МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ имени академика С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»

А.И. МОИСЕЕВ, Д.Б. ЖМУРОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Самарский государственный аэрокосмический университете имени академика С.П. Королева (национальный исследовательский университет)» в качестве учебника для студентов, обучающихся по образовательной программе высшего профессионального образования по специальности «Информационная безопасность автоматизированных систем»

САМАРА
Издательство СГАУ
2013

УДК 004.075
ББК 32.81я7
М748

Рецензенты: канд. техн. наук, доцент А. Д. П а ц ю к;
д-р техн. наук, профессор В. А. З е л е н с к и й

Моисеев А.И.
М748 **Информационная безопасность распределённых информационных систем:** учеб. / *А.И. Моисеев, Д.Б. Жмуров*. – Самара: Изд-во Самар. гос. аэрокосм. ун-та, 2013. – 180 с.

ISBN 978-5-7883-0943-9

В учебнике изложены правовые основы обеспечения безопасности информационных технологий, объясняется политика государства в этой области. Рассматривается государственная концепция построения системы защиты информации в распределенных информационных системах. Особое внимание уделено рассмотрению разведывательных средств и совокупности методов противодействия незаконному доступу к информации.

Предназначен для студентов факультета информатики, обучающихся по направлению подготовки специалистов 090303.65 «Информационная безопасность автоматизированных систем» (специалитет) в 9 семестре, и студентов других специальностей, изучающих информационные технологии.

УДК 004.075
ББК32.81я7

ISBN978-5-7883- 0943-9

ОГЛАВЛЕНИЕ

1 ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1.1 Политика государства в области защиты информации

Современный этап развития системы обеспечения информационной безопасности государства и общества характеризуется переходом от тотального сокрытия большого объёма сведений к гарантированной защищённости принципиально важных данных, обеспечивающей:

- конституционные права и свободы граждан, предприятий и организаций в сфере информатизации;
- необходимый уровень безопасности информации, подлежащей защите;
- защищенность систем формирования и использования информационных ресурсов (технологий, систем обработки и передачи данных).

Ключевым моментом политики государства в данной области является осознание необходимости защиты любых информационных ресурсов и информационных технологий, неправомерное обращение с которыми может нанести ущерб их обладателю (собственнику, владельцу, пользователю) или иному лицу.

В Стратегии развития информационного общества в Российской Федерации (утверждена Президентом Российской Федерации 07.02.2009 № Пр-212) одной из ключевых задач, требующих решения для достижения целей формирования и развития информационного общества в России, значится:

- противодействие использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам России;
- обеспечение безопасности функционирования информационно-телекоммуникационной инфраструктуры;
- обеспечение безопасности функционирования информационных и телекоммуникационных систем ключевых объектов инфра-

структуры Российской Федерации, в том числе критических объектов и объектов повышенной опасности;

- повышение уровня защищённости корпоративных и индивидуальных информационных систем;
- создание единой системы информационно-телекоммуникационного обеспечения нужд государственного управления, обороны страны, национальной безопасности и правопорядка;
- совершенствование правоприменительной практики в области противодействия угрозам использования информационных и телекоммуникационных технологий во враждебных целях;
- обеспечение неприкосновенности частной жизни, личной и семейной тайны, соблюдение требований по обеспечению безопасности информации ограниченного доступа;
- противодействие распространению идеологии терроризма и экстремизма, пропаганде насилия.

Развитие информационного общества в Российской Федерации базируется на принципах минимизации рисков и угроз национальной безопасности России, связанных с враждебным и преступным использованием возможностей информационно-коммуникационных технологий, укреплении доверия и безопасности при их использовании.

В Стратегии национальной безопасности Российской Федерации до 2020 года (утверждена Указом Президента Российской Федерации от 12.05.2009 № 537) сказано, что государственная политика Российской Федерации в области национальной безопасности обеспечивается согласованными действиями всех элементов системы обеспечения национальной безопасности при координирующей роли Совета Безопасности Российской Федерации за счёт реализации комплекса мер организационного, нормативно-правового и информационного характера.

