ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

УТВЕРЖДЕНЫ
Заместителем директора ФСТЭК России
15 февраля 2008 г.

РЕКОМЕНДАЦИИ
ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ
В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

Содержание

Обозначения и сокращения

АТС – автоматическая телефонная станция
ИСПДн – информационная система персональных данных
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ОТСС – основные технические средства связи
ПДн – персональные данные
ПЭМИН – побочные электромагнитные излучения и наводки
ПМВ – программно-математическое воздействие
СЗПДн – система защиты персональных данных

1. Термины и определения

В настоящем документе используются следующие термины и их определения:

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.

Зона 1 – пространство вокруг аппаратных средств информационных систем персональных данных, на границе и за пределами которого уровень наведенного от аппаратных средств информационных систем персональных данных информативного сигнала в технических средствах, а также в посторонних проводах и линиях передачи информации, имеющих выход за пределы контролируемой зоны, не превышает нормированного значения.

Зона 2 – пространство вокруг аппаратных средств информационных систем персональных данных, на границе и за пределами которого напряженность электромагнитного поля информативного сигнала не превышает нормированного значения.

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.

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

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.

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.

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

Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – рекомендации) разработаны ФСТЭК России на основании Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» с учетом действующих нормативных документов ФСТЭК России по защите информации.

Рекомендации предназначены для использования при проведении работ по обеспечению безопасности персональных данных (ПДн) при их обработке в следующих информационных системах персональных данных (ИСПДн):

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).

В рекомендациях рассматриваются вопросы обеспечения безопасности ПДн, оценки опасности угроз безопасности ПДн, применения способов, мер и средств защиты ПДн.

Документ предназначен для использования операторами ИСПДн, специалистами по обеспечению безопасности информации, руководителями организаций, проводящих работы по обработке ПДн в ИСПДн.

3. Понятие информационной системы персональных данных. Классификация информационных систем персональных данных

В соответствии с Федеральным законом «О персональных данных» под информационной системой персональных данных понимается информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных. В настоящем документе рассматриваются только ИСПДн, в которых обработка данных осуществляется с использованием средств автоматизации.

Классификация ИСПДн осуществляется с учетом категорий и объема накапливаемых, обрабатываемых и распределяемых с их использованием ПДн с целью установления методов и средств защиты, необходимых для обеспечения безопасности ПДн. Состав и функциональное содержание методов и средств защиты зависит от вида и степени ущерба, возникающего вследствие реализации угроз безопасности ПДн. При этом ущерб возникает за счет неправомерного или случайного уничтожения, изменения, блокирования, копирования, распространения ПДн или от иных неправомерных действий с ними. В зависимости от объекта, причинение ущерба которому, в конечном счете, вызывается неправомерными действиями с ПДн, рассматриваются два вида ущерба: непосредственный и опосредованный.

Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту ПДн. Он возникает за счет незаконного использования (в том числе распространения) ПДн или за счет несанкционированной модификации этих данных и может проявляться в виде:

нанесения вреда здоровью субъекта ПДн;

незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта;

потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием ПДн;

нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь путем осуществления контактов с ним по различным поводам без его на то согласия (например – рассылка персонифицированных рекламных предложений и т.п.).

Опосредованный ущерб связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности экономических, политических, военных, медицинских, правоохранительных, социальных, кредитно-финансовых и иных государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с ПДн.

Классификация ИСПДн проводится государственными органами, муниципальными органами, юридическими и физическими лицами, организующими и(или) осуществляющими обработку ПДн, а также определяющими цели и содержание обработки ПДн (операторами ИСПДн) 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.

Классификация ИСПДн проводится на этапе их создания или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и средств защиты информации, необходимых для обеспечения безопасности персональных данных.

Проведение классификации информационных систем включает в себя следующие этапы:

сбор и анализ исходных данных по информационной системе;

присвоение информационной системе соответствующего класса и его документальное оформление.

При проведении классификации информационной системы учитываются следующие исходные данные:

категория обрабатываемых в информационной системе персональных данных – $X_{ПД}$;

объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) – $X_{НПД}$;

заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;

структура информационной системы;

наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;

режим обработки персональных данных;

режим разграничения прав доступа пользователей информационной системы;

местонахождение технических средств информационной системы.

Определяются следующие категории обрабатываемых в информационной системе персональных данных ($X_{ПД}$):

категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;

категория 4 – обезличенные и (или) общедоступные персональные данные.

В зависимости от объема обрабатываемых в ИСПДн персональных данных $X_{НПД}$ может принимать следующие значения:

1 – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов ПДн или персональные данные субъектов ПДн в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 – в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов ПДн или персональные данные субъектов ПДн, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 – в информационной системе одновременно обрабатываются персональные данные менее чем 1000 субъектов ПДн или персональные данные субъектов ПДн в пределах конкретной организации.

По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы – информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам должны быть отнесены:

информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов ПДн;

информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений,

порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

По структуре информационные системы подразделяются:

на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);

на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);

на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения к сетям международного информационного обмена, и системы, не имеющие таких подключений.

По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

По результатам анализа исходных данных информационной системе присваивается один из следующих классов:

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

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

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

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

Класс информационной системы определяется в соответствии с таблицей.

