ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

УТВЕРЖДЕНЫ
Заместителем директора ФСТЭК России
15 февраля 2008 г.

ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОРГАНИЗАЦИИ И ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Примечание: пометка «для служебного пользования» снята Решением ФСТЭК России от 11 ноября 2009 г.

Содержание

Обозначения и сокращения

АВС – антивирусные средства
ВПр – вредоносная программа
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
МЭ – межсетевой экран
НДВ – недекларированные возможности
НСД – несанкционированный доступ
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭВМ – персональная электронно-вычислительная машина
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений

1. Термины и определения

В настоящем документе используются следующие термины и их определения:

Безопасность персональных данных – состояние защищенности персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Недекларированные возможности – функциональные возможности средств вычислительной техники и (или) программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

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

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы 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 и т.п.), средства защиты информации.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уполномоченное оператором лицо – лицо, которому на основании договора оператор поручает обработку персональных данных.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

2. Общие положения

2.1. Настоящий документ разработан на основе Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, с целью совершенствования методического обеспечения деятельности в данной области государственных и муниципальных органов, юридических и физических лиц, организующих и (или) осуществляющих обработку персональных данных (ПДн), определяющих цели и содержание обработки ПДн (операторов), а также заказчиков и разработчиков информационных систем персональных данных (ИСПДн) при решении ими задач по обеспечению безопасности ПДн.

2.2. Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Мероприятия по обеспечению безопасности ПДн формулируются в зависимости от класса ИСПДн, определяемого с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства.

2.3. Положения настоящего документа не распространяются на ИСПДн, обрабатывающие ПДн, отнесенные в установленном порядке к сведениям, составляющими государственную тайну. Порядок и содержание мероприятий по защите информации, содержащей сведения, составляющие государственную тайну, определяются в соответствии с нормативными и методическими документами в области защиты государственной тайны.

2.4. Настоящий документ является методическим документом, определяющим мероприятия по организации и техническому обеспечению безопасности ПДн (не криптографическими методами) при их обработке в ИСПДн, в интересах решения задач:

проведения мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

своевременного обнаружения фактов несанкционированного доступа (НСД) к ПДн;

недопущения воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;

постоянного контроля за обеспечением уровня защищенности ПДн.

Обеспечение безопасности ПДн с использованием криптографических методов в настоящем документе не рассматривается. Порядок организации и обеспечения указанных работ определяется в соответствии с нормативными документами Федеральной службы безопасности Российской Федерации.

2.5. Настоящий документ применяется для обеспечения безопасности ПДн при их обработке в ИСПДн следующих видов:

ИСПДн государственных органов, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных;

ИСПДн муниципальных органов, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных;

ИСПДн юридических лиц, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных;

ИСПДн физических лиц, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных (за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд).

2.6. Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ по созданию ИСПДн. Результатом этих работ должно являться создание системы (подсистемы) защиты персональных данных ИСПДн.

2.7. Для обеспечения безопасности ПДн при их обработке в ИСПДн осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в ИСПДн.

2.8. Основными мероприятиями по организации и техническому обеспечению безопасности ПДн в ИСПДн являются:

мероприятия по организации обеспечения безопасности ПДн, включая классификацию ИСПДн;

мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн, включающие мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с ПДн, мероприятия по закрытию технических каналов утечки ПДн при их обработке в информационных системах, мероприятия по защите ПДн от несанкционированного доступа и определению порядка выбора средств защиты ПДн при их обработке в ИСПДн.

2.9. При обработке ПДн в ИСПДн возможно возникновение угроз безопасности ПДн, включающих совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Модель угроз применительно к конкретной ИСПДн разрабатывается в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Выявление и учет угроз безопасности ПДн в конкретных условиях составляют основу для планирования и осуществления мероприятий, направленных на обеспечение безопасности ПДн при их обработке в ИСПДн.

3. Основные мероприятия по организации обеспечения безопасности персональных данных

3.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

3.2. Обязанности по реализации необходимых организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, возлагаются на оператора.

Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн оператором или уполномоченным им лицом должно назначаться структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности ПДн.

3.3. Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

3.4. Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы (подсистемы) защиты персональных данных (СЗПДн). Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

3.5. Рекомендуются следующие стадии создания СЗПДн:

предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;

стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;

стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

3.6. На предпроектной стадии по обследованию ИСПДн рекомендуются следующие мероприятия:

устанавливается необходимость обработки ПДн в ИСПДн;

определяется перечень ПДн, подлежащих защите от НСД;

определяются условия расположения ИСПДн относительно границ контролируемой зоны (КЗ);

определяются конфигурация и топология ИСПДн в целом и ее отдельных компонентов, 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 ИСПДн, условия их расположения, общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;

определяются режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;

определяется класс ИСПДн;

уточняется степень участия должностных лиц в обработке ПДн, характер их взаимодействия между собой;

определяются (уточняются) угрозы безопасности ПДн применительно к конкретным условиям функционирования ИСПДн (разработка частной модели угроз).

3.7. По результатам предпроектного обследования на основе настоящего документа с учетом установленного класса ИСПДн задаются конкретные требования по обеспечению безопасности ПДн, включаемые в техническое (частное техническое) задание на разработку СЗПДн.

3.8. Техническое (частное техническое) задание на разработку СЗПДн должно содержать:

обоснование разработки СЗПДн;

исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;

класс ИСПДн;

ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;

конкретизацию мероприятий и требований к СЗПДн;

перечень предполагаемых к использованию сертифицированных средств защиты информации;

обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;

состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

3.9. В целях дифференцированного подхода к обеспечению безопасности ПДн в зависимости от объема обрабатываемых ПДн и угроз безопасности жизненно важным интересам личности, общества и государства ИСПДн подразделяются на следующие классы:

класс 1 (К1) – ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

класс 2 (К2) – ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

класс 3 (К3) – ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

класс 4 (К4) – ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Классификация ИСПДн проводится оператором в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

3.10. На стадии проектирования и создания ИСПДн (СЗПДн) проводятся следующие мероприятия:

разработка задания и проекта проведения работ (в том числе строительных и строительно-монтажных) по созданию (реконструкции) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн;

выполнение работ в соответствии с проектной документацией;

обоснование и закупка совокупности используемых в ИСПДн серийно выпускаемых технических средств обработки, передачи и хранения информации;

разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

обоснование и закупка совокупности используемых в ИСПДн сертифицированных технических, программных и программно-технических средств защиты информации и их установка;

проведение сертификации по требованиям безопасности информации технических, программных и программно-технических средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные средства защиты информации;

разработка и реализация разрешительной системы доступа пользователей к обрабатываемой на ИСПДн информации;

определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации, с их обучением по направлению обеспечения безопасности ПДн;

разработка эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);

выполнение других мероприятий, характерных для конкретных ИСПДн и направлений обеспечения безопасности ПДн.

3.11. На стадии ввода в действие ИСПДн (СЗПДн) осуществляются:

выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;

опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации;

организация охраны и физической защиты помещений ИСПДн, исключающих несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации;

оценка соответствия ИСПДн требованиям безопасности ПДн.

Оценка соответствия ИСПДн требованиям безопасности ПДн проводится в виде:

для ИСПДн 1 и 2 классов – обязательной сертификации (аттестации) по требованиям безопасности информации;

для ИСПДн 3 класса – декларирования соответствия требованиям безопасности информации.

Для ИСПДн 4 класса оценка соответствия проводится по решению оператора.

3.12. Для ИСПДн, находящихся в эксплуатации до введения в действие Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», должен быть предусмотрен комплекс мероприятий по их доработке, обеспечивающий безопасность ПДн в соответствии с требованиями Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ и «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, в срок до 1 января 2010 г.

3.13. Для функционирующих ИСПДн доработка (модернизация) СЗПДн должна проводиться в случае, если:

изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);

изменился состав угроз безопасности ПДн в ИСПДн;

изменился класс ИСПДн.

