МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
Барнаульский юридический институт

В.А. Кемпф, Л.М. Осинцева

Специальная техника органов внутренних дел: технические средства защиты информации

Учебное пособие

Барнаул 2017

ББК 67.401.133.1с51 + 32.97р30
К 352

Кемпф, В.А., Осинцева, Л.М.
К 352 Специальная техника органов внутренних дел: технические средства защиты информации : учебное пособие / В.А. Кемпф, Л.М. Осинцева. – Барнаул : Барнаульский юридический институт МВД России, 2017. – 44 с.

ISBN 978-5-94552-264-0

Рецензенты:

Бенцлер А.В. – начальник отдела защиты информации центра информационных технологий, связи и защиты информации ГУ МВД России по Алтайскому краю;

Еськов А.В. – доктор технических наук, доцент, профессор кафедры информационной безопасности Краснодарского университета МВД России.

В учебном пособии рассматриваются основные направления обеспечения безопасности информационных систем; организационные и технические мероприятия, направленные на защиту информации ограниченного доступа; технические средства защиты информации от утечки по техническим каналам; нормативно-правовое регулирование мероприятий по защите объектов ОВД от утечки информации ограниченного доступа, а также вопросы контроля эффективности защиты информации.

Учебное пособие предназначено для учебно-методического обеспечения образовательного процесса в организациях высшего образования системы МВД России по дисциплине «Специальная техника ОВД».

ББК 67.401.133.1с51 + 32.97р30

ISBN 978-5-94552-264-0

Глава 1

Основные направления обеспечения безопасности информационных систем

Информационная среда, представляющая собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений, играет всё большую роль на современном этапе развития общества.

Особенностями современной информационной инфраструктуры являются:

- увеличение числа автоматизированных процессов в системах обработки информации;
- применение облачной архитектуры для построения информационных систем;
- накопление и длительное хранение больших массивов данных на электронных носителях;
- интеграция в единую базу данных информации различной направленности;
- непосредственный доступ к ресурсам компьютерной системы большого количества пользователей различной категории и с различными правами доступа в системе.

Значимое место в общей структуре информационной сферы занимают информационные системы. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» подразумевает под информационной системой совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

1.1. Основные понятия в области безопасности информационных систем

Безопасность информационных систем является частью более широкой проблемы – информационной безопасности. В этой связи уместно рассматривать ряд общих подходов к безопасности, в значительной степени применимых и в отношении информационных систем.

Надежная информационная система определяется как система, использующая достаточные аппаратные и программные средства, обеспечивающая одновременную достоверную обработку информации разной степени секретности различными пользователями или группами пользователей без нарушения прав доступа, целостности и конфиденциальности данных и поддерживающая свою работоспособность в условиях воздействия на нее совокупности внешних и внутренних угроз.

Таким образом, информация, получаемая субъектами посредством информационных систем, должна обладать следующими свойствами:

- доступностью;
- целостностью;
- конфиденциальностью.

Доступность информации – свойство информационных ресурсов, определяющее возможность за приемлемое время выполнить ту или иную операцию над данными или получить нужную информацию уполномоченными на это лицами.

Целостность информации – неизменность информации в процессе ее хранения, обработки и передачи по каналам связи.

Конфиденциальность информации – защищенность информации от несанкционированного доступа.

Безопасность информационных систем – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, нарушающих доступность, целостность или конфиденциальность информации.

Защита информации – комплекс мер, направленных на обеспечение информационной безопасности.

Угрозой безопасности информации называют действие или событие, которое может привести к нарушению достоверности, целостности или конфиденциальности хранящейся, передаваемой или обрабатываемой информации.

При этом следует отметить, что речь идет о защите не только хранящейся в информационной базе информации, но и информации, передаваемой по каналам связи или обрабатываемой программным обеспечением.

Определим ряд понятий, наиболее часто используемых при анализе безопасности информационных систем.

Угроза – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Фактор – явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Источник угрозы – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Уязвимость (информационной системы) – свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Атака – попытка реализации угрозы.

1.2. Классификации угроз

Основными видами угроз безопасности информационных систем и угроз интересам субъектов информационных отношений являются:

- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.);
- сбои и отказы оборудования (технических средств) компьютерной системы;
- последствия ошибок проектирования и разработки компонентов компьютерной системы (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);
- ошибки эксплуатации (пользователей, операторов и другого персонала);

• преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Таким образом, всё множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).

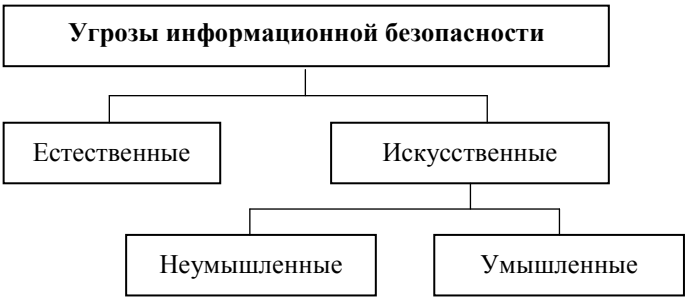

Рис. 1. Классификация угроз информационной безопасности

Естественные угрозы – это угрозы, вызванные воздействиями на компьютерную систему и ее элементы объективных физических процессов или стихийных природных явлений, не зависящих от человека.

Искусственные угрозы – это угрозы компьютерной системе, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить непреднамеренные и преднамеренные.

Непреднамеренные угрозы (неумышленные, случайные) – угрозы, вызванные ошибками при проектировании информационной системы и ее элементов, ошибками персонала.

Преднамеренные (умышленные) угрозы – угрозы, связанные с корыстными устремлениями людей.

1.3. Направления защиты информации в информационных системах

С целью обеспечения защиты информации и противостояния вышеперечисленным угрозам современные информационные системы включают в себя подсистемы безопасности, которые реализуют принятую политику безопасности. Политика безопасности в зависимости от

целей и условий функционирования системы определяет права доступа субъектов к ресурсам, регламентирует порядок аудита действий пользователей в системе, защиты сетевых коммуникаций, формулирует способы восстановления системы после случайных сбоев и т.д.

В соответствии с ГОСТом Р 50922-2006 «Защита информации. Основные термины и определения» под защитой информации понимается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Выделяют следующие виды защиты информации: правовую, техническую, криптографическую и физическую *(рис. 2)*.

Рис. 2. Виды защиты информации

Правовая защита информации включает в себя разработку нормативно-правовых документов, регламентирующих отношения, которые возникают при осуществлении права на поиск, получение, передачу, производство и распространение информации, а также применение этих документов, надзор и контроль за их исполнением.

Техническая защита информации – обеспечение безопасности информации, подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств без применения криптографических методов.

Криптографическая защита информации осуществляется криптографическими средствами, которые с помощью специальных математических алгоритмов осуществляют преобразование информации, передаваемой по линиям связи или хранящейся в технических средствах таким образом, что при несанкционированном доступе невозможно ознакомиться с ее содержанием.