Угрозы информационной безопасности в ходе реализации настоящей Стратегии предотвращаются за счёт совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации, повышения уровня защищённости корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.

Меры нормативной правовой поддержки регулирования вопросов информатизации и защиты информации в Российской Федерации определяются на основании:

- Конституции Российской Федерации и федеральных конституционных законов;
- международных договоров и соглашений;
- законов Российской Федерации (кодексеальных и общего действия);
- указов и распоряжений Президента Российской Федерации;
- постановлений и распоряжений Правительства Российской Федерации;
- технических регламентов;
- национальных стандартов (государственных) и стандартов организаций;
- нормативных правовых актов (положения, порядки, руководства, концепции и другие нормативные и методические документы) уполномоченных федеральных органов исполнительной власти.

1.2 Защищаемая информация

Согласно Доктрине информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895) под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В Конституции Российской Федерации, а также Декларации прав и свобод человека и гражданина Российской Федерации определено, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Ограничения этого права могут устанавливаться законом только в целях охраны личной, семейной, профессиональной, коммерческой и государственной тайны, а также нравственности.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» предусматривает разделение информации на категории свободного и ограниченного доступа (право на тайну). В свою очередь информация ограниченного доступа подразделяется на информацию, отнесённую к государственной тайне и конфиденциальную (рис. 1.1).

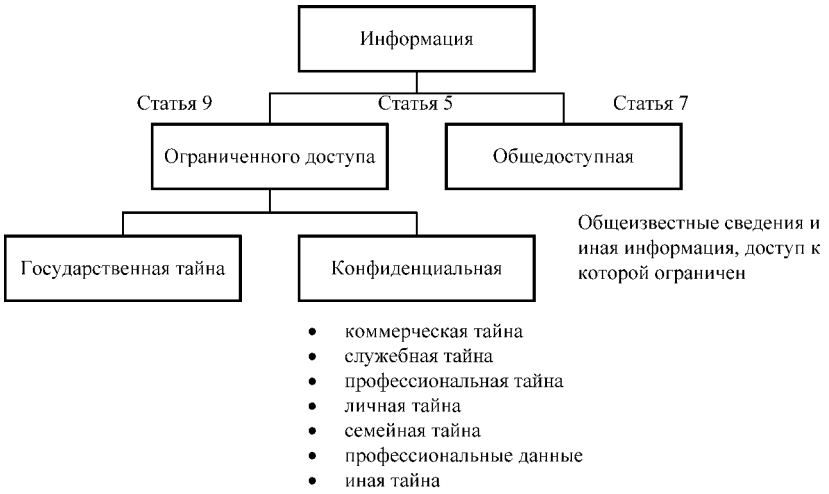

Рис. 1.1. Классификация информации

Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне». Условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за её разглашение устанавливаются федеральными законами.

Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

В Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» даны следующие определения:

информация – сведения (сообщения, данные) независимо от формы их представления;

информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

доступ к информации – возможность получения информации и её использования;

конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя;

предоставление информации – действия, направленные на получение информации определённым кругом лиц или передачу информации определённому кругу лиц;

распространение информации – действия, направленные на получение информации неопределённым кругом лиц или передачу информации неопределённому кругу лиц;

электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

документированная информация – зафиксированная на материальном носителе путём документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях её материальный носитель;

оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в её базах данных.

Согласно ст. 6 данного Федерального закона ***обладатель информации имеет право:***

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

При этом обладатель информации обязан:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Кроме того, обладатель информации, оператор информационной системы ***в случаях, установленных законодательством Российской Федерации,*** обязаны обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности (ФСБ России) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России), в пределах их полномочий. При создании и эксплуатации государственных информационных систем, используемые в целях защиты информации методы и способы её защиты должны соответствовать указанным требованиям.