3.14. В соответствии с положениями Федерального закона от 8 августа 2001 г. № 128 «О лицензировании отдельных видов деятельности» и требованиями постановления Правительства Российской Федерации от 16 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации» операторы ИСПДн при проведении мероприятий по обеспечению безопасности ПДн (конфиденциальной информации) при их обработке в ИСПДн 1,2 и 3 (распределенные системы) классов должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации в установленном порядке.

4. Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

4.1. В интересах технического обеспечения безопасности ПДн при их обработке в ИСПДн в зависимости от класса информационной системы должны быть реализованы следующие мероприятия:

мероприятия по защите от НСД и неправомерных действий к ПДн при их обработке в ИСПДн;

мероприятия по защите информации от утечки по техническим каналам.

4.2. В состав мероприятий по защите ПДн при их обработке в ИСПДн от НСД и неправомерных действий входят следующие мероприятия:

защита от НСД при однопользовательском режиме обработки ПДн;

защита от НСД при многопользовательском режиме обработки ПДн и равных правах доступа к ним субъектов доступа;

защита от НСД при многопользовательском режиме обработки ПДн и разных правах доступа;

защита информации при межсетевом взаимодействии ИСПДн;

антивирусная защита;

обнаружение вторжений.

Мероприятия по защите ПДн реализуются в рамках подсистем: управления доступом, регистрации и учета, обеспечения целостности, криптографической защиты, антивирусной защиты, обнаружения вторжений.

Мероприятия по обнаружению вторжений в ИСПДн проводятся в соответствии с требованиями нормативных документов Федеральной службы безопасности Российской Федерации.

Кроме этого, в ИСПДн должен проводиться контроль на наличие недекларированных возможностей в программном и программно-аппаратном обеспечении и анализ защищенности системного и прикладного программного обеспечения.

4.2.1. Для ИСПДн 4 класса перечень мероприятий по защите ПДн определяется оператором в зависимости от ущерба, который может быть нанесен вследствие несанкционированного или непреднамеренного доступа к ПДн.

4.2.2. Для ИСПДн 3 класса при однопользовательском режиме обработки ПДн должны проводиться следующие мероприятия:

а) в подсистеме управления доступом:

должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;

при наличии подключения ИСПДн к сетям общего пользования должно применяться межсетевое экранирование, при котором межсетевой экран (МЭ) должен обеспечивать принятие решения по фильтрации для каждого сетевого пакета независимо, идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ, возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия, регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова, контроль целостности своей программной и информационной части, фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств, фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов, фильтрацию с учетом любых значимых полей сетевых пакетов, восстановление после сбоев и отказов оборудования, возможность регламентного тестирования реализации правил фильтрации, процесса идентификации, аутентификации и регистрации действий администратора МЭ, контроль целостности программной и информационной части МЭ, восстановления после сбоев и отказов;

должна проводиться идентификация и аутентификация субъектов доступа при входе в средство защиты от программно-математических воздействий (ПМВ) и перед выполнением ими любых операций по управлению функциями средства защиты от ПМВ по паролю (или с использованием иного механизма аутентификации) условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

любые действия субъектов доступа по управлению функциями средства защиты от ПМВ должны выполняться только после проведения его успешной аутентификации;

должны быть предусмотрены механизмы блокирования доступа к средствам защиты от ПМВ при выполнении устанавливаемого числа неудачных попыток ввода пароля;

должна проводиться идентификация файлов, каталогов, программных модулей, внешних устройств, используемых средства защиты от ПМВ;

б) в подсистеме регистрации и учета:

должна осуществляться регистрация входа (выхода) субъекта доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку);

должна проводиться регистрация входа (выхода) субъектов доступа в средство защиты от ПМВ, регистрация загрузки и инициализации этого средства и ее программного останова. В параметрах регистрации указывается время и дата входа (выхода) субъекта доступа в средство защиты от ПМВ или загрузки (останова) этого средства, а также идентификатор субъекта доступа, инициировавшего данные действия;