$X_{ПД}$ \ $X_{НПД}$	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1

категория 1	К1	К1	К1

Применительно к специальным информационным системам после определения класса системы оператором должна быть разработана модель угроз безопасности персональных данных с использованием методических документов, разрабатываемых в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»[1], и проведена оценка актуальности угроз. По результатам оценки требования по защите ИСПДн от различных угроз могут быть скорректированы по сравнению с типовыми, приведенными в разделе 5. Решение об этом принимает оператор ИСПДн.

В случае выделения в составе информационной системы подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

Результаты классификации информационных систем оформляются соответствующим актом оператора.

Класс информационной системы может быть пересмотрен:

по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

В целом обеспечение безопасности ПДн при их обработке в ИСПДн достигается реализацией совокупности организационных и технических мер, причем в интересах обеспечения безопасности ПДн в обязательном порядке подлежат защите технические и программные средства, используемые при обработке ПДн, и носители информации. При организации и осуществлении защиты ПДн необходимо руководствоваться требованиями нормативных и методических документов по защите информации в автоматизированных системах, учитывая при этом, что ПДн, в соответствии с Федеральным законом от 27 июля 2006 г. № 152 «О персональных данных», отнесены к информации ограниченного доступа.

В связи с тем, что ИСПДн по своим характеристикам и номенклатуре угроз безопасности ПДн близки к наиболее распространенным, так называемым «офисным», информационным системам, целесообразно при их защите максимально использовать традиционные подходы к технической защите информации в автоматизированных системах.

[1] Собрание законодательства Российской Федерации 2007, № 48, часть II, ст. 6001.

4. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности мероприятий, осуществляемых на всех стадиях жизненного цикла ИСПДн, согласованных по цели, задачам, месту и времени, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз. Обеспечение безопасности ПДн при их обработке в автоматизированных ИСПДн должно проводиться путем выполнения комплекса организационных и технических мероприятий (применения технических средств) в рамках системы (подсистемы) защиты персональных данных, развертываемой в ИСПДн в процессе ее создания или модернизации.

Порядок организации обеспечения безопасности ПДн в ИСПДн должен предусматривать:

оценку обстановки;

обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;

разработку замысла обеспечения безопасности ПДн;

выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и замыслом защиты;

решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;

обеспечение реализации принятого замысла защиты;

планирование мероприятий по защите ПДн;

организацию и проведение работ по созданию системы защиты персональных данных (СЗПДн) в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДн или ее элементов в ИСПДн, а также решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн;

разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн;

развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн;

доработку СЗПДн по результатам опытной эксплуатации.

Оценка обстановки (рисунок 1) является этапом, во многом определяющим эффективность решения задач обеспечения безопасности ПДн. Она основывается на результатах комплексного обследования ИСПДн, в ходе которого, прежде всего, проводится определение защищаемой информации и ее категорирование по важности.

При оценке обстановки определяется необходимость обеспечения безопасности ПДн от угроз:

Рисунок 1. Содержание оценки обстановки

уничтожения, хищения аппаратных средств ИСПДн, и (или) носителей информации путем физического доступа к элементам ИСПДн;

утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН);

перехвата информации при передаче по проводным (кабельным) линиям связи;

хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

воспрепятствования функционированию ИСПДн путем преднамеренного электромагнитного воздействия на ее элементы;

непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

При оценке обстановки должна учитываться степень ущерба, который может быть причинен в случае неправомерного использования соответствующих ПДн.

Обоснование требований по обеспечению безопасности ПДн, обрабатываемых в ИСПДн, проводится в соответствии с нормативными и методическими документами уполномоченных федеральных органов исполнительной власти, обязательными к применению стандартами и на основании «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных». При этом выявление и оценка актуальности угроз безопасности персональных данных при их обработке в ИСПДн осуществляется с использованием «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» и «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Разработка замысла обеспечения безопасности ПДн является важным этапом организации обеспечения безопасности ПДн, в ходе которого осуществляется выбор основных способов защиты ПДн.

Рекомендуемый порядок формирования замысла показан на рисунке 2.

При выборе способов обеспечения безопасности ПДн, обрабатываемых в ИСПДн, необходимо определить организационные меры и технические (аппаратные, программные и программно-аппаратные) средства защиты. При выборе технических средств защиты следует использовать сертифицированные средства защиты информации.

Решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты является важным аспектом поддержания требуемого уровня безопасности ПДн.

