8. Указ Президента Российской Федерации от 06.03.97 г. № 188 “Перечень сведений конфиденциального характера”.
9. Постановление Правительства Российской Федерации от 03.11.94 г. №1233 “Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органов исполнительной власти”.
10. Решение Гостехкомиссии России и ФАПСИ от 27.04.94 г. № 10 “Положение о государственном лицензировании деятельности в области защиты информации” (с дополнением).
11. Постановление Правительства Российской Федерации от 11.04.2000 г. № 326 “О “лицензировании отдельных видов деятельности”.
12. “Сборник руководящих документов по защите информации от несанкционированного доступа” Гостехкомиссия России, Москва, 1998 г.
13. ГОСТ Р 51275-99 “Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения”
14. ГОСТ Р 50922-96 “Защита информации. Основные термины и определения”
15. ГОСТ Р 51583-2000 “Порядок создания автоматизированных систем в защищенном исполнении”
16. ГОСТ Р 51241-98 “Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний”.
17. ГОСТ 12.1.050-86 “Методы измерения шума на рабочих местах”.
18. ГОСТ Р ИСО 7498-1-99 “Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель”.
19. ГОСТ Р ИСО 7498-2-99 “Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации”.
20. ГОСТ 2.114- 95 “Единая система конструкторской документации. Технические условия”.
21. ГОСТ 2.601- 95 “Единая система конструкторской документации. Эксплуатационные документы”.
22. ГОСТ 34.201- 89 “Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем”.
23. ГОСТ 34.602- 89 “Информационная технология. Комплекс стандартов на

- автоматизированные системы. Техническое задание на создании автоматизированных систем”.
24. ГОСТ 34.003- 90 “Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения”.
 25. РД Госстандарта СССР 50-682-89 “Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения”.
 26. РД Госстандарта СССР 50-34.698-90 “Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов”.
 27. РД Госстандарта СССР 50-680-89 “Методические указания. Автоматизированные системы. Основные положения”.
 28. ГОСТ 34.601- 90 “Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания”
 29. ГОСТ 6.38-90 “Система организационно-распорядительной документации. Требования к оформлению”.
 30. ГОСТ 6.10- 84 “Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники, ЕСКД, ЕСПД и ЕСТД”.
 31. ГОСТ Р-92 “Система сертификации ГОСТ. Основные положения”.
 32. ГОСТ 28195-89 “Оценка качества программных средств. Общие положения”.
 33. ГОСТ 28806-90 “Качество программных средств. Термины и определения”.
 34. ГОСТ Р ИСО\МЭК 9126- 90 “Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению”.
 35. ГОСТ 2.111-68 “Нормоконтроль”.
 36. ГОСТ Р 50739-95 “Средства вычислительной техники. Защита от несанкционированного доступа к информации”.
 37. РД Гостехкомиссии России “Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недеklarированных возможностей”, Москва, 1999г.
 38. РД Гостехкомиссии России “Средства защиты информации. Специальные общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам”, Москва, 2000г.
 39. ГОСТ В 15.201-83 “Тактико-техническое (техническое) задание на выполнение ОКР”.
 40. ГОСТ В 15.101-95 “Тактико-техническое (техническое) задание на выполнение НИР”
 41. ГОСТ В 15.102-84 “Тактико-техническое задание на выполнение аванпроекта”
 42. ГОСТ В 15.103-79 “Порядок выполнения аванпроекта. Основные положения”
 43. ГОСТ В 15.203-96 “Порядок выполнения ОКР. Основные положения”
 45. Решение Гостехкомиссии России от 14.03.95 г. № 32 “Типовое положение о Совете (Технической комиссии) министерства, ведомства, органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от ее утечки по техническим каналам”.
 46. Решение Гостехкомиссии России от 14.03.95 г. № 32 “Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации”.
 47. Решение Гостехкомиссии России от 14.03.95 г. № 32 “Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам на предприятии (в учреждении, организации)”.

48. СанПиН 2.2.2.542-96 “Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организация работы”.
49. ГОСТ Р 50948-96. “Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности”.
50. ГОСТ Р 50949-96 “Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности.”
51. ГОСТ Р 50923-96 “Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения.”
52. Решение Гостехкомиссии России от 03.10.95 г. № 42 “Типовые требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и ее утечки по техническим каналам на объекте”.