должна проводиться регистрация событий проверки и обнаружения ПМВ. В параметрах регистрации указываются время и дата проверки или обнаружения ПМВ, идентификатор субъекта доступа, инициировавшего данные действия, характер выполняемых действий по проверке, тип обнаруженной вредоносной программы (ВПр), результат действий средства защиты по блокированию ПМВ;

должна проводиться регистрация событий по внедрению в средство защиты от ПМВ пакетов обновлений. В параметрах регистрации указываются время и дата обновления, идентификатор субъекта доступа, инициировавшего данное действие, версия и контрольная сумма пакета обновления;

должна проводиться регистрация событий запуска (завершения) работы модулей средства защиты от ПМВ. В параметрах регистрации указываются время и дата запуска (завершения) работы, идентификатор модуля, идентификатор субъекта доступа, инициировавшего данное действие, результат запуска (завершения) работы;

должна проводиться регистрация событий управления субъектом доступа функциями средства защиты от ПМВ. В параметрах регистрации указываются время и дата события управления каждой функцией, идентификатор и спецификация функции, идентификатор субъекта доступа, инициировавшего данное действие, результат действия;

должна проводиться регистрация событий попыток доступа программных средств к модулям средства защиты от ПМВ или специальным ловушкам. В параметрах регистрации указываются время и дата попытки доступа, идентификатор модуля, идентификатор и спецификация модуля средства защиты от ПМВ (специальной ловушки), результат попытки доступа;

должна проводиться регистрация событий отката для средства защиты от ПМВ. В параметрах регистрации указываются время и дата события отката, спецификация действий отката, идентификатор субъекта доступа, инициировавшего данное действие, результат действия;

данные регистрации должны быть защищены от их уничтожения или модификации нарушителем;

должны быть реализованы механизмы сохранения данных регистрации в случае сокращения отведенных под них ресурсов;

должны быть реализованы механизмы просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров;

должен проводиться автоматический непрерывный мониторинг событий, которые могут являться причиной реализации ПМВ (создание, редактирование, запись, компиляция объектов, которые могут содержать ВПр).

должен быть реализован механизм автоматического анализа данных регистрации по шаблонам типовых проявлений ПМВ с автоматическим их блокированием и уведомлением администратора безопасности;

в) в подсистеме обеспечения целостности:

должна быть обеспечена целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонентов СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ;

должна осуществляться физическая охрана ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации;

должно проводиться периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД;

должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности;

должна проводиться проверка целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм;

должны быть обеспечена возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности;

должны быть реализованы механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм;

г) в подсистеме антивирусной защиты:

должна проводиться автоматическая проверка на наличие ВПр или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВПр, по их типовым шаблонам и с помощью эвристического анализа;

должны быть реализованы механизмы автоматического блокирования обнаруженных ВПр путем их удаления из программных модулей или уничтожения;

должна выполняться регулярно (при первом запуске средств защиты ПДн от ПМВ и с устанавливаемой периодичностью) проверка на предмет наличия в них ВПр;

должна инициироваться автоматическая проверка ИСПДн на предмет наличия ВПр при выявлении факта ПМВ;

должен быть реализован механизм отката для устанавливаемого числа операций удаления ВПр из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВПр.

4.2.3. Для ИСПДн 2 класса при однопользовательском режиме обработки ПДн должны проводиться все мероприятия, соответствующие 3 классу, а также следующие мероприятия:

а) в подсистеме управления доступом:

при наличии подключения ИСПДн к сетям общего пользования должно проводиться межсетевое экранирование, при этом МЭ должен выполнять те же функции, что и для ИСПДн 3 класса, а также обеспечивать фильтрацию на транспортном уровне запросов на установление виртуальных соединений, фильтрацию на прикладном уровне запросов к прикладным сервисам, фильтрацию с учетом даты (времени), возможность аутентификации входящих
и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети, регистрацию и учет запросов на установление виртуальных соединений, локальную сигнализацию попыток нарушения правил фильтрации, блокирование доступа неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации
не подтвердилась, регистрацию действия администратора межсетевого экрана
по изменению правил фильтрации, возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа
регистрационной информации;