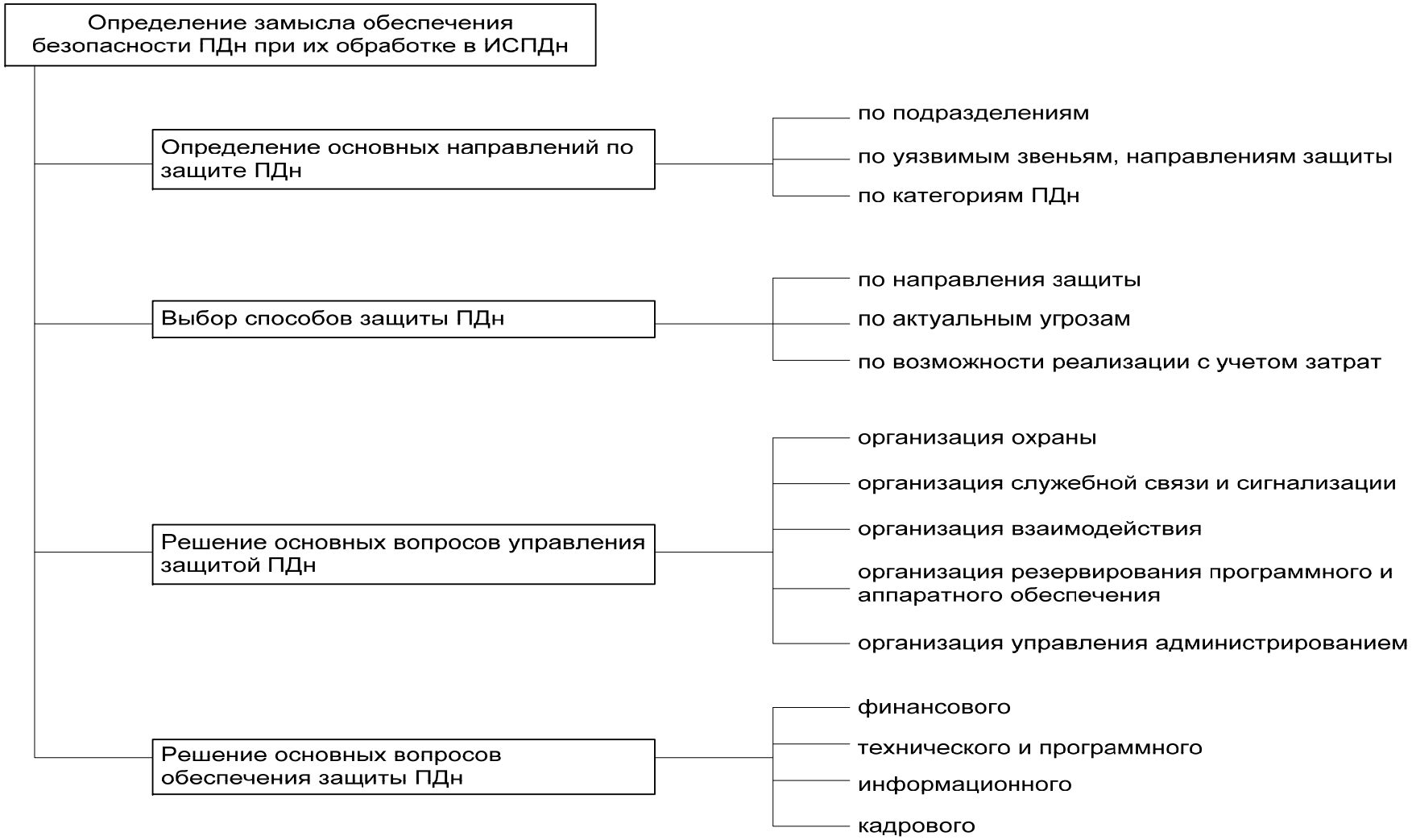

Рисунок 2. Порядок формирования замысла обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

К основным вопросам управления относятся:

распределение функций управления доступом к данным и их обработкой между должностными лицами;

определение порядка изменения правил доступа к защищаемой информации;

определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;

определение порядка действий должностных лиц в случае возникновения нештатных ситуаций;

определение порядка проведения контрольных мероприятий и действий по его результатам.

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Он может проводиться оператором или на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

Решение основных вопросов обеспечения защиты ПДн должно предусматривать подготовку кадров, выделение необходимых финансовых и материальных средств, закупку и разработку программного и аппаратного обеспечения.

При подготовке документации по вопросам обеспечения безопасности ПДн при их обработке в ИСПДн и эксплуатации СЗПДн в обязательном порядке разрабатываются:

положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн;

требования по обеспечению безопасности ПДн при обработке в ИСПДн;

должностные инструкции персоналу ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

Испытания СЗПДн проводятся в процессе развертывания и ввода в опытную эксплуатацию ИСПДн в соответствии с частным техническим заданием. Заключение по результатам испытаний должно содержать вывод о степени соответствия СЗПДн заданным требованиям по обеспечению безопасности ПДн.

5. Обеспечение безопасности персональных данных в информационных системах персональных данных

Обоснование комплекса мероприятий по обеспечению безопасности ПДн в ИСПДн производится с учетом результатов оценки опасности угроз и определения класса ИСПДн на основе «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных».

При этом должны быть определены мероприятия по:

выявлению и закрытию технических каналов утечки ПДн в ИСПДн;

защите ПДн от несанкционированного доступа и неправомерных действий;

установке, настройке и применению средств защиты.

Мероприятия по выявлению и закрытию технических каналов утечки ПДн в ИСПДн формулируются на основе анализа и оценки угроз безопасности ПДн.

Мероприятия по защите ПДн при их обработке в ИСПДн от несанкционированного доступа и неправомерных действий включают:

управление доступом;

регистрацию и учет;

обеспечение целостности;

контроль отсутствия недекларированных возможностей;

антивирусную защиту;

обеспечение безопасного межсетевого взаимодействия ИСПДн;

анализ защищенности;

обнаружение вторжений.

Подсистему управления доступом, регистрации и учета рекомендуется реализовывать на базе программных средств блокирования несанкционированных действий, сигнализации и регистрации. Это специальные, не входящие в ядро какой-либо операционной системы программные и программно-аппаратные средства защиты самих операционных систем, электронных баз ПДн и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами защиты и направлены на исключение или затруднение выполнения опасных для ИСПДн действий пользователя или нарушителя. К ним относятся специальные утилиты и программные комплексы защиты, в которых реализуются функции диагностики, регистрации, уничтожения, сигнализации и имитации.

Средства диагностики осуществляют тестирование файловой системы и баз ПДн, постоянный сбор информации о функционировании элементов подсистемы обеспечения безопасности информации.