Физическая защита информации осуществляется путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. К физической защите относятся средства инженерно-технической укрепленности охраняемых объектов и технические средства охраны.

Организационные мероприятия по обеспечению защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

К основным направлениям защиты информации относят защиту:

- от утечки;
- несанкционированного воздействия;
- непреднамеренного воздействия;
- разглашения;
- несанкционированного доступа.

Защита информации от утечки – предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами.

Защита информации от несанкционированного воздействия – предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия – предотвращение воздействия на защищаемую информацию ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения – предотвращение несанкционированного доведения защищаемой информации до заинтересо-

ванных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа – предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Защита информации от преднамеренного воздействия – предотвращение преднамеренного воздействия, в т.ч. электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

Защита информации от иностранной разведки – предотвращение получения защищаемой информации иностранной разведкой.

Цель защиты информации – предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Объект защиты информации – информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

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

Система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Политика безопасности информации – совокупность документированных правил, процедур, практических приёмов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Безопасность информации – состояние защищённости информации, при котором обеспечены её конфиденциальность, доступность и целостность.

Носитель защищаемой информации – физическое лицо или материальный объект, в т.ч. физическое поле, в котором информация находит своё отражение в виде символов, образов, сигналов, техниче-

ских решений и процессов, количественных характеристик физических величин.

Защищаемый объект информации – объект информации, предназначенный для обработки защищаемой информации с требуемым уровнем её защищённости.

Защищаемая информационная система – информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем её защищённости.

Глава 2

Организационные и технические мероприятия, направленные на защиту информации ограниченного доступа

Согласно статье 16 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

1) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Таким образом, согласно вышеуказанному федеральному закону, защита информации должна быть комплексной, т.е. сочетать в себе организационное и инженерно-техническое направления защиты.

2.1. Организационная защита информации ограниченного доступа

Организационная защита информации ограниченного доступа – это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что несанкционированный доступ к информации становится невозможным или существенно затрудняется за счёт проведения организационных мероприятий.

Организационные мероприятия, следовательно, играют большую роль в создании надёжного механизма защиты информации, т.к. возможности несанкционированного использования сведений ограниченного распространения в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать только с помощью технических средств, программно-математических методов и физических мер.

К организационным мероприятиям можно отнести:

• мероприятия, осуществляемые при проектировании, строительстве и оборудовании служебных зданий и помещений. Цель этих мероприятий – исключение возможности тайного проникновения на территорию и в помещения; обеспечение удобства контроля прохода и перемещения людей, проезда транспорта и других средств передвижения; создание отдельных зон по типу конфиденциальности работ с самостоятельными системами доступа и т.п.;

• мероприятия, осуществляемые при подборе персонала, включающие ознакомление с сотрудниками, их изучение, обучение правилам работы с информацией ограниченного доступа, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

• организация и поддержание пропускного режима и контроля посетителей;

• организация охраны помещений и территории;

• организация хранения и использования документов и носителей информации ограниченного распространения, включая порядок учёта, выдачи, исполнения и возвращения;

• организация защиты информации;

• организация регулярного обучения сотрудников.

Среди основных условий организационной защиты информации можно выделить следующие:

• непрерывный всесторонний анализ функционирования системы защиты информации в целях принятия своевременных мер по повышению её эффективности;

• безоговорочное соблюдение руководством и персоналом установленных норм и правил защиты информации ограниченного доступа.

Многогранность сферы организационной защиты информации в органах внутренних дел требует существования специальной службы безопасности, обеспечивающей и направляющей реализацию всех организационных мероприятий.

Приказом МВД России от 2 июля 2012 г. № 660 утверждено Типовое положение о подразделении информационных технологий, связи и защиты информации территориального органа Министерства внутренних дел Российской Федерации. В соответствии с данным положением подразделение ИТСиЗИ является структурным подразделением территориального органа, обеспечивающим и осуществляющим в пределах

своей компетенции в т.ч. функции по противодействию техническим разведкам; технической (в т.ч. криптографической) защите информации; радиоэлектронной борьбе; использованию электронной подписи; защите персональных данных при их автоматизированной обработке; также функции шифровального органа.

Основными задачами подразделения ИТСиЗИ в области защиты информации являются:

- организация и реализация мероприятий по технической (в т.ч. криптографической) защите информации и противодействию техническим разведкам;
- обеспечение функционирования и безопасности шифрованной связи в территориальном органе.

В целях реализации указанных задач подразделения ИТСиЗИ выполняют следующие функции в области защиты информации:

- осуществление в пределах своей компетенции мероприятий по защите государственной тайны, информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, защите персональных данных при их автоматизированной обработке, а также контроля за их проведением подразделениями территориального органа;
- осуществление мероприятий по противодействию техническим разведкам; радиоэлектронной борьбе; технической (криптографической) защите информации;
- осуществление контроля за обеспечением в подразделениях территориального органа исполнения предписаний нормативных правовых актов в области защиты информации, в т.ч. за порядком обращения с шифрованной информацией;
- информирование руководства территориального органа, а также по его поручениям руководителей подразделений территориального органа о выявленных и возможных угрозах информационной безопасности территориального органа;
- осуществление мероприятий по внедрению и использованию в территориальном органе средств электронной подписи;
- организация шифровальной службы в территориальном органе, руководство органами криптографической защиты информации по специальным вопросам и контроль за их деятельностью;
- подготовка и направление в установленном порядке в уполномоченное подразделение МВД России сведений и донесений по вопросам шифровальной службы МВД России;

• организация и обеспечение бесперебойной шифрованной связи в интересах руководства и подразделений территориального органа с органами управления, соединениями и воинскими частями войск национальной гвардии РФ, организациями и подразделениями системы МВД России, временными формированиями МВД России, развернутыми в регионах, где введено чрезвычайное положение, в зонах вооруженных конфликтов, в местах со сложной оперативной обстановкой, другими федеральными органами исполнительной власти в мирное время, при наступлении чрезвычайных обстоятельств, при введении режима чрезвычайного положения, а также в период мобилизации и в военное время. Разработка и реализация мероприятий по обеспечению безопасности шифрованной связи в территориальном органе;

• обеспечение ведения учета шифрработников территориального органа.

Организационные механизмы защиты информации определяют порядок и условия комплексного использования имеющихся сил и средств, эффективность которых зависит от применяемых методов технической защиты.

2.2. Техническая защита информации ограниченного доступа

Техническая защита информации, используемая в комплексе с организационными мерами, играет исключительную роль в обеспечении защиты информации при её хранении, накоплении и обработке с использованием средств автоматизации.

В общем случае под техническими средствами защиты информации понимают технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты информации ограниченного доступа, а также средства, устройства и системы контроля эффективности защиты информации.

Технические средства защиты информации – устройства и приборы, предназначенные для обеспечения защиты информации, исключения её утечек, создания помех (препятствий) техническим средствам съема информации.

Криптографические средства защиты информации – средства и устройства, обеспечивающие защиту информации ограниченного доступа путём её криптографического преобразования (шифрования).