должны быть реализованы мероприятия по разграничению доступа к средствам защиты от ПМВ те же, что и для 3 класса ИСПДн;

б) в подсистеме обеспечения целостности дополнительно обеспечивается контроль целостности программной и информационной части МЭ по контрольным суммам;

в) в подсистеме антивирусной защиты должны проводиться те же мероприятия, что и в ИСПДн 3 класса, а также дополнительно в ИСПДн должен проводиться непрерывный автоматический мониторинг информационного обмена с внешней сетью с целью выявления ВПр.

4.2.4. Для ИСПДн 1 класса при однопользовательском режиме обработки ПДн должны проводиться все мероприятия, соответствующие 2 классу, а также следующие мероприятия:

а) в подсистеме управления доступом:

при наличии подключения ИСПДн к сетям общего пользования должно проводиться межсетевое экранирование, при этом МЭ должен выполнять те же функции, что и для ИСПДн 2 класса, и дополнительно обеспечивать возможность сокрытия субъектов (объектов) и (или) прикладных функций защищаемой ИСПДн, сигнализацию попыток нарушения правил фильтрации, регистрацию и учет запрашиваемых сервисов прикладного уровня, программируемую реакцию на события в МЭ, идентификацию
и аутентификацию администратора МЭ при его запросах на доступ по идентификатору (коду) и паролю временного действия, блокирование доступа неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату информации, контроль за целостностью своей программной и информационной части по контрольным суммам как в процессе загрузки, так и динамически, оперативное восстановление свойств экранирования;

должен быть реализован механизм ролевого разграничения доступа
ко всем модулям средств защиты от ПМВ и для выполнения всех функций управления средством, позволяющий определять права ролей субъектов
на доступ к модулям средства защиты от ПМВ и на выполнение функций управления этим средством;

должен быть реализован механизм контроля информационных потоков ко всем модулям средства защиты от ПМВ;

импорт и экспорт объектов (сообщений, данных, программ и т.п.) должен выполняться субъектом доступа со специальной ролью «оператора ввода/вывода»;

для каждого субъекта доступа должен быть определен перечень исполняемых модулей, которые он может активизировать;

должна проводиться идентификация и аутентификация субъектов доступа при входе в средство защиты от ПМВ и перед выполнением ими любых операций (распределенных по группам операций) по управлению функциями средства защиты от ПМВ, с использованием паролей (или иных механизмов аутентификации) условно-постоянного действия, при этом для каждой группы операций должен быть предусмотрен индивидуальный пароль;

аутентификационная информация субъектов доступа должна быть защищена от НСД нарушителя;

должны быть реализованы механизмы блокирования терминала субъекта доступа самим субъектом доступа или в случае истечения заданного интервала времени неактивности субъекта доступа;

должна проводиться автоматическая идентификация и аутентификация аппаратного обеспечения ИСПДн, необходимого для функционирования средства защиты от ПМВ;

б) в подсистеме регистрации и учета:

должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами ИСПДн с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности, спецификация устройства выдачи - логическое имя (номер) внешнего устройства;

должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

должно проводиться несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации;

должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютера и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов);

должен быть реализован механизм ролевого разграничения доступа ко всем модулям средства защиты от ПМВ и для выполнения всех функций управления средством, позволяющий определять права ролей субъектов на доступ к модулям средства и на выполнение функций управления средством;

импорт и экспорт объектов (сообщений, данных, программ и т.п.) должен выполняться субъектом доступа со специальной ролью «оператора ввода/вывода»;

для каждого субъекта доступа должен быть определен перечень исполняемых модулей, которые он может активизировать;

должна проводиться идентификация и аутентификация субъектов доступа при входе в средство защиты от ПМВ и перед выполнением ими любых операций (распределенных по группам операций) по управлению функциями средства защиты от ПМВ, с использованием паролей (или иных механизмов аутентификации) условно-постоянного действия, содержащих не менее устанавливаемого минимального числа символов, при этом для каждой группы операций должен быть предусмотрен индивидуальный пароль;