Следует также отметить, что согласно ст. 8 не может быть ограничен доступ:

- к нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информации о состоянии окружающей среды;
- информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
- иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Например, ст. 5 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» гласит, что «режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

- содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
- о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
- о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

- о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
- о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;
- об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
- о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами».

Кроме того, постановлением Правительства РСФСР от 05.12.1991 № 35 установлено, что коммерческую тайну предприятия и предпринимателя не могут составлять:
- учредительные документы и Устав;
- регистрационные удостоверения, лицензии, патенты;
- сведения по установленным формам отчетности о финансово-хозяйственной деятельности ...;
- документы о платежеспособности;
- сведения о численности, составе работающих, их заработной плате, штате и условиях труда, а также о наличии свободных рабочих мест;
- документы об уплате налогов и обязательных платежах;
- сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда;
- сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

Также, постановлением Правительства Российской Федерации от 03.11.1994 № 1233 установлено, что не могут быть отнесены к служебной информации ограниченного распространения:
- акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

- сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;
- описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;
- порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;
- решение по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;
- сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

Перечень сведений конфиденциального характера определён в Указе Президента Российской Федерации от 06.03.1997 № 188 с изменениями от 23.09.2005 №1111:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (***персональные данные***), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, составляющие тайну ***следствия и судопроизводства***, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации;
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (***служебная тайна)***;
- сведения, связанные с ***профессиональной деятельностью,*** доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами ***(коммерческая тайна)***;
- сведения о ***сущности изобретения,*** полезной модели или промышленного образца до официальной публикации информации о них.

1.3 Персональные данные

В Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» даны следующие определения:

- ***персональные данные*** – любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- ***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;
- ***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;
- ***распространение персональных данных*** – действия, направленные на передачу персональных данных определённому кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
- ***использование персональных данных*** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

- ***блокирование персональных данных*** – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- ***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;
- ***обезличивание персональных данных*** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
- ***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;
- ***конфиденциальность персональных данных*** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;
- ***трансграничная передача персональных данных*** – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;
- ***общедоступные персональные данные*** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

1.4 Меры по обеспечению безопасности персональных данных

Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации в соответствии с частью 2 настоящей статьи, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии её хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

Кроме всего прочего ***оператор*** до начала обработки персональных данных ***обязан уведомить уполномоченный орган*** по защите прав субъектов персональных данных о своём намерении осуществлять обработку персональных данных, за исключением случаев обработки персональных данных:

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;
- полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные

не будут распространяться без согласия в письменной форме субъектов персональных данных;

- являющихся общедоступными персональными данными,
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;
- включённых в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных:

1) В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

2) В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

3) В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трёх рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трёх рабочих дней с даты выявления непра-

вомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4) В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трёх рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5) В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трёх рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

Следует также отметить, что Российская Федерация ратифицировала Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных Федеральным законом от **19.12.2005** № 160-**ФЗ** «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», в которой установлено следующее:

1) Российская Федерация заявляет, что ... не будет применять Конвенцию к персональным данным:

а) обрабатываемым физическими лицами исключительно для личных и семейных нужд;

б) отнесённым к государственной тайне в порядке, установленном законодательством Российской Федерации о государственной тайне;

2) Российская Федерация заявляет, что ... будет применять Конвенцию к персональным данным, которые не подвергаются автоматизированной обработке, если применение Конвенции соответствует

характеру действий, совершаемых с персональными данными без использования средств автоматизации;

3) Российская Федерация заявляет, что ... оставляет за собой право устанавливать ограничения права субъекта персональных данных на доступ к персональным данным о себе в целях защиты безопасности государства и общественного порядка.

Согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (утверждено постановлением Правительства Российской Федерации от 15.09.2008 № 687) обработка персональных данных, содержащихся в информационной системе персональных данных либо извлечённых из такой системы (далее – персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из неё.