Программные средства защиты информации – системы защиты средств автоматизации (персональных компьютеров и компьютерных сетей) от внешнего воздействия или вторжения.

Инженерно-техническое направление включает в себя аппаратные средства защиты информации.

К аппаратным средствам относятся механические, электромеханические, электронные, оптические, лазерные, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для обеспечения безопасности и защиты информации.

Инженерно-технические средства применяются для решения следующих задач:

- препятствия визуальному наблюдению и дистанционному подслушиванию;
- нейтрализации побочных электромагнитных излучений и наводок (далее – ПЭМИН);
- обнаружения технических средств подслушивания и магнитной записи, несанкционированно устанавливаемых или проносимых в организацию;
- защиты информации, передаваемой в средствах связи и системах автоматизированной обработки информации.

По своему предназначению аппаратные средства подразделяются на средства выявления и средства защиты (или существенного ослабления) несанкционированного доступа.

К классу защитной спецтехники относится огромное количество аппаратов, устройств и систем: приборы обнаружения и нейтрализации средств акустической разведки, средства защиты абонентской телефонной сети, средства защиты съёма информации из помещений, приборы для обнаружения инфракрасного и видеонаблюдения и др.

Глава 3

Технические средства защиты информации от утечки по акустическим, электрическим, электромагнитным и визуально-оптическим каналам

3.1. Технические каналы утечки информации

В общем случае информация передается полем или веществом: акустической волной, электромагнитным излучением, электрическим током, листом бумаги с текстом и т.д. Система передачи информации состоит из передатчика, канала передачи информации, приёмника и получателя информации. Однако ввиду физической природы передачи информации при выполнении определённых условий возможно возникновение системы передачи информации, которая передаёт информацию вне зависимости от желания отправителя или получателя информации. Такую систему называют техническим каналом утечки информации.

Утечка информации по техническому каналу – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. Технический канал утечки информации (ТКУИ), так же как и канал передачи информации, состоит из источника сигнала, физической среды его распространения и приемной аппаратуры злоумышленника. На рисунке 3 приведена структура технического канала утечки информации.

Рис. 3. Структура технического канала утечки информации

Основными техническими каналами возможной утечки информации на объектах системы ОВД являются: акустический, электромагнитный и визуально-оптический.

3.2. Акустический канал утечки информации

Акустическая информация возникает в помещениях в ходе речевого общения, а также при функционировании систем звукоусиления и звуковоспроизведения. Носителем информации в этом случае являются акустические колебания – механические колебания частиц упругой среды, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины. Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 100 Гц до 7 кГц.

Технические каналы утечки акустической (речевой) информации в зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата разделяют на воздушные, вибрационные, электроакустические, оптико-электронный и параметрические.

В **вибрационных** каналах средой распространения акустических колебаний являются конструктивные элементы зданий, стены, потолки, трубы и другие твёрдые тела. Для перехвата информации в этих случаях используются стетоскопы, в которых в качестве приёмников сигнала используются контактные микрофоны или вибродатчики. Электронные стетоскопы не требуют проникновения в защищаемое помещение.

Современные электронные стетоскопы имеют настолько большой коэффициент усиления, что способны воспринимать даже такие слабые звуковые колебания, как тихий шепот и шорох. Чувствительные элементы электронных стетоскопов устанавливаются на стенах, за подвесными потолками, на трубах систем отопления и водоснабжения, за дверными проемами, на коробах воздуховодов вентиляционных систем. Преобразованный стетоскопом акустический сигнал передаётся далее по радиоканалу, инфракрасному или проводному каналу.

Электроакустические каналы утечки информации образуются за счёт электроакустических преобразований, при которых акустические сигналы преобразуются в электрические. Наиболее известны такие акустоэлектрические преобразователи, как системы звукового вещания, телефоны и микрофоны.

Таблица 1

Технические каналы утечки акустической информации

Воздушные	**Вибрационные**
Перехват акустических сигналов микрофонами, объединёнными с механическими устройствами звукозаписи	Перехват акустических сигналов электронными стетоскопами
Перехват акустических сигналов направленными микрофонами	Перехват акустических колебаний стетоскопами, объединенными с устройствами передачи информации по радиоканалу
Перехват акустических сигналов микрофонами, объединёнными с устройствами передачи информации радиоканалу	Перехват акустических колебаний стетоскопами, объединенными с устройствами передачи информации по оптическому каналу в ИК-диапазоне
Перехват акустических сигналов микрофонами, объединёнными с устройствами передачи информации по сети электропитания	**Параметрические**
Перехват акустических сигналов микрофонами, объединёнными с устройствами передачи информации по телефонной линии	Перехват акустического сигнала путём приёма и детектирования побочных электромагнитных излучений
Перехват акустических сигналов микрофонами, объединёнными с устройствами подключения к телефонной линии по сигналам вызова от внешнего абонента	Перехват акустического сигнала путём «высокочастотного облучения» специальных полуактивных закладных устройств
Перехват акустических сигналов микрофонами, объединенными с устройствами передачи информации по трубам водоснабжения, отопления и т.п.	**Электроакустические**
Оптико-электронный (лазерный)	Перехват акустических колебаний через вспомогательные технические средства и системы (ВТСС), обладающие «микрофонным эффектом», путём подключения к их соединительным линиям
Перехват акустических сигналов путём лазерного зондирования оконных стекол	Перехват акустических колебаний через ВТСС путём «высокочастотного навязывания»

В оптико-электронном канале утечки акустической информации съём информации реализуется с помощью инфракрасного лазера. Под действием звуковой волны тонкие отражающие поверхности, например стекло, начинают вибрировать. Лазерное излучение направляется на отражающую поверхность под углом полного отражения. Отражённый лазерный луч модулируется и поступает на вход приёмника оптического излучения. В приёмнике полученный сигнал подвергается демодуляции, усиливается и воспроизводится в виде исходного акустического сигнала.

Методы защиты акустической (речевой) информации разделяются на *пассивные* и *активные*.

Пассивные методы направлены на уменьшение уровней акустических сигналов, проникающих за пределы защищаемого помещения, а также на ослабление продуктов электроакустических преобразований во вспомогательных и основных технических средствах и системах, а также в соединяющих их цепях.

Активные методы предусматривают создание маскирующих помех и подавление или уничтожение технических средств акустической разведки.

Звукоизоляция является основным *пассивным методом* защиты акустической (речевой) информации. Выделение акустического сигнала злоумышленниками возможно, если отношение сигнал/шум лежит в определённом диапазоне. Основная цель применения пассивных средств защиты информации – снижение соотношения сигнал/шум в возможных точках перехвата информации за счёт максимального снижения уровня информативного сигнала. Таким образом, звукоизоляция локализует источники излучения в замкнутом пространстве с целью снижения отношения сигнал/шум до предела, исключающего или значительно затрудняющего съём акустической информации.

Когда пассивные методы защиты не могут обеспечить необходимый уровень безопасности, применяют *активные методы* защиты, в частности акустическое или вибрационное **зашумление**.