Средства уничтожения предназначены для уничтожения остаточных данных и могут предусматривать аварийное уничтожение данных в случае угрозы НСД, которая не может быть блокирована системой.

Средства сигнализации предназначены для предупреждения операторов при их обращении к защищаемым ПДн и для предупреждения администратора при обнаружении факта НСД к ПДн и других фактов нарушения штатного режима функционирования ИСПДн.

Средства имитации моделируют работу с нарушителями при обнаружении попытки НСД к защищаемым ПДн или программным средствам. Имитация позволяет увеличить время на определение места и характера НСД, что особенно важно в территориально распределенных сетях, и дезинформировать нарушителя о месте нахождения защищаемых ПДн.

Подсистема обеспечения целостности реализуется преимущественно операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

Подсистема контроля отсутствия недекларированных возможностей реализуется в большинстве случае на базе систем управления базами данных, средств защиты информации, антивирусных средств защиты информации.

Для обеспечения безопасности ПДн и программно-аппаратной среды ИСПДн, осуществляющей обработку этой информации, рекомендуется применять специальные средства антивирусной защиты, выполняющие:

обнаружение и (или) блокирование деструктивных вирусных воздействий на общесистемное и прикладное программное обеспечение, реализующее обработку ПДн, а также на ПДн;

обнаружение и удаление неизвестных вирусов;

обеспечение самоконтроля (предотвращение инфицирования) данного антивирусного средства при его запуске.

При выборе средств антивирусной защиты целесообразно учитывать следующие факторы:

совместимость указанных средств со штатным программным обеспечением ИСПДн;

степень снижения производительности функционирования ИСПДн по основному назначению;

наличие средств централизованного управления функционированием средств антивирусной защиты с рабочего места администратора безопасности информации в ИСПДн;

возможность оперативного оповещения администратора безопасности информации в ИСПДн обо всех событиях и фактах проявления программно-математических воздействий (ПМВ);

наличие подробной документации по эксплуатации средства антивирусной защиты;

возможность осуществления периодического тестирования или самотестирования средства антивирусной защиты;

возможность наращивания состава средств защиты от ПМВ новыми дополнительными средствами без существенных ограничений работоспособности ИСПДн и «конфликта» с другими типами средств защиты.

Описание порядка установки, настройки, конфигурирования и администрирования средств антивирусной защиты, а также порядка действий в случае выявления факта вирусной атаки или иных нарушений требований по защите от программно-математических воздействий должны быть включены в руководство администратора безопасности информации в ИСПДн.

Для осуществления разграничения доступа к ресурсам ИСПДн при межсетевом взаимодействии применяется межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами (МЭ). Межсетевой экран устанавливается между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран входит в состав защищаемой сети. Для него путем настроек отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 3 и 4 классов рекомендуется использовать МЭ не ниже пятого уровня защищенности.

Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 2 класса рекомендуется использовать МЭ не ниже четвертого уровня защищенности.

Для обеспечения безопасного межсетевого взаимодействия в ИСПДн 1 класса рекомендуется использовать МЭ не ниже третьего уровня защищенности.

Подсистема анализа защищенности реализуется на основе использования средств тестирования (анализа защищенности) и контроля (аудита) безопасности информации.

Средства анализа защищенности применяются с целью контроля настроек защиты операционных систем на рабочих станциях и серверах и позволяют оценить возможность проведения нарушителями атак на сетевое оборудование, контролируют безопасность программного обеспечения. Для этого они исследуют топологию сети, ищут незащищенные

или несанкционированные сетевые подключения, проверяют настройки межсетевых экранов. Подобный анализ производится на основании детальных описаний уязвимостей настроек средств защиты (например, коммутаторов, маршрутизаторов, межсетевых экранов) или уязвимостей операционных систем или прикладного программного обеспечения. Результатом работы средства анализа защищенности является отчет, в котором обобщаются сведения об обнаруженных уязвимостях.

Средства обнаружения уязвимостей могут функционировать на сетевом уровне (в этом случае они называются «network-based»), уровне операционной системы («host-based») и уровне приложения («application-based»). Применяя сканирующее программное обеспечение, можно быстро составить карту всех доступных узлов ИСПДн, выявить используемые на каждом из них сервисы и протоколы, определить их основные настройки и сделать предположения относительно вероятности реализации НСД.

По результатам сканирования системы вырабатывают рекомендации и меры, позволяющие устранить выявленные недостатки.

В интересах выявления угроз НСД за счет межсетевого взаимодействия применяются системы обнаружения вторжений. Такие системы строятся с учетом особенностей реализации атак, этапов их развития и основаны на целом ряде методов обнаружения атак.

Выделяют три группы методов обнаружения атак:

сигнатурные методы;

методы выявления аномалий;

комбинированные методы (использующие совместно алгоритмы, определенные в сигнатурных методах и методах выявления аномалий).

Сигнатурные методы выявления атак основаны на том, что большинство возможных сетевых атак известны и развиваются по схожим сценариям.

Метод выявления аномалий базируется на сравнении так называемого профиля нормального поведения пользователя с реальным поведением. При этом могут выявляться аномалии в сигнатурах атак (отклонения от известных сигнатур), выявляемые статистическими методами, аномалии трафика (например, в интенсивности передачи пакетов данных с определенным сетевым адресом отправителя), выявляемые как обычными статистическим методами, так и специфическими методами, основанными, например, на использовании аппарата нейронных сетей, аномалии в служебных данных, вызванные ошибками нарушителя и др. При использовании данного метода предполагается, что отклонение от нормального поведения является подозрительным и может быть оценено как признак атаки.