Также следует отметить, что согласно Указу Президента Российской Федерации от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» руководителям государственных органов предписано:

- обеспечить защиту персональных данных государственных гражданских служащих Российской Федерации, содержащихся в их личных делах, от неправомерного их использования или утраты за счет средств государственных органов в порядке, установленном федеральными законами;
- определить лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных государственных гражданских служащих Российской Федерации в государственном органе и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и

технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы) установлены «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённым постановлением Правительства Российской Федерации от 17.11.2007 № 781.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой но техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых

обеспечивается путём реализации соответствующих организационных мер и (или) путём применения технических средств.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведётся работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Возможные каналы утечки информации при обработке персональных данных в информационных системах определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (далее – уполномоченное лицо). Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищённости персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в пункте 14 настоящего Положения, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора или уполномоченного лица.

При обнаружении нарушений порядка предоставления персональных данных оператор или уполномоченное лицо незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных установлены постановлением Правительства Российской Федерации от 06.07.2008 № 512.

Под материальным носителем понимается машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность.

Настоящие требования не распространяются на отношения, возникающие при использовании:

а) оператором информационной системы персональных данных (далее – оператор) материальных носителей для организации функционирования информационной системы персональных данных, оператором которой он является;

б) бумажных носителей для записи и хранения биометрических персональных данных.

Оператор утверждает порядок передачи материальных носителей уполномоченным лицам, а также обязан:

а) осуществлять учёт количества экземпляров материальных носителей;

б) осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель.

Федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области *персональных* данных, согласно постановлению Правительства Российской Федерации от 16.03.2009 № *228,* является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных утверждены постановлением Правительства Российской Федерации от 06.06.2008 № 512.

Настоящие требования применяются при использовании материальных носителей, на которые осуществляется запись биометрических персональных данных, а также при хранении биометрических персональных данных вне информационных систем персональных данных.

Под материальным носителем понимается машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность (далее – материальный носитель).

Настоящие требования не распространяются на отношения, возникающие при использовании:

а) оператором информационной системы персональных данных (далее – оператор) материальных носителей для организации функционирования информационной системы персональных данных, оператором которой он является;

б) бумажных носителей для записи и хранения биометрических персональных данных.

Порядок передачи материальных носителей уполномоченным лицам утверждает оператор. Оператор вправе установить не противоречащие требованиям законодательства Российской Федерации

дополнительные требования к технологиям хранения биометрических персональных данных вне информационных систем персональных данных в зависимости от методов и способов защиты биометрических персональных данных в информационных системах персональных данных этого оператора. Оператор обязан:

а) осуществлять учёт количества экземпляров материальных носителей;

б) осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель.

Порядок проведения классификации информационных систем персональных данных утверждён совместным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 № 55/86/20. Также следует отметить методические документы ФСТЭК России и ФСБ России:

- методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена Заместителем директора ФСТЭК России 14.02.2008);
- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена Заместителем директора ФСТЭК России 15.02.2008);
- положение о методах и способах защиты информации в информационных системах персональных данных (утверждено Приказом ФСТЭК России от 05.02.2010 № 58, зарегистрировано в Минюсте России 19.02.2010 № 16456);
- методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144);
- типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622).

1.5 Коммерческая тайна

В Федеральном законе от 29.07.2004 № 98-ФЗ **«О коммерческой тайне»** даны следующие определения:

- ***коммерческая тайна*** – режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;
- ***информация, составляющая коммерческую тайну (секрет производства)*** – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введён режим коммерческой тайны;
- ***обладатель информации, составляющей коммерческую тайну*** – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании ограничило доступ к этой информации и установило в отношении её режим коммерческой тайны;
- ***разглашение информации, составляющей коммерческую тайну*** – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, включающих в себя:

- определение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и/или лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Меры по охране конфиденциальности информации признаются разумно достаточными, если:
- исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;
- обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

К сожалению, вступивший в действие Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» не в полной мере обеспечивает неприкосновенность соответствующей информации. В соответствии со статьёй 6 этого Закона, «Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну». При отказе собственника информационных ресурсов добровольно выдать информацию, составляющую коммерческую тайну, она может быть получена в судебном порядке. При этом какого-либо возмещения издержек собственника на предоставление информации не предусматривается. Кроме того, данный Закон не предусматривает отмены ранее принятых нормативных документов по вопросам защиты коммерческой тайны, в том числе и в части, противоречащей Закону. Данное обстоятельство, к сожалению, не способствует устранению

существовавших до принятия Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» правовых коллизий.