Для защиты помещений применяют генераторы шума и системы вибрационного зашумления, которые формируют шумовые, «речеподобные» и комбинированные помехи.

Средства создания акустических помех можно разделить на следующие виды:

- генераторы шума в акустическом диапазоне;
- устройства виброакустической защиты;
- технические средства ультразвуковой защиты помещений.

Ещё одним распространённым *активным методом* защиты акустической информации от утечки является применение подавителей диктофонов.

Диктофон является одним из наиболее популярных средств для съёма информации. Это обусловлено простотой использования, малыми размерами и относительной дешевизной данных устройств. Поэтому в настоящее время вопрос подавления диктофонов часто выделяют в отдельную тему при рассмотрении способов защиты информации от утечки по акустическим каналам утечки.

Для подавления диктофонов используют генераторы мощных шумовых сигналов дециметрового диапазона частот. Эти сигналы воздействуют на микрофонные цепи и усилительные устройства диктофонов и записываются на диктофон вместе с полезными сигналами. Зона, в которой устройство может подавлять диктофоны, зависит от мощности излучения, свойств антенны и типа зашумляющего сигнала. Средний радиус зоны подавления – 5 метров, ширина сектора – от 30 до 80 градусов.

3.3. Побочные электромагнитные излучения и наводки

При функционировании радиоэлектронных средств и электрических приборов возникают побочные излучения электромагнитных полей (ЭМ-полей), которые могут содержать защищаемую информацию. Источниками излучений чаще всего являются токопроводящие цепи, содержащие статические или динамические заряды. Носители информации могут попадать в цепи непосредственно в процессе обработки информации, а также через паразитные связи.

Защита информации от утечки через ПЭМИН осуществляется с применением **пассивных и активных методов и средств.**

Пассивные методы защиты информации от утечек через ПЭМИН направлены:

- на снижение уровня побочных электромагнитных излучений информационных сигналов технических средств на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения техническим средством съёма информации на фоне естественных шумов;
- снижение уровня наводок побочных электромагнитных излучений в посторонних проводниках и соединительных линиях, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством съёма информации на фоне естественных шумов;
- снижение уровня или исключение проникания информационных сигналов в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством съёма информации на фоне естественных шумов.

Активные методы защиты информации от утечек через ПЭМИН направлены:

- на генерацию маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного сигнала техническим средством съёма информации;
- формирование маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного сигнала техническим средством съёма информации.

Одним из наиболее эффективных пассивных методов защиты от паразитных электромагнитных излучений является экранирование.

Экранирование – локализация электромагнитной энергии в определённом пространстве за счёт ограничения распространения её всеми возможными способами.

Наиболее распространенными металлами для изготовления экранов являются сталь, медь, алюминий, латунь. Популярность этих материалов в первую очередь обусловлена высокой эффективностью экрани-

рования. Вследствие возможности использования сварки при монтаже экрана среди перечисленных материалов популярна сталь.

Недостатками листовых металлических экранов являются высокая стоимость, большой вес, крупные габариты и сложность монтажа. Этих недостатков лишены металлические сетки. Они легче, дешевле, проще в изготовлении и размещении.

Для экранирования также применяются фольгированные материалы. К ним относятся электрически тонкие материалы толщиной 0,01-0,05 мм. Фольгированные материалы в основном производятся из диамагнитных материалов – алюминия, латуни, цинка.

Применение токопроводящих красок значительно облегчает процесс электромагнитного экранирования, т.к. такие краски недороги, не требуют квалифицированных работ по монтажу, просты в применении.

Экранирование ТСПИ и соединительных цепей эффективно только в случае их правильного **заземления**. Заземление состоит из заземлителя и заземляющего проводника, соединяющего заземляемое устройство с заземлителем. Заземлитель – это проводящая часть, которая может быть простым металлическим стержнем (чаще всего стальным, реже медным) или сложным комплексом элементов специальной формы.

Еще одним методом локализации опасных сигналов является **фильтрация опасных сигналов**. Фильтрация применяется к источникам электромагнитных полей и наводок с целью предотвращения распространения опасных сигналов за их пределы. Для фильтрации в цепях питания технических средств применяются разделительные трансформаторы и помехоподавляющие фильтры.

Разделяющие трансформаторы обеспечивают развязку первичной и вторичной цепей по сигналам наводки, т.е. наводки первичной обмотки трансформатора не должны попадать во вторичную. Для уменьшения влияния паразитных индуктивных и ёмкостных связей между обмотками трансформатора ставят экран. Чаще всего экран представляет собой заземлённую прокладку или фольгу, которая укладывается между двумя обмотками трансформатора. Благодаря этому наводки, возникающие в первичной цепи, «выбирают» путь с наименьшим сопротивлением. Применение в разделительных трансформаторах экранирования позволяет существенно (более чем на 40 дБ) уменьшить уровень наводок.

К пассивным средствам защиты от утечек акустической информации по проводным линиям относят и **помехоподавляющие фильтры**. Основное назначение таких фильтров – пропускать сигналы с частотами, лежащими в заданной полосе частот, и подавлять (ослаблять) сигналы с частотами, лежащими за пределами этой полосы. Помехоподавляющие фильтры применяются для исключения просачивания информационных сигналов в цепи электропитания и линии телефонной связи.

Рассмотренные выше пассивные методы защиты обеспечивают снижение отношения сигнал/шум на границе контролируемой зоны. При этом нередко данное отношение превышает установленный допустимый уровень, несмотря на применение фильтров и экранирования. В таких случаях применяют **активные методы защиты**, создающие помехи для технических средств съёма информационных сигналов и уменьшающие отношение сигнал/шум на входе приёмной аппаратуры.

Исключение перехвата ПЭМИН по электромагнитному каналу обеспечивается **пространственным зашумлением**, а для исключения съёма наведённых информационных сигналов с посторонних проводников и соединительных линий технических средств обработки, передачи и хранения информации применяют **линейное зашумление**.

Системы пространственного зашумления обычно строятся на основе генераторов типа «синфазные помехи» и «белый шум». Генераторы синфазных помех применяются преимущественно для защиты компьютеров. В качестве сигнала зашумления в этом случае используются импульсы со случайной амплитудой, синхронизированные с импульсами защищаемого информационного сигнала, т.е. с тактовым генератором компьютера. Таким образом, генерируются так называемые имитационные помехи, по спектральному составу похожие на защищаемые сигналы. При этом выделение информационного сигнала практически невозможно даже с применением наиболее совершенных методов цифровой фильтрации.

Генератор «белого шума» представляет собой широкополосный сигнал с равномерным энергетическим спектром во всём рабочем диапазоне частот. Уровень мощности такого сигнала существенно превышает уровень мощности побочных электромагнитных излучений (ПЭМИ). «Белый шум» применяется для защиты многих устройств, в

частности электронно-вычислительной техники, систем внутреннего телевидения и т.п.

Генератор имитационной помехи выполняется в виде отдельной платы, вставляемой в свободный слот компьютера. Генераторы «белого шума», как правило, изготавливают в виде отдельного блока с питанием от электросети.