аутентификационная информация субъектов доступа должна быть защищена от НСД нарушителя;

должны быть реализованы механизмы блокирования терминала субъекта доступа самим субъектом доступа или в случае истечения заданного интервала времени неактивности субъекта доступа;

должна проводиться автоматическая идентификация и аутентификация аппаратного обеспечения ИСПДн, необходимого для функционирования средства защиты от ПМВ;

в) в подсистеме обеспечения целостности:

должна осуществляться физическая охрана ИСПДн (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается ИСПДн, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений ИСПДн;

должны использоваться сертифицированные средства защиты информации;

должен проводиться автоматический контроль корректности функционирования аппаратного обеспечения ИСПДн, необходимого для функционирования средства защиты от ПМВ;

должны быть реализованы механизмы автоматического восстановления средства защиты от ПМВ после сбоев, с обеспечением минимизации потерь информации при сбое;

средство защиты от ПМВ должна быть интегрирована в общую СЗПДн, при этом должно быть исключено дублирование механизмов защиты;

г) в подсистеме антивирусной защиты:

должен проводиться непрерывный согласованный по единому сценарию автоматический мониторинг информационного обмена по каналам ИСПДн с целью выявления проявлений ПМВ;

должна проводиться автоматическая проверка на наличие ПМВ при импорте в ИСПДн всех программных средств, которые могут содержать ВПр, путем проверочной их активизации в специальной изолированной виртуальной среде, моделирующей среду ИСПДн, с анализом их кода методами трассировки и отладки непосредственно во время активного состояния программных средств;

должны быть реализованы программные ловушки, имитирующие уязвимые для реализации ПМВ объекты ИСПДн, при этом места размещения ловушек и их проявления должны автоматически меняться с течением времени.

4.2.5. Для ИСПДн 3 класса при многопользовательском режиме обработки ПДн и равных правах доступа к ним разных пользователей должны проводиться следующие мероприятия:

а) в подсистеме управления доступом:

должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

при отсутствии подключения к сетям общего пользования в распределенной ИСПДн должны применяться МЭ, обеспечивающие выполнение тех же функций, что МЭ для ИСПДн, подключенных к сетям общего пользования и функционирующих в однопользовательском режиме;

при наличии подключения к сетям общего пользования в ИСПДн должны применяться МЭ, обеспечивающие выполнение тех же функций, что и МЭ для ИСПДн, подключенных к сетям общего пользования и функционирующих в однопользовательском режиме, а также дополнительно обеспечивающие возможность сокрытия субъектов (объектов) и (или) прикладных функций защищаемой сети, возможность трансляции сетевых адресов, дистанционную сигнализацию попыток нарушения правил фильтрации, регистрацию и учет запрашиваемых сервисов прикладного уровня, программируемую реакцию на события в МЭ, идентификацию и аутентификацию администратора МЭ при его

запросах на доступ по идентификатору (коду) и паролю временного действия, блокирование доступа неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась, методами, устойчивыми к пассивному и активному перехвату информации, контроль целостности своей программной и информационной части по контрольным суммам как в процессе загрузки, так и динамически, оперативное восстановление свойств экранирования;

должны быть проведены мероприятия по разграничению доступа к средствам защиты от ПМВ такие же, как и для ИСПДн 3 класса с однопользовательским режимом;

б) в подсистеме регистрации и учета:

должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная);

должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

должны быть проведены мероприятия по регистрации и учету применительно к средствам защиты от ПМВ такие же, как и для ИСПДн 3 класса с однопользовательским режимом;

в) в подсистеме обеспечения целостности:

должна быть обеспечена целостность программных средств в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонентов СЗИ, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;

должна осуществляться физическая охрана ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации, особенно в нерабочее время;

должно проводиться периодическое тестирование функций средств защиты информации в составе СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД;

должны быть в наличии средства восстановления средств защиты информации в составе СЗПДн, предусматривающие ведение двух копий программных средств защиты, их периодическое обновление и контроль работоспособности;

должны быть проведены мероприятия по обеспечению целостности средств защиты от ПМВ такие же, как и для ИСПДн 3 класса с однопользовательским режимом;

г) в подсистеме антивирусной защиты должны быть проведены мероприятия по защите от ПМВ такие же, как и для ИСПДн 3 класса с однопользовательским режимом.