Также следует отметить наличие методических документов по технической защите информации, составляющей коммерческую тайну, выпущенных ФСТЭК России:

- методические рекомендации по технической защите информации, составляющей коммерческую тайну (утверждены заместителем директора ФСТЭК России 25.12.2006);
- пособие по организации технической защиты информации, составляющей коммерческую тайну (утверждено заместителем директора ФСТЭК России 25.12.2006).

1.6 Служебная тайна

Общий порядок обращения с документами и другими материальными носителями информации (фото-, кино-, видео-, и аудиопленки, машинные носители информации и др.), содержащими служебную информацию ограниченного распространения, в федеральных органах исполнительной власти, а также на подведомственных им предприятиях, в учреждениях и организациях определён в «Положении о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», утверждённом постановлением Правительства Российской Федерации от 03.11.1994№ 1233.

К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуется служебной необходимостью.

На документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования».

Только лишь руководителям федерального органа исполнительной власти разрешено определять в пределах своей компетенции:

- категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения;
- порядок передачи служебной информации ограниченного распространения другим органам и организациям;
- порядок снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения;
- организацию защиты служебной информации ограниченного распространения.

Должностные лица, принявшие решение об отнесении служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность принятого решения и за соблюдение ограничений, предусмотренных настоящим Положением.

Служебная информация ограниченного распространения без санкции соответствующего должностного лица не подлежит разглашению (распространению).

За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, государственный служащий (работник организации) может быть привлечён к дисциплинарной или иной предусмотренной законодательством ответственности.

Следует также отметить, что согласно и. 1 Указа Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети «Интернет», не допускается.

При необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, указанных выше, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для операторов информационных систем, владельцев информационно-телекоммуникационных сетей и (или) средств вычислительной техники.

Государственные органы в целях защиты общедоступной информации, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, используют только средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.

Размещение технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, осуществляется только при наличии сертификата, разрешающего эксплуатацию таких технических средств в указанных помещениях. Финансирование расходов, связанных с размещением технических средств в указанных помещениях федеральных органов государственной власти, осуществляется в пределах бюджетных ассигнований, предусмотренных в федеральном бюджете на содержание этих органов.

1.7 Банковская тайна

В ст.26 Федерального закона от 02.12.1990 № 395-**1 «О банках и банковской деятельности»** сказано, что «Кредитная организация, Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах её клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону».

Кроме всего прочего, согласно ст.857 части второй **Гражданского кодекса Российской Федерации** (Федеральный закон от 25.01.1996 № 14-ФЗ) «Банк гарантирует тайну счёта и банковского вклада, операций по счёту и сведений о клиенте».

Следовательно, к основным объектам банковской тайны, согласно действующему законодательству, относятся:

Тайна банковского счета – сведения о счетах клиентов и корреспондентов и действиях с ними в кредитной организации (о расчетном, текущем, бюджетном, депозитном, валютном, корреспондентском и т.п. счете, об открытии, закрытии, переводе, переоформлении счета и т.п.);

Тайна операций по банковскому счету – сведения о принятии и зачислении поступающих на счет клиента денежных средств, о выполнении его распоряжений по перечислению и выдаче соответствующих сумм со счета, а также проведении других операций и сделок по банковскому счету, предусмотренных договором банковского счета или законом, установленными в соответствии с ним банковскими правилами, обычаями делового оборота.

Тайна банковского вклада – сведения обо всех видах вкладов клиента в кредитной организации (срочные, до востребования, в пользу третьих лиц, либо на иных условиях, предусмотренных публичным договором банковского вклада).