Системы **линейного зашумления** применяются для маскировки наведённых опасных сигналов в выходящих за пределы контролируемой зоны посторонних проводниках и соединительных линиях технических средств.

Система линейного зашумления в общем случае состоит из генератора шумового сигнала, который формирует шумовое маскирующее напряжение в заданной полосе частот. Генераторы шума подключаются непосредственно к линии.

3.4. Визуально-оптический канал утечки информации

Визуально-оптический канал утечки информации образуется в результате распространения электромагнитных волн оптического диапазона, отражённых от объектов и окружающей обстановки, и реализуется путём применения специальных технических средств, расширяющих возможности органа зрения человека по видению в условиях малой освещённости, при удаленности объектов наблюдения и недостаточности углового разрешения. При этом часто осуществляют документирование зрительной информации с применением электронных носителей.

Довольно широко для наблюдения применяются *видеосъёмка* и *фотографирование*. Используемые **видеокамеры** могут быть проводными, радиопередающими, носимыми и т.д. Современная аппаратура позволяет вести наблюдение при дневном освещении, в условиях сумерек, ночью, на сверхблизком расстоянии, на удалении до нескольких километров. Чувствительные матрицы камер работают в видимом свете и в инфракрасном диапазоне.

Для наблюдения в условиях низкой освещенности или плохой видимости используются приборы ночного видения и тепловизоры. В основу современных **приборов ночного видения** заложен принцип преобразования отражённого излучения инфракрасного диапазона в слабое поле электронов, усиления полученного электронного изобра-

жения с помощью микроканального усилителя и конечного преобразования с помощью люминесцентного экрана в видимое изображение. Изображение формируется при этом в видимой глазом области спектра (как правило, в зелёной области спектра). Изображение на люминесцентном экране воспринимается непосредственно глазом человека или регистрирующим прибором. Приборы ночного видения способны воспринимать излучение в ближнем ИК-диапазоне, пассивные приборы используют для работы отражённый свет звезд и луны, активные приборы содержат в своём составе источники ИК-излучения на основе галогенных ламп с ИК-фильтром или полупроводниковых или лазерных ИК-излучателей, что позволяет вести наблюдение в полной темноте. Конструктивно приборы ночного видения выполняются в виде биноклей, монокуляров, визиров, очков ночного видения, прицелов для стрелкового оружия.

Тепловизоры воспринимают собственное тепловое излучение объектов и работают на участке спектра частот 8-13 мкм, в котором находится максимум теплового излучения предметов. При этом на работу тепловизоров не оказывают влияние туман, дождь, снег и т.д. К недостаткам тепловизоров можно отнести низкое угловое разрешение.

В настоящее время на рынке представлены неохлаждаемые тепловизоры с разрешением по температуре до 0,1^{o}C.

Приборы для документирования изображения включают в себя комплекты аппаратуры: высококачественный прибор ночного видения, инфракрасный излучатель, опорно-поворотное устройство (штатив), устройство регистрации изображения (фотокамера, видеокамера). Компоненты таких систем изготавливаются по установленным стандартам и легко совмещаются со стандартными объективами.

Стремительное развитие микротехнологий позволило создать сверхминиатюрные камеры, вследствие чего значительно упростилась задача несанкционированного получения видеоинформации. Достижения в области миниатюризации позволяют разместить подобную видеокамеру практически в любых предметах интерьера или личных вещах.

Современные оптоволоконные системы наблюдения базируются на световодах и имеют в своём составе оптический кабель длиной до трёх метров. Такие системы, имея угол обзора до 65^{o} и широкий диапазон фокусировки, позволяют проникать в помещения через замочные

скважины, кабельные и отопительные вводы, вентиляционные шахты, потолки и другие отверстия. Высокая чувствительность обеспечивает нормальную работу даже при слабом освещении. Стандартными возможностями подобных систем являются чтение и фотографирование документов на столах, заметок в настольных календарях, настенных таблиц и диаграмм, информации с мониторов компьютеров.

Способы обнаружения скрытых камер гораздо сложнее распознавания других каналов утечки информации. Сегодня поиск работающих видеокамер с передачей сигнала по радиоканалу и проводам осуществляется методом нелинейной локации и методом анализа спектра. Все схемы современных электронных устройств состоят из полупроводниковых компонентов, поэтому могут быть обнаружены специальными приборами, называемыми нелинейными локаторами. Кроме того, работающие видеокамеры излучают электромагнитные волны радиодиапазона: при этом «шумят» электронные схемы управления ПЗС-матрицами видеокамер. Так как каждая камера имеет присущий только ей спектр побочного излучения, работающую видеокамеру можно обнаружить и идентифицировать специальным прибором обнаружения видеокамер. Такой прибор, являющийся, по сути, упрощённым анализатором спектра, снимает профиль спектра побочного излучения камеры и сравнивает его с хранящимися в памяти прибора эталонными спектрами известных камер, что в итоге позволяет указать не только на наличие видеокамеры, но и вывести предположительную информацию о её типе, производителе и т.д. Сложность применения таких приборов заключается в малом уровне излучений некоторых видов камер и наличии большого количества электромагнитных помех.

Глава 4

Нормативно-правовое регулирование мероприятий по защите объектов ОВД от утечки информации ограниченного доступа

4.1. Виды информации ограниченного доступа, обрабатываемой на объектах информатизации ОВД

В зависимости от правового режима доступа выделяют следующие виды информации:

- общедоступная информация;
- информация с ограниченным доступом.

Информацию с ограниченным доступом, в свою очередь, подразделяют:

- на государственную тайну;
- персональные данные;
- тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20.08.2004 № 119-ФЗ «О государственной защите потерпевших, свидетелей и других участников уголовного судопроизводства»;
- служебную тайну;
- профессиональную тайну;
- коммерческую тайну;
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Информацию с ограниченным доступом, не составляющую государственную тайну, называют *конфиденциальной информацией*.

В системе ОВД к государственной тайне относятся сведения, перечень которых определяется приказом Министра внутренних дел и федеральным законодательством.

Важным признаком государственной тайны является степень секретности сведений, отнесённых к ней.

В Российской Федерации принята следующая система обозначения сведений, составляющих государственную тайну: *особой важности; совершенно секретно; секретно.*

Гриф секретности проставляется на документах или изделиях (их упаковках или сопроводительных документах), а содержащиеся под этими грифами сведения являются государственной тайной.

Правила отнесения сведений, составляющих государственную тайну, утверждённые Постановлением Правительства РФ от 4 сентября 1995 г. № 870, определяют степени секретности:

- к сведениям *особой важности* относят такие сведения, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких областях;
- к *совершенно секретным* сведениям относят такие сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отраслям экономики Российской Федерации в одной или нескольких областях;
- к *секретным* сведениям относят все иные сведения из числа сведений, составляющих государственную тайну. Ущерб может быть нанесён интересам предприятия, учреждения или организации.