4.2.6. Для ИСПДн 2 класса при многопользовательском режиме обработки ПДн и равных правах доступа к ним разных пользователей должны проводиться все мероприятия по 3 классу при многопользовательском режиме обработки ПДн, а также следующие мероприятия:

а) в подсистеме управления доступом:

должна осуществляться идентификация терминалов, технических средств обработки ПДн, узлов ИСПДн, каналов связи, внешних устройств ИСПДн по их логическим адресам (номерам);

должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

б) в подсистеме обеспечения целостности:

должно проводиться резервное копирование ПДн на отчуждаемые носители информации;

должны быть проведены мероприятия по обеспечению целостности средств защиты от ПМВ такие же, как и для ИСПДн 2 класса с однопользовательским режимом;

в) в подсистеме антивирусной защиты на всех технических средствах ИСПДн должен проводиться непрерывный согласованный по единому сценарию автоматический мониторинг информационного обмена в ИСПДн с целью выявления проявлений ПМВ.

4.2.7. Для ИСПДн 1 класса при многопользовательском режиме обработки ПДн и равных правах доступа к ним разных пользователей должны проводиться все мероприятия по 2 классу при многопользовательском режиме обработки ПДн, а также следующие мероприятия:

а) в подсистеме управления доступом должно осуществляться управление потоками информации с помощью меток конфиденциальности, при этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации;

б) в подсистеме регистрации и учета:

должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами ИСПДн с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ;

должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный – несанкционированный);

должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого файла;

должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров в составе ИСПДн, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого объекта – логическое имя (номер);

должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютеров и внешних накопителей. Очистка

осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов);

в) в криптографической подсистеме:

должно осуществляться шифрование ПДн, записываемых на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;

должны использоваться сертифицированные средства криптографической защиты.

г) в подсистеме обеспечения целостности:

должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы средств защиты информации в составе СЗПДн;

должны использоваться сертифицированные средства защиты.

4.2.8. Для ИСПДн 3 класса при многопользовательском режиме обработки ПДн и разных правах доступа к ним разных пользователей должны проводиться следующие мероприятия:

а) в подсистеме управления доступом:

должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длинной не мене шести буквенно-цифровых символов.

при отсутствии подключения к сетям общего пользования в распределенной ИСПДн должно проводиться межсетевое экранирование, при этом МЭ должен выполнять такие же функции, как и с ИСПДн 2 класса с многопользовательским режимом и равными правами доступа пользователей;

при наличии подключения к сетям общего пользования в распределенной ИСПДн должно проводиться межсетевое экранирование, при этом межсетевой экран должен выполнять такие же функции, как и с ИСПДн 1 класса при многопользовательском режиме и равных правах доступа пользователей;

б) в подсистеме регистрации и учета:

должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная – несанкционированная), идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

должен проводиться учет защищаемых носителей в журнале (картотеке) с регистрацией их выдачи (приема).

в) в подсистеме обеспечения целостности:

должна быть обеспечена целостность программных средств защиты информации в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием

трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

должна осуществляться физическая охрана ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации, особенно в нерабочее время;

должно проводиться периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД;

должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности;

г) в подсистеме антивирусной защиты:

должна проводиться автоматическая проверка на наличие ВПр или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВПр, по их типовым шаблонам и с помощью эвристического анализа;

должны быть реализованы механизмы автоматического блокирования обнаруженных ВПр путем их удаления из программных модулей или уничтожения;

должна регулярно выполняться проверка на предмет наличия ВПр в средствах защиты от ПМВ (при первом запуске средства защиты от ПМВ и с устанавливаемой периодичностью);

факт выявления ПМВ должен инициировать автоматическую проверку на предмет наличия ВПр;

должен быть реализован механизм отката для устанавливаемого числа операций удаления ВПр из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВПр.