Тайна частной жизни клиента или корреспондента – сведения о клиенте или корреспонденте, составляющие его личную, семейную тайну и сохраняемые законом как персональные данные этого клиента или корреспондента.

1.8 Информация в ключевых системах информационной инфраструктуры

Надёжное обеспечение информационной безопасности критически важных объектов является одним из важнейших условий для успешного экономического и социально-политического развития российского общества, укрепления обороноспособности страны и безопасности государства. Решение этой проблемы во многом определяется защищённостью информационных ресурсов, телекоммуникационных систем и сетей критически важных объектов, создаваемых и используемых как государственными, так и негосударственными организациями, от угроз преступного или террористического характера в сфере компьютерной информации, деструктивного информационного воздействия со стороны других государств.

В настоящее время федеральными органами исполнительной власти, наделёнными полномочиями нормативно-правового регулирования вопросов обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации, являются ФСТЭК России и ФСБ России.

22 сентября 2006 г. в Государственную Думу был внесён Законопроект (№ п/п: 1 Код: 340741-4) «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры», который был снят с рассмотрения 11.03.2008 в связи с отзывом субъектом права законодательной инициативы.

Тем не менее, ФСТЭК России были разработаны следующие нормативно-методические документы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры:

- общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утверждены заместителем директора ФСТЭК России 18.05.2007);
- базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утверждены заместителем директора ФСТЭК России 18.05.2007);
- методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утверждены заместителем директора ФСТЭК России 18.05.2007);
- рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утверждены заместителем директора ФСТЭК России 19.11.2007).

1.9 Классификация информации ограниченного доступа

Исходя из вышеизложенного, можно ввести простую и понятную классификацию тайн:

- ***по собственнику*** (государственная, негосударственная и т.п.);
- ***по владельцу*** (в своих или чужих руках – государственная, коммерческая, банковская, профессиональная, служебная, персональные данные как особый институт охраны неприкосновенности частного лица и т.п.);
- ***по области применения***, в которой извлекается выгода от монопольного владения (экономическая – коммерческая, политическая, военная и т.п.);
- по степени важности (гриф).

Другие Федеральные законы и нормативные правовые акты Российской Федерации предусматривают:

- лицензирование деятельности предприятий, учреждений и организаций в области защиты информации;
- сертификацию средств защиты информации и средств контроля эффективности защиты, используемых в АС;
- аттестацию (аттестование) автоматизированных информационных систем, обрабатывающих информацию с ограниченным доступом на соответствие требованиям по безопасности информации при проведении работ со сведениями соответствующей степени конфиденциальности (секретности);

- возложение решения вопросов организации лицензирования, аттестации и сертификации на органы государственного управления в пределах их компетенции, определенной законодательством Российской Федерации;
- создание автоматизированных информационных систем в защищенном исполнении и специальных подразделений, обеспечивающих защиту информации с ограниченным доступом, являющейся собственностью государства, а также осуществление контроля защищенности информации и предоставление прав запрещать или приостанавливать обработку информации в случае невыполнения требований по обеспечению ее защиты;
- определение прав и обязанностей субъектов в области защиты информации.

1.10 Лицензирование в области защиты информации

Лицензирование – деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, осуществлению лицензионного контроля, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования.

Лицензия – специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью, в случае, если в заявлении о предоставлении лицензии указывалось на необходимость выдачи такого документа в электронном виде.

Законодательство Российской Федерации предусматривает установление Правительством Российской Федерации порядка ведения *лицензионной* деятельности, перечня видов деятельности, на осуществление которых требуется лицензия, и органов, уполномоченных на ведение лицензионной деятельности.

В соответствии со статьёй 12 Федерального закона от 04.05.2011 № 99-ФЗ ***«О лицензировании отдельных видов деятельности»***

обязательному лицензированию подлежат следующие виды деятельности (в области защиты информации):

- разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств *(за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);*
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;
- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка и производство средств защиты конфиденциальной информации;
- деятельность по технической защите конфиденциальной информации.