Для обнаружения вторжений в ИСПДн 3 и 4 классов рекомендуется использовать системы обнаружения сетевых атак, использующие сигнатурные методы анализа.

Для обнаружения вторжений в ИСПДн 1 и 2 классов рекомендуется использовать системы обнаружения сетевых атак, использующие наряду с сигнатурными методами анализа методы выявления аномалий.

Для защиты ПДн от утечки по техническим каналам применяются организационные и технические мероприятия, направленные на исключение утечки акустической (речевой), видовой информации, а также утечки информации за счет побочных электромагнитных излучений и наводок.

При реализации технических мероприятий используются технические пассивные и активные средства защиты.

Защита акустической (речевой) информации заключается в реализации мер, исключающих возможность ее перехвата с использованием технических средств при

осуществлении пользователями ИСПДн голосового ввода ПДн в ИСПДн или воспроизведении ПДн акустическими средствами ИСПДн, и обеспечивается путем звукоизоляции помещений, в которых устанавливаются аппаратные средства ИСПДн, и применением организационных мер, направленных на исключение несанкционированного доступа в эти помещения.

Звукоизоляция ограждающих конструкций помещений, их систем вентиляции и кондиционирования в местах возможного перехвата информации должна исключать возможность прослушивания акустической (речевой) информации при осуществлении пользователями ИСПДн голосового ввода ПДн в ИСПДн или воспроизведении ПДн акустическими средствами ИСПДн.

Для снижения вероятности перехвата информации по виброакустическому каналу необходимо исключить возможность установки посторонних предметов на внешней стороне ограждающих конструкций помещений и выходящих из них инженерных коммуникаций (систем отопления, вентиляции, кондиционирования).

Звукоизоляция (виброизоляция) помещений является основным пассивным способом защиты акустической (речевой) информации и направлена на локализацию источников акустических сигналов внутри них.

Звукоизоляция оценивается величиной ослабления акустического сигнала и обеспечивается с помощью архитектурных и инженерных решений, а также применением специальных строительных и отделочных материалов.

При оценке звукоизоляции помещений необходимо отдельно рассмотреть звукоизоляцию элементов конструкции помещения (стены, пол, потолок, окна, двери) и систем инженерного обеспечения (приточно-вытяжная вентиляция, отопление, кондиционирование).

В случае, если звукоизоляция помещения не обеспечивает требуемой эффективности защиты информации, то для ее повышения используют специальные звукопоглощающие материалы.

Звукопоглощающие материалы могут быть сплошными и пористыми. Обычно пористые материалы используют в сочетании со сплошными.

Для снижения величины вибрационного сигнала используются мягкие прокладки (виброизолирующие опоры), которыми развязываются друг от друга различные ограждающие конструкции. В качестве таких прокладок применяют твердую резину, пробку, свинец.

При звукопоглощающей отделке внутреннего пространства помещений можно добиться повышения звукоизоляции на 10 – 15 дБ, что является достаточным для обеспечения требований по защите ПДн.

Система приточно-вытяжной вентиляции и воздухообмена защищаемых помещений не должна быть связана с системой вентиляции других помещений и иметь свой отдельный забор и выброс воздуха. Вентиляционные камеры забора и выброса рекомендуется располагать на крыше здания, а сами вентиляционные отверстия не должны выходить в места возможного дистанционного контроля.
В случае невозможности выполнения этого требования рекомендуется на вводах (выводах) каналов вентиляционных систем в зону (из зоны) защищаемых помещений устанавливать акустические фильтры и глушители звука, а в разрыв воздуховода – мягкие вставки из плотной ткани или резины.

Существующие акустические фильтры различных моделей при их погонной длине порядка 2 м обеспечивают получение затухания порядка 40 – 50 дБ.

Одним из наиболее слабых звукоизолирующих элементов ограждающих конструкций помещений являются двери и окна.

Стандартные одинарные двери не могут обеспечить требования по звукоизоляции, даже если выполнены требования по плотности и тщательности исполнения и подгонки дверного полотна к дверной коробке и устранены щели между дверью и полом.

Увеличение звукоизолирующей способности дверей достигается применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами.

Для усиления звукоизоляции помещений могут быть использованы специальные звукоизолирующие двери.

Звукоизоляция окон с одинарным остеклением соизмерима со звукоизоляцией одинарных дверей и недостаточна для надежной защиты информации в помещении.

Обычные окна с двойными переплетами обладают более высокой (на 4 – 5 дБ) звукоизолирующей способностью по сравнению с окнами со спаренными переплетами. Применение упругих прокладок значительно улучшает звукоизоляционные качества окон.

Повышение звукоизоляции до 5 дБ наблюдается при облицовке межстекольного пространства по периметру звукопоглощающим покрытием.

Существенное повышение звукоизоляции в сравнении с обычным окном дают оконные блоки специальной конструкции. Такие блоки выполняются из комбинаций стекол, установленных на определенном расстоянии и имеющих высококачественный притвор из уплотняющей резины, что в совокупности обеспечивает звукоизоляцию 40 – 50 дБ.

Пассивные методы защиты информации, как правило, реализуются при строительстве или реконструкции зданий на этапе разработки проектных решений, что позволяет заранее учесть типы строительных конструкций, способы прокладки коммуникаций, оптимальные места размещения защищаемых помещений.