4.2.9. Для ИСПДн 2 класса при многопользовательском режиме обработки ПДн и разных правах доступа к ним разных пользователей должны проводиться все мероприятия по 3 классу при многопользовательском режиме обработки ПДн и разных правах доступа к ним, а также следующие мероприятия:

а) в подсистеме управления доступом:

должна осуществляться идентификация терминалов, компьютеров, узлов сети ИСПДн, каналов связи, внешних устройств компьютеров по логическим именам;

должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

б) в подсистеме регистрации и учета:

должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная – несанкционированная), идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке;

должна осуществляться регистрация выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются (дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи - логическое имя (номер) внешнего устройства, краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ;

должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный – несанкционированный),

должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого файла;

должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого объекта - логическое имя (номер);

должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютеров и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов);

в) в подсистеме обеспечения целостности должны проводиться мероприятия такие же, как и в ИСПДн 2 класса с многопользовательским режимом обработки ПДн и равными правами доступа.

г) в подсистеме антивирусной защиты должны проводиться мероприятия такие же, как и в ИСПДн 2 класса с многопользовательским режимом обработки ПДн и равными правами доступа.

4.2.10. Для ИСПДн 1 класса при многопользовательском режиме обработки ПДн и разных правах доступа к ним разных пользователей должны проводиться все мероприятия по 2 классу при многопользовательском режиме обработки ПДн и разных правах доступа, а также следующие мероприятия:

а) в подсистеме управления доступом:

должна осуществляться идентификация терминалов, компьютеров, узлов сети ИСПДн, каналов связи, внешних устройств компьютеров по логическим именам и (или) адресам;

должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации;

б) в подсистеме регистрации и учета:

должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются дата и время изменения полномочий, идентификатор субъекта доступа (администратора), осуществившего изменения;

должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал (учетную карточку), учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

должна осуществляться сигнализация попыток нарушения защиты;

в) в подсистеме обеспечения целостности должны проводиться такие же мероприятия, как и в ИСПДн 2 класса с многопользовательским режимом и равными правами доступа пользователей, а также:

должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы средств защиты информации в составе СЗПДн;

должны использоваться сертифицированные средства защиты.

4.3. Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации – СЗИ, в том числе и встроенных в общесистемное и прикладное программное обеспечение – ПО), должен быть обеспечен соответствующий уровень контроля отсутствия в нем НДВ.

4.4. Анализ защищенности должен проводиться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) анализа защищенности (САЗ).

Для ИСПДн САЗ должна быть обеспечена возможность выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ).

4.5. В ИСПДн 1 и 2 классов должны быть реализованы мероприятия по защите ПДн от утечки за счет побочных электромагнитных излучений и наводок.

4.5.1. Для исключения утечки ПДн за счет ПЭМИН в ИСПДн 1 класса реализуются следующие мероприятия:

использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств;

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;

обеспечение развязки цепей электропитания объектов защиты с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы КЗ, и информационными цепями, по которым циркулирует защищаемая информация.

4.5.2. В ИСПДн 2 класса для обработки информации рекомендуется 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).

4.6. Если в ИСПДн предусмотрены функции голосового ввода ПДн в ИСПДн либо воспроизведение информации акустическими средствами ИСПДн, то для ИСПДн 1 класса должны быть реализованы мероприятия по защите акустической (речевой) информации.

Мероприятия по защите акустической (речевой) информации заключаются в обеспечении звукоизоляции ограждающих конструкций помещений, в которых расположена ИСПДн, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе ПДн в ИСПДн либо воспроизведении информации акустическими средствами ИСПДн.

4.7. Для исключения просмотра текстовой и графической видовой информации, отображаемой устройствами вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн, рекомендуется оборудовать помещения, в которых они установлены, шторами (жалюзи).