В рамках рассматриваемых видов деятельности были выпущены отдельные постановления Правительства Российской Федерации, разъясняющие порядок лицензирования. Среди них:

- Постановление Правительства Российской Федерации от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности»;
- Постановление Правительства Российской Федерации от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»;
- Постановление Правительства Российской Федерации от 31.08.2006 № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;

- Постановление Правительства Российской Федерации от 29.12.2007 № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

- **Необходимо отметить постановление Правительства Российской Федерации от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».**

Под ***технической защитой конфиденциальной информации*** понимается комплекс мероприятий и (или) услуг по её защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию в целях её уничтожения, искажения или блокирования доступа к ней.

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет Федеральная служба по техническому и экспортному контролю.

Лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:

- наличие в штате соискателя лицензии (лицензиата) специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;
- наличие у соискателя лицензии (лицензиата) помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации, и принадлежащих ему по праву собственности или на ином законном основании;
- наличие на любом законном основании производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;
- использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и(или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;

- использование предназначенных для осуществления лицензируемой деятельности программ для электронно-вычислительных машин и баз данных на основании договора с их правообладателем;

- наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации в соответствии с перечнем, установленным Федеральной службой по техническому и экспортному контролю.

Таким образом, вся деятельность по обеспечению технической защиты конфиденциальной информации подпадает под обязательное лицензирование, т.е. владелец АС, в рамках которой обрабатывается, хранится или передаётся конфиденциальная информация, должен обладать лицензией на проведение работ по технической защите информации либо привлекать для проведения подобных работ компании, обладающие такой лицензией.

Другим важным документом, требующим особого внимания, является постановление Правительства Российской Федерации от 29.12.2007 № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами». Настоящим постановлением утверждены сразу четыре положения:

- Положение о лицензировании деятельности по распространению шифровальных (криптографических) средств;
- Положение о лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств;
- Положение о лицензировании предоставления услуг в области шифрования информации;
- Положение о лицензировании разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

К шифровальным (криптографическим) средствам (средствам криптографической защиты информации) относятся:

а) средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации от несанкционированного доступа при её передаче по каналам связи и (или) при её обработке и хранении;

б) средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие

алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путём ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации).

Лицензирование по указанным видам деятельности осуществляется Федеральной службой безопасности Российской Федерации.

Указанные выше положения не работают поотношению к деятельности по распространению, техническому обслуживанию, разработке, производству, предоставлению услуг в области шифрования информации с использованием:

а) шифровальных (криптографических) средств, предназначенных для защиты информации, содержащей сведения, составляющие государственную тайну;

б) шифровальных (криптографических) средств, являющихся компонентами доступных для продажи без ограничений посредством розничной торговли, либо сделок по почтовым запросам, либо электронных сделок, либо сделок по телефонным заказам программных операционных систем, криптографические возможности которых не могут быть изменены пользователями, которые разработаны для установки пользователем самостоятельно без дальнейшей существенной поддержки поставщиком и техническая документация (описание алгоритмов криптографических преобразований, протоколы взаимодействия, описание интерфейсов и т.д.) на которые является доступной, в том числе для проверки (за исключением разработки, производства);

в) персональных кредитных карточек со встроенной микроЭВМ, криптографические возможности которых не могут быть изменены пользователями (за исключением разработки, производства);

г) портативных или мобильных радиотелефонов гражданского назначения (в том числе предназначенных для использования в коммерческих гражданских системах сотовой радиосвязи), которые не способны к сквозному шифрованию;

д) приёмной и передающей аппаратуры радиовещания, коммерческого телевидения или иной аппаратуры коммерческого типа для вещания на ограниченную аудиторию без шифрования цифрового сигнала, в которой шифрование ограничено функциями управления видео- или аудиоканалами;