В случае технической невозможности использования пассивных средств защиты помещений или если они не обеспечивают выполнение требуемых норм по звукоизоляции, используются активные меры защиты, заключающиеся в создании маскирующих акустических и вибрационных помех.

Способы защиты помещений путем создания акустических и вибрационных помех часто называют способами акустической и вибрационной маскировки, а системы (средства) создания маскирующих акустических и вибрационных помех – системами (средствами) вибрационной и акустической маскировки.

Акустическая маскировка используется для защиты речевой информации от утечки по прямому акустическому каналу путем создания акустических шумов в местах возможного размещения микрофонов средств разведки или нахождения посторонних лиц.

Виброакустическая маскировка используется для защиты речевой информации от утечки по вибрационному и акустооптическому (оптико-электронному) каналам и заключается в создании вибрационных шумов в элементах строительных конструкций, в инженерных коммуникациях, оконных рамах и стеклах. Виброакустическая маскировка эффективно используется для подавления таких средств перехвата информации, как электронные стетоскопы, радиостетоскопы, а также лазерные акустические системы разведки.

Для исключения возможности утечки информации за счет электроакустического преобразования необходимо оконечные устройства телефонной связи, имеющие прямой

выход в городскую автоматическую телефонную станцию (АТС), оборудовать сертифицированными средствами защиты информации от утечки за счет электроакустического преобразования.

К основным организационным мероприятиям по защите информации от утечки за счет побочных электромагнитных излучений и наводок относятся:

использование в ИСПДн сертифицированных технических средств защиты информации;

выбор помещений для установки аппаратных средств ИСПДн;

установление контролируемой зоны вокруг ИСПДн;

выбор мест установки аппаратных средств в помещениях;

разнос аппаратных средств ИСПДн и их соединительных линий от посторонних проводников;

организация режима и контроля доступа в помещения, в которых установлены аппаратные средства ИСПДн.

В ИСПДн должны использоваться только сертифицированные по требованиям безопасности информации технические средства и системы защиты.

Помещения, в которых устанавливаются аппаратные средства ИСПДн, выбираются с учетом их экранирующих свойств, расстояния до границы контролируемой зоны и значения зоны 2, указанной в предписании на эксплуатацию аппаратных средств ИСПДн.

В большинстве случаев только организационными мероприятиями не удается обеспечить требуемую эффективность защиты информации и необходимо проведение технических мероприятий по защите информации.

Технические мероприятия направлены на закрытие каналов утечки информации путем уменьшения отношения сигнал/шум в местах возможного размещения аппаратуры перехвата до величин, обеспечивающих невозможность выделения информационного сигнала аппаратурой перехвата.

В зависимости от используемых средств технические способы защиты информации подразделяются на пассивные и активные.

Пассивные способы защиты информации направлены:

на ослабление побочных электромагнитных излучений (информационных сигналов) аппаратных средств ИСПДн на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством перехвата на фоне естественных шумов;

на ослабление наводок побочных электромагнитных излучений аппаратных средств ИСПДн в посторонних проводниках и соединительных линиях технических средств, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством перехвата на фоне естественных шумов;

на исключение (ослабление) проникновения информационных сигналов в цепи электропитания аппаратных средств ИСПДн, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения аппаратурой перехвата на фоне естественных шумов.

Активные способы защиты информации используются в том случае, когда проведением организационных мероприятий и использованием пассивных средств защиты не обеспечивается требуемая эффективность защиты, и направлены на создание:

маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения побочных электромагнитных излучений средством перехвата в местах возможного размещения;

маскирующих электромагнитных помех в цепях электропитания аппаратных средств ИСПДн с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного сигнала средством перехвата в местах возможного размещения;

маскирующих электромагнитных помех в цепях заземления ИСПДн с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного сигнала средством перехвата в местах возможного размещения.

Активные способы связаны с созданием маскирующих пространственных электромагнитных помех и осуществляются с целью закрытия электромагнитных и электрических каналов утечки информации в том случае, если минимальное расстояние от аппаратных средств ИСПДн до границы контролируемой зоны менее значения зоны 2 для данного технического средства. Для создания маскирующих пространственных электромагнитных помех используются широкополосные генераторы шума со специальными антеннами, обеспечивающие постановку шумовых помех во всем диапазоне возможных побочных электромагнитных излучений и наводок. Один генератор шума может использоваться для защиты одного или нескольких аппаратных средств ИСПДн.

Если в здании расположено несколько аппаратных средств ИСПДн, то для их защиты может использоваться единая система пространственного зашумления, включающая в свой состав один или несколько генераторов шума и соответствующие антенные системы. Генераторы шума при этом могут устанавливаться как внутри помещений, так и вне их (например, на крыше здания). Места размещения генераторов шума выбирают таким образом, что бы обеспечить максимальный уровень помехового сигнала в местах возможного размещения аппаратуры перехвата.

При установке системы пространственного электромагнитного зашумления в помещении помеховый сигнал наводится на соединительных линиях технических средств, посторонних проводниках, цепях электропитания, тем самым затрудняя нарушителю получение информации по электрическим каналам утечки информации.