В соответствии с законом для организации, обрабатывающей государственную тайну, обязательным условием является наличие лицензии ФСБ «На осуществление работ с использованием сведений, составляющих государственную тайну». В «Положении по аттестации объектов информатизации по требованиям безопасности информации» от 25.11.1994 предусмотрена обязательная аттестация объектов, обрабатывающих государственную тайну.

Один из распространенных в органах внутренних дел видов информации ограниченного доступа – *служебная тайна*, что непосредственно связано с функционированием самой системы ОВД. В соответствии с Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденным Постановлением Правительства РФ от 3 ноября 1994 г. № 1233, к служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью.

В системе МВД России служебную тайну составляет информация, которая:

- образуется в процессе деятельности органов, подразделений и учреждений системы МВД России и войск национальной гвардии РФ или передана им из других федеральных органов исполнительной власти;
- не составляет государственной тайны, однако её разглашение (распространение) может нанести ущерб интересам МВД России;
- имеет действительную или потенциальную ценность и может являться предметом посягательств в силу неизвестности её другим лицам и отсутствия к ней свободного доступа на законных основаниях.

Другая разновидность конфиденциальной информации, в больших объемах обрабатываемая в информационных системах МВД, – персональные данные.

Персональные данные – это любая информация, относящаяся к определенному физическому лицу, в т.ч. его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»).

Сведения, относящиеся к персональным данным, необходимы сотрудникам органов внутренних дел для предотвращения преступлений и административных правонарушений; выявления обстоятельств, способствующих их совершению; осуществления оперативно-разыскной деятельности; производства дознания и предварительного следствия; экспертно-криминалистической деятельности; розыска лиц и похищенного имущества; выдачи гражданам различного рода лицензий и разрешений и т.д.

4.2. Обработка персональных данных, содержащихся в информационных системах ОВД

В системе Министерства внутренних дел в настоящее время используются более 100 различных информационных систем персональных данных (далее – ИСПДн), которые в соответствии с требованиями руководящих документов нуждаются в защите.

В данный момент основным действующим нормативным документом, определяющим требования к защите ИСПДн, является Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Порядок выполнения мероприятий по защите персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, определяет Приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации», который также устанавливает меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, а также определяет обязанности должностных лиц.

Вышедший 16 сентября 2013 г. Приказ МВД от 15 июля 2013 г. № 538 «О внесении изменений в Приказ МВД России от 06.072012 № 678 "Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации"», утвердил замену устаревшей терминологии в соответствии с Постановлением Правительства № 1119 и ввел в качестве методических документов, регламентирующих установление класса защищённости информационной системы и уровня защищённости персональных данных, Постановление Правительства № 1119 от 01.11.2012, приказы ФСТЭК № 17 от 11.02.2013 и № 21 от 18.02.2013.

Для информационных систем, обрабатывающих персональные данные, устанавливаются четыре класса защищённости, определяющие уровни защищённости содержащейся в них информации. Самый низкий класс – четвертый, самый высокий – первый.

Классы защищённости информационных систем персональных данных определены в соответствии с требованиями Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Определение уровней защищённости персональных данных в ИСПДн проводится в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об

утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». В информационных системах устанавливаются четыре уровня защищённости персональных данных.

В соответствии с информационным сообщением ФСТЭК от 15.07.2013 № 240/22/2637 в качестве методического документа при реализации защиты технических средств государственных информационных систем, обрабатывающих конфиденциальную информацию, в целях нейтрализации угроз безопасности информации, связанных с утечкой информации посредством информативных электрических сигналов и физических полей (защита от утечки по техническим каналам), применяется методический документ Гостехкомиссии «СТР-К».

При применении криптографических средств защиты в информационных системах, обрабатывающих персональные данные, обязателен для исполнения Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости».

Глава 5

Контроль эффективности защиты информации: категорирование объектов, аттестация объектов, спецпроверки

Важным и необходимым направлением работ по защите информации является контроль эффективности защиты. Этот вид деятельности проводится, прежде всего, силами подразделений, отвечающих за информационную защиту, а также руководителями структурных подразделений. Составной частью контроля защиты информации является контроль инженерно-технической защиты, заключающийся, прежде всего, в определении (измерении) показателей эффективности защиты техническими средствами и сравнении их с нормативными показателями.

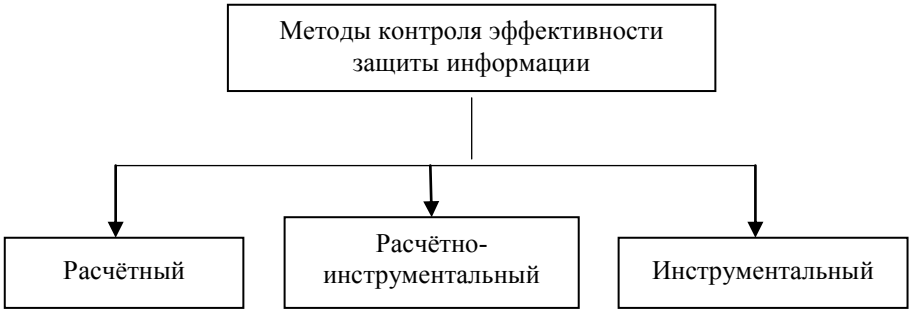

Рис. 4. Методы контроля эффективности защиты информации

В настоящее время используются расчётные, расчётно-инструментальные и инструментальные методы контроля эффективности защиты информации.

Различают также следующие виды контроля эффективности защиты:

- предварительный контроль;
- периодический контроль;
- постоянный контроль.

Предварительный контроль проводится при любых изменениях состава, структуры и алгоритма функционирования системы защиты информации, в т.ч.:

- после установки нового технического средства защиты или изменения организационных мер;
- после проведения профилактических и ремонтных работ средств защиты;
- после устранения выявленных нарушений в системе защиты.

Периодический контроль осуществляется с целью обеспечения систематического наблюдения за уровнем защиты. Он проводится выборочно (применительно к отдельным темам работ, структурным подразделениям или всей организации) по планам, утверждённым руководителем организации, а также вышестоящими органами.

Постоянный контроль осуществляется выборочно силами подразделений информационной безопасности и привлекаемых сотрудников с целью объективной оценки уровня защиты информации и выявления слабых мест в системе защиты информации. Кроме того, такой контроль оказывает психологическое влияние на сотрудников, формируя ответственное отношение к обеспечению соблюдения правил обработки информации ограниченного доступа.

Кроме того, существует деление мер контроля эффективности защиты информации на организационные и технические, в совокупности представляющие собой такие этапы оценки эффективности, как категорирование, аттестацию объектов, проведение специальных проверок, специальных исследований и специальных обследований.

5.1. Категорирование и аттестация объектов информатизации ОВД

Эффективность защиты информации на объекте обеспечивается, как известно, в соответствии с категорией важности этого объекта.

Категорирование объектов информатизации производится в первую очередь по виду обрабатываемой на объекте информации.

Категорирование объекта защиты – установление градаций важности защиты объекта защиты.