Системы линейного электромагнитного зашумления применяются для маскировки наведенных информационных сигналов и используются в том случае, когда минимальное расстояние от аппаратных средств ИСПДн до границы контролируемой зоны более значения зоны 2, но не обеспечивается требуемый пространственный разнос аппаратных средств ИСПДн и их соединительных линий или посторонних проводников (например, инженерных коммуникаций), имеющих выход за пределы контролируемой зоны (то есть расстояние между ними менее значения зоны 1), или питание ИСПДн осуществляется от трансформаторной подстанции, расположенной за пределами контролируемой зоны, или к системе заземления ИСПДн возможно подключение потребителей, расположенных вне контролируемой зоны.

Эффективным способом ослабления побочных электромагнитных излучений аппаратных средств ИСПДн является экранирование их источников.

Экранироваться могут не только отдельные элементы (узлы) и блоки аппаратуры, но и их соединительные линии и кабели электропитания.

Наиболее экономичным способом экранирования информационных линий связи между устройствами ИСПДн считается групповое размещение их информационных кабелей в экранирующий распределительный короб.

В случае экономической нецелесообразности экранирования каждого технического средства или невозможности создания условий обеспечения требуемой эффективности экранирования отдельных технических средств, могут экранироваться помещения в целом.

Экранирование является также эффективным способом ослабления наводок побочных электромагнитных излучений аппаратных средств ИСПДн и их соединительных линий. Экранирование аппаратных средств ИСПДн и соединительных линий эффективно только при правильном их заземлении.

Эффективным способом исключения проникновения побочных электромагнитных излучений за пределы контролируемой зоны через инженерные коммуникации и экраны соединительных линий технических средств и кабелей электропитания является установка в них специальных диэлектрических вставок и их заземление.

Исключение (ослабление) проникновения информационных сигналов в цепи электропитания ИСПДн, выходящие за пределы контролируемой зоны, осуществляется путем установки в них помехоподавляющих фильтров, разделительных трансформаторов, а также использованием для питания ИСПДн агрегатов (источников) бесперебойного питания.

Разделительные трансформаторы обеспечивают развязку первичной и вторичной цепей по сигналам наводки. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки.

Помехоподавляющие фильтры представляют собой фильтры низких частот. Они пропускают сигналы с частотами ниже граничной частоты и подавляют – с частотами выше граничной частоты. Как правило, граничная частота фильтра типа помехоподавляющих фильтров составляет 20 – 150 кГц.

Необходимым условием по защите аппаратных средств ИСПДн является их правильное заземление.

В настоящее время существуют различные типы заземлений. Наиболее часто используются одноточечные, многоточечные и комбинированные (гибридные) схемы.

Одноточечная последовательная схема заземления наиболее проста. Однако ей присущи недостатки, связанные с протеканием обратных токов различных цепей по общему участку заземляющей цепи. Вследствие этого возможно появление опасного сигнала в посторонних цепях.

В одноточечной параллельной схеме заземления этих недостатков нет. Однако такая схема требует большого числа протяженных заземляющих проводников, из-за чего может возникнуть проблема с обеспечением малого сопротивления заземления участков цепи.

Кроме того, между заземляющими проводниками могут возникать нежелательные связи, которые создают несколько путей заземления для каждого устройства. В результате в

системе заземления могут возникнуть уравнительные токи и появиться разность потенциалов между различными устройствами.

Многоточечная схема заземления практически свободна от недостатков, присущих одноточечной схеме. В этом случае отдельные устройства и участки корпуса индивидуально заземлены. При проектировании и реализации многоточечной системы заземления необходимо принимать специальные меры для исключения замкнутых контуров.

Заземление ИСПДн должно быть выполнено в соответствии с определенными правилами.

Основные требования, предъявляемые к системе заземления, заключаются в следующем:

система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с ИСПДн;

сопротивления заземляющих проводников, а также земляных шин должны быть минимальными, при этом сопротивление должно быть не более 4 Ом;

каждый заземляемый элемент должен быть присоединен к заземлителю или к заземляющей магистрали при помощи отдельного ответвления;

в системе заземления должны отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землей;

следует избегать использования общих проводников в системах экранирующих заземлений, защитных заземлений и сигнальных цепей;

качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надежность и механическую прочность контакта в условиях климатических воздействий и вибрации;

присоединение заземляющих проводников к заземлителям, заземляющему контуру и заземляющим конструкциям должно быть выполнено сваркой, а к корпусам технических средств – сваркой или надежным болтовым соединением;

заземляющие проводники должны иметь покрытие, предохраняющее их от коррозии;

контактные соединения должны исключать возможность образования гальванических пар для предотвращения коррозии в цепях заземления;

запрещается использовать в качестве заземляющего устройства провода электросетей (нулевые фазы), металлоконструкции зданий, имеющие соединение с землей, металлические оболочки подземных кабелей, металлические трубы систем отопления, водоснабжения, канализации.

На практике наиболее часто в качестве заземлителей применяют:

стержни из металла, обладающие высокой электропроводностью, погруженные в землю и соединенные с наземными металлоконструкциями средств ИСПДн;

сеточные заземлители, изготовленные из элементов с высокой электропроводностью и погруженные в землю (служат в качестве дополнения к заземляющим стержням).

С целью защиты информации от утечки по цепям электропитания система электропитания ИСПДн должна удовлетворять следующим требованиям:

электропитание ИСПДн рекомендуется осуществлять от подстанции, расположенной в пределах контролируемой зоны;

подключение к распределительному устройству трансформаторной подстанции, питающей ИСПДн, посторонних потребителей, расположенных за пределами контролируемой зоны, должно быть исключено;

система электропитания ИСПДн должна быть выполнена в соответствии с требованиями, предъявляемыми к электроустановкам напряжением до 1кВ;

цепи электропитания на участке «подстанция – силовой щит ИСПДн» должны прокладываться экранированными (бронированными) кабелями и не должны иметь выходов за пределы контролируемой зоны;

распределительные устройства и силовые щиты системы электропитания ИСПДн должны располагаться в пределах контролируемой зоны;

помещения, в которых установлены распределительные устройства и силовые щиты, должны закрываться на замки и опечатываться.