При категорировании объектов информатизации, обрабатывающих информацию, составляющую государственную тайну, выделяют три типа объектов защиты:

1) автоматизированная система (АС – автономная ПЭВМ или локальная вычислительная сеть);

2) выделенное помещение (ВП – для проведения секретных переговоров);

3) система изготовления и размножения документов (СИРД – копировальная техника и т.п.).

При обработке в информационных системах информации, составляющей государственную тайну, обязательно выполнение требований методического документа Гостехкомиссии (ФСТЭК) «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам» (СТР). Содержание самого документа также составляет государственную тайну.

Для объектов информатизации, обрабатывающих конфиденциальную информацию, категорирование не проводится, и правовое регулирование средств защиты определяется федеральными законами, ведомственными приказами и приказами ФСТЭК.

Следующим этапом после категорирования объекта информатизации является его аттестация.

Аттестация предусматривает аттестационные испытания (комплексную проверку) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Соответствие объекта требованиям безопасности подтверждается посредством специального документа – аттестата соответствия.

Аттестация объектов информатизации – это комплекс организационно-технических мероприятий, в результате которых подтверждается, что объект соответствует требованиям нормативно-технических документов по безопасности информации, утверждённых ФСТЭК и ФСБ России.

Деятельность по аттестации объектов информатизации по требованиям безопасности информации (за исключением средств криптографической защиты информации) осуществляет ФСТЭК России.

В качестве органов по аттестации могут выступать региональные учреждения и организации по защите информации, специальные центры ФСТЭК России, которые прошли соответствующую аккредитацию.

Аттестацию внутренних объектов информатизации системы МВД России также могут проводить аккредитованные отделы защиты информации региональных центров информационных технологий, связи и защиты информации МВД России.

Аккредитация ФСТЭК органов аттестации проводится в соответствии с «Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации».

Органы по аттестации несут ответственность за выполнение своих функций, за сохранение в секрете информации, полученной в ходе аттестации, а также за соблюдение авторских прав заказчика.

В структуру системы аттестации входят:

- ФСТЭК России – федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации;
- органы по аттестации объектов информатизации по требованиям безопасности информации;
- испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;
- заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

Органы по аттестации выполняют следующие функции:

- аттестуют объекты информатизации и выдают аттестаты соответствия;
- контролируют безопасность информации, циркулирующей на аттестованных объектах информатизации, и их эксплуатацию;
- отменяют и приостанавливают действие выданных этим органом аттестатов соответствия;
- формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;
- ведут информационную базу аттестованных этим органом объектов информатизации;
- взаимодействуют с ФСТЭК России и ежеквартально информируют его о своей деятельности в области аттестации.

В рамках системы аттестации ФСТЭК осуществляет следующие функции:

- организует обязательную аттестацию объектов информатизации;
- создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;
- устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;
- организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;
- аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определённых видов работ;
- осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;
- рассматривает апелляции, возникающие в процессе аттестации объектов информатизации и контроля за эксплуатацией аттестованных объектов информатизации;
- организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.

Испытательные лаборатории проводят испытания несертифицированных устройств, используемых на аттестуемом объекте информатизации. Список таких лабораторий утверждает ФСТЭК России.

5.2. Специальные проверки, специальные обследования и специальные исследования объектов

Принято выделять три группы мероприятий по выявлению технических каналов утечки информации:

- специальные проверки;
- специальные обследования;
- специальные исследования, включающие в себя:
  - выявление внедренных закладок в защищаемом помещении;
  - выявление самотехнических и других доработок технических средств и систем (ТСС), приводящих к усилению естественных свойств ТСС;
  - выявление программных закладок, имеющих процессорное управление.

Специальная проверка технических средств и систем представляет собой комплекс инженерно-технических мероприятий, проводимых с использованием необходимых технических средств. Цель проверки – исключение перехвата информации, содержащей государственную тайну, с помощью внедренных в защищаемое помещение закладок и других технических средств разведки. Основные определения приведены в ГОСТе Р 51583-2014 «Порядок создания автоматизированных систем в защищённом исполнении».

Специальная проверка (СП) – проверка компонентов автоматизированной системы, осуществляемая с целью поиска и изъятия закладочного устройства.

Специальная проверка технических средств и систем состоит из следующих этапов:

- приём-передача технического средства, формирование исходных данных для составления программы проведения специальной проверки;
- разработка программы проведения специальной проверки технического средства;
- проведение технической проверки;
- анализ результатов и оформление отчетных документов.

Специальные обследования (СО) выделенных помещений – комплекс инженерно-технических мероприятий, проводимых с использованием необходимых, в т.ч. и специализированных, технических средств. Цель СО – выявление возможно внедрённых специальных электронных средств перехвата информации, содержащей государственную тайну, в ограждающих конструкциях, предметах мебели и интерьера выделенных помещений.

Проведение поисковых мероприятий включает в себя:

- радиообнаружение;
- осмотр помещения;
- обследование электрических и электронных приборов;
- проверка проводных коммуникаций.

Для **радиообнаружения** используются такие технические средства, как радиочастотометры, индикаторы поля, сканирующие приёмники, анализаторы спектра и т.д. Для эффективного радиообнаружения предварительно формируют карту загрузки радиодиапазона. Карту загрузки получают на расстоянии от 300 до 1 000 м от исследуемого объекта.

Сравнение этой карты с картой радиодиапазона исследуемого помещения упростит обнаружение излучающих объектов, локализованных в исследуемом помещении. Эффективность радиоконтроля во многом зависит от квалификации операторов, проводящих проверку.

Осмотр включает в себя визуальный осмотр помещения и находящихся в нем предметов. При этом чтобы исключить пропуск места установки закладного устройства, контроль проводят по заранее определенной схеме. Как правило, осмотр проводят по часовой стрелке. Во время осмотра все электронные приборы временно удаляют из помещения или перемещают в одно место. Стены и потолки осматривают на выявление наличия изменения тона окраски и отверстий неизвестного назначения. Мебель, препятствующая осмотру стен, пола и потолка, отодвигается. Сама мебель также подвергается тщательному осмотру. Электроосветительные приборы и электророзетки отключают, снимают и разбирают. Для осмотра труднодоступных мест применяют эндоскопы и комплекты досмотровых зеркал. Предметы, размещаемые на стенах, осматривают снаружи и внутри на изменение тона покрытия или характерные «пылевые» следы. Проверяют окна в открытом и закрытом состояниях, обращая внимания на полости, шторы, карнизы и подоконники. Обследуются все предметы в помещении.

Все объекты, вызвавшие сомнения при осмотре, подвергаются технической проверке. Проверка предметов мебели и интерьера проводится на подготовленной площадке, предварительно проверенной на наличие помех, с применением средства нелинейной локации и переносного рентгеновского аппарата.

Следующим шагом является **проверка электрических и электронных приборов**. Электрические приборы (настольные лампы, нагревательные приборы и т.п.) перед проверкой включают в сеть и с помощью индикатора поля определяют наличие в них источника радиоизлучения. При обнаружении радиоизлучений, не заложенных конструкцией, прибор проверяют с помощью комплекса радиообнаружения. Затем проверяемый прибор обесточивают, разбирают и осматривают.

Наибольшие трудности вызывает обнаружение закладочных устройств в электронных приборах (компьютерах, оргтехнике, электронных часах и т.п.). Облегчает обнаружение сравнение снимков исследуемого прибора с типовыми блоками аналогичных приборов. Осо-

бое внимание уделяют наличию в приборе небольших элементов неизвестного назначения и элементов, отличающихся от аналогичных на эталонных изображениях.

Далее осуществляют **проверку проводных коммуникаций.** Осмотр каждой линии начинают с установления трассы её прохождения в помещение. Как правило, сначала проверяют электросеть, затем телефонные линии и кабели сигнализации. При этом особое внимание уделяется линиям, назначение которых неизвестно.

Специальные исследования (СИ) – выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем и оценка соответствия защиты информации требованиям нормативных документов по защите информации.

Задачей СИ является выявление и измерение **опасных сигналов** – информационных сигналов в потенциальных каналах утечки информации. Задача специального исследования сводится к измерению сигнала передатчика защищаемой информации и пересчету измеренных значений к величине, которая может поступить на вход технического средства съема информации. Затем по специальным методикам происходит вычисление отношения сигнал/шум и сравнение его с нормированными величинами.

При проведении специальных исследований акустического, виброакустического каналов утечки информации, а также ПЭМИН успешно эксплуатируется ряд автоматизированных комплексов, которые существенно облегчают работу оператора.

Оценка защищенности объектов от утечек информации по акустическому, виброакустическому, электрическому и электромагнитному каналам является задачей, требующей большой квалификации операторов и наличия дорогой аппаратуры. Документы ФСТЭК и Гостехкомиссии, по которым оценивается защищенность на объектах, обрабатывающих информацию, составляющую государственную тайну, не доступны для общего пользования, поэтому для оценки их защищённости привлекаются организации, у которых есть лицензия ФСТЭК на проведение специальных исследований: они имеют в своём арсенале методики ограниченного доступа, квалифицированных специалистов и необходимые технические средства.

Список литературы

1. Еськов А.В., Кирюшин И.И. Защита информационных систем с содержанием персональных данных, эксплуатируемых в ОВД // Проблемы правоохранительной деятельности. 2015. № 2. С. 76-79.

2. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006 (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 28.01.2014 № 3-ст). Национальный стандарт РФ. URL: http://standartgost.ru/g/ГОСТ_Р_51583-2014 (дата обращения: 02.11.2016).

3. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: ГОСТ Р 21583-2014 (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 28.01.2014 № 3-ст). Национальный стандарт РФ. URL: http://standartgost.ru/g/ГОСТ_Р_50922-2006 (дата обращения: 02.11.2016).

4. Кемпф В.А. Технические средства контроля и досмотра: учеб. пособие. Барнаул: БЮИ МВД России, 2013. 43 с.

5. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федеральный закон от 27 июля 2006 г. № 149-ФЗ (действ. ред., 2016). Доступ из справ.-правовой системы «КонсультантПлюс».

6. Об оперативно-розыскной деятельности [Электронный ресурс]: федеральный закон от 12 августа 1995 г. № 144-ФЗ (действ. ред., 2016 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

7. Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации (с изм. и доп.) [Электронный ресурс]: приказ МВД РФ от 6 июля 2012 г. № 678. Доступ из справ.-правовой системы «КонсультантПлюс».

8. Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности (с изм. и доп.) [Электронный ресурс]: постановление Правительства РФ от 3 ноября 1994 г. № 1233. Доступ из справ.-правовой системы «КонсультантПлюс».

9. Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности (с изм. и доп.) [Электронный ресурс]: постановление Правительства РФ от 4 сентября 1995 г. № 870. Доступ из справ.-правовой системы «КонсультантПлюс».

10. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости [Электронный ресурс]: приказ ФСБ России от 10.07.2014 № 378. Доступ из справ.-правовой системы «КонсультантПлюс».

11. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: приказ ФСТЭК России от 18.02.2013 № 21. Доступ из справ.-правовой системы «КонсультантПлюс».

12. Об утверждении Типового положения и подразделении информационных технологий, связи и защиты информации территориального органа Министерства внутренних дел Российской Федерации [Электронный ресурс]: приказ МВД России от 2 июля 2012 г. № 660. Доступ из справ.-правовой системы «КонсультантПлюс».

13. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: постановление Правительства РФ от 01.11.2012 № 1119. Доступ из справ.-правовой системы «КонсультантПлюс».

14. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]: приказ ФСТЭК России от 11.02.2013 № 17. Доступ из справ.-правовой системы «КонсультантПлюс».

15. О внесении изменений в приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации» [Электронный ресурс]: приказ

МВД России от 15 июля 2013 г. № 538. Доступ из справ.-правовой системы «КонсультантПлюс».

16. О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства (с изм. и доп.) [Электронный ресурс]: федеральный закон от 20 августа 2004 г. № 119-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

17. О персональных данных [Электронный ресурс]: федеральный закон от 27 июля 2006 г. № 152-ФЗ (действ. ред., 2016 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

18. О связи [Электронный ресурс]: федеральный закон от 7 июля 2003 г. № 126-ФЗ (в ред. федерального закона от 06.07.2016 № 374-ФЗ). Доступ из справ.-правовой системы «КонсультантПлюс».

19. По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]: информационное сообщение Федеральной службы по техническому и экспортному контролю от 15 июля 2013 г. № 240/22/2637. Доступ из справ.-правовой системы «КонсультантПлюс».

20. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ 25 ноября 1994 г.) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

21. Специальная техника органов внутренних дел: словарь / сост. В.Э. Баумтрог. Барнаул: БЮИ МВД России, 2009. 92 с.

22. Специальная техника органов внутренних дел: учебник в 2 ч. М.: ДГСК МВД России. 2014. Ч. 1. 264 с.

23. Специальная техника органов внутренних дел: хрестоматия / сост. В.Э. Баумтрог. Барнаул: БЮИ МВД России, 2014. 142 с.

24. Торокин А.А. Инженерно-техническая защита информации: учеб. пособие. М.: Гелиос АРВ, 2005.

25. Хорев А.А. Способы и средства защиты информации. М.: МО РФ, 1998. 316 с.

Содержание

Учебное издание

Кемпф Виктор Александрович
Осинцева Людмила Михайловна

Специальная техника органов внутренних дел: технические средства защиты информации

Учебное пособие

Редактор О.Н. Татарникова
Корректура, компьютерная верстка С.В. Калининой
Дизайн обложки В.Н. Дроздкова

Лицензия ЛР № 02213552 от 14.07.1999 г.
Лицензия Плр № 020109 от 05.07.1999 г.

Подписано в печать 12.04.2017. Формат 60х90 1/16.
Ризография. Усл. п.л. 2,8. Тираж 146 экз. Заказ 216
Барнаульский юридический институт МВД России.
Научно-исследовательский и редакционно-издательский отдел.
656038, Барнаул, ул. Чкалова, 49; www.бюи.мвд.рф.