При выполнении данных требований обеспечивается требуемая эффективность защиты ПДн, обрабатываемых ИСПДн, от утечки по цепям электропитания без применения технических средств и методов защиты информации.

В случаях, если трансформаторная подстанция расположена за пределами контролируемой зоны или к распределительным устройствам, питающим ИСПДн, подключены посторонние потребители, расположенные за пределами контролируемой зоны, то для защиты цепей электропитания ИСПДн должны использоваться технические средства, обеспечивающие фильтрацию опасных сигналов, или системы активного зашумления.

Для фильтрации сигналов в цепях питания ИСПДн используются разделительные трансформаторы и помехоподавляющие фильтры.

Разделительные трансформаторы должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Проникновение наводок во вторичную обмотку объясняется наличием резистивных и емкостных цепей связи между обмотками.

В настоящее время существует большое количество различных типов помехоподавляющих фильтров, обеспечивающих ослабление нежелательных сигналов в разных участках частотного диапазона. Это фильтры нижних и верхних частот, полосовые и заграждающие фильтры. Основное назначение фильтров – пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе частот, и подавлять (ослаблять) сигналы с частотами, лежащими за пределами этой полосы.

Для исключения просачивания информационных сигналов в цепи электропитания используются фильтры нижних частот. Фильтр нижних частот пропускает сигналы с частотами ниже граничной частоты и подавляет – с частотами выше граничной частоты.

Фильтры, которые устанавливаются в цепи питания отдельных технических средств непосредственно в помещениях, где производится обработка защищаемой информации, или же вблизи этих помещений, классифицируются как «фильтры для локальных цепей». Они рассчитаны на электропитание одного или нескольких технических средств и обеспечивают подавление информативных сигналов в фазном, нулевом и заземляющем проводах однофазной сети.

Другая группа фильтров, классифицируемая как «объектовые фильтры», устанавливается в цепи электропитания группы технических средств или ИСПДн в целом и обеспечивает подавление информативных сигналов в кабелях питания трехфазной сети.

В зависимости от числа фильтруемых линий фильтры могут быть двухпроводными, трехпроводными и четырехпроводными.

Выбор фильтра определяется величиной рабочего напряжения, номинального рабочего тока цепи, в которую он включается, и требуемой величиной вносимого затухания в полосе частот подавления с учетом уровней спектральных составляющих информативного сигнала.

Реализация пассивных методов защиты, основанных на применении экранирования и фильтрации, приводит к ослаблению уровней побочных электромагнитных излучений и наводок (опасных сигналов) основных технических средств связи (ОТСС) в местах возможного размещения аппаратуры перехвата. Однако в ряде случаев, несмотря на применение пассивных методов защиты, уровни побочных излучений на границе контролируемой зоны превышают допустимые нормы. В этом случае применяются активные меры защиты, основанные на создании помех аппаратуре перехвата, что приводит к уменьшению отношения опасный сигнал/шум (с/ш) до требуемых нормированных значений.

Для создания помех используются системы пространственного и линейного зашумления. Системы пространственного зашумления используются для исключения перехвата побочных электромагнитных излучений, а системы линейного зашумления – для исключения «съема» наводок информационных сигналов с посторонних проводников и соединительных линий технических средств.

В системах пространственного зашумления в основном используются помехи типа «белого шума» или «синфазные помехи».

При использовании систем пространственного зашумления необходимо помнить, что наряду с помехами средствам разведки создаются помехи и другим радиоэлектронным средствам (например, системам телевидения, радиосвязи). Поэтому при вводе в эксплуатацию системы пространственного зашумления необходимо проводить специальные исследования по требованиям обеспечения электромагнитной совместимости.

Пространственное зашумление эффективно не только для закрытия электромагнитного, но и электрического каналов утечки информации, так как помеховый сигнал при излучении наводится в соединительных линиях аппаратных средств ИСПДн и посторонних проводниках, выходящих за пределы контролируемой зоны.

Системы линейного зашумления применяются для маскировки наведенных опасных сигналов в цепях электропитания, посторонних проводниках и соединительных линиях аппаратных средств ИСПДн, выходящих за пределы контролируемой зоны. Они используются в том случае, если не обеспечивается требуемый их разнос от аппаратных средств ИСПДн и их соединительных линий (то есть если расстояние между ними меньше значения зоны 1), однако при этом расстояние от аппаратных средств ИСПДн до границы контролируемой зоны больше, чем значение зоны 2.

Системы линейного зашумления, обеспечивающие непосредственный ввод шумового сигнала, используются в основном для зашумления линий электропитания.

При отсутствии специальных устройств для ввода шумового сигнала в различные токопроводящие инженерные коммуникации и другие проводники может использоваться обычная гибкая антенна, которая наматывается вокруг них.

Защита видовой информации достигается исключением 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. Исключение просмотра текстовой и графической видовой информации обеспечивается использованием штор или жалюзи в помещениях, в которых установлены устройства отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технические средства обработки графической, видео- и буквенно-цифровой информации.