е) специально разработанных и применяемых только для банковских и финансовых операций шифровальных (криптографических) средств в составе терминалов единичной продажи (банкоматов), криптографические возможности которых не могут быть изменены пользователями;

ж) специально разработанных и применяемых только в составе контрольно-кассовых машин шифровальных (криптографических) средств защиты фискальной памяти (за исключением разработки, производства);

з) шифровальных (криптографических) средств независимо от их назначения, реализующих симметричные криптографические алгоритмы и обладающих максимальной длиной криптографического ключа менее 56 бит, а также реализующих асимметричные криптографические алгоритмы, основанные либо на разложении на множители целых чисел, либо на вычислении дискретных логарифмов в мультипликативной группе конечного поля, либо на дискретном логарифме в группе, отличной от названной, и обладающих максимальной длиной криптографического ключа 128 бит;

и) беспроводного оборудования, осуществляющего шифрование информации только в радиоканале с максимальной дальностью беспроводного действия без усиления и ретрансляции менее 400 м в соответствии с техническими условиями производителя (за исключением оборудования, используемого на критически важных объектах);

к) шифровальных (криптографических) средств, используемых для защиты технологических каналов информационно-телекоммуникационных систем и сетей, не относящихся к критически важным объектам.

Лицензионными требованиями и условиями при распространении шифровальных (криптографических) средств являются:

а) наличие у соискателя лицензии (лицензиата) на праве собственности или на ином законном основании помещений, технологического, испытательного, контрольно-измерительного оборудования, иных объектов и сооружений, необходимых для осуществления лицензируемой деятельности;

б) наличие в штате у соискателя лицензии (лицензиата) следующего квалифицированного персонала:

- руководитель и (или) лицо, уполномоченное руководить работами по лицензируемой деятельности, имеющие высшее профессиональное образование и (или) профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области не менее 5 лет;
- инженерно-технические работники, имеющие высшее профессиональное образование или прошедшие переподготовку (повышение квалификации) в области информационной безопасности с получением специализации, необходимой для работы с шифровальными (криптографическими) средствами;

в) выполнение соискателем лицензии (лицензиатом) при осуществлении лицензируемой деятельности требований, устанавливаемых в соответствии со статьями 11.2 и 13 Федерального закона «О федеральной службе безопасности»;

г) представление соискателем лицензии (лицензиатом) в лицензирующий орган перечня шифровальных (криптографических) средств, в том числе иностранного производства, не имеющих сертификата Федеральной службы безопасности Российской Федерации или Федерального агентства правительственной связи и информации при Президенте Российской Федерации, технической документации, определяющей состав, характеристики и условия эксплуатации этих средств, и (или) образцов шифровальных (криптографических) средств;

д) использование соискателем лицензии (лицензиатом) программ для электронно-вычислительных машин и баз данных на основании договора, заключённого с правообладателем, в соответствии со статьей 14 Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных».

При осуществлении деятельности по техническому обслуживанию в дополнение к вышеперечисленным лицензионным требованиям и условиям добавляются:

- реализация криптографических алгоритмов, рекомендованных лицензирующим органом, в разрабатываемых шифровальных (криптографических) средствах, применяемых в информацион-

но-телекоммуникационных системах и сетях критически важных объектов, федеральных органов исполнительной власти, органов исполни тельной власти субъектов Российской Федерации, органов местного самоуправления и организаций, осуществляющих выполнение работ или оказание услуг с использованием шифровальных (криптографических) средств для государственных и муниципальных нужд;

- применение лицензиатом средств обработки информации, аттестованных в соответствии с требованиями по защите информации.

При предоставлении услуг в области шифрования информации в дополнение к вышеперечисленным лицензионным требованиям и условиям добавляются:

- ведение лицензиатом учета изготовления, выдачи, возврата и уничтожения ключевых документов;
- обеспечение лицензиатом уничтожения исходной ключевой информации путем физического уничтожения носителя, на котором она расположена, или путем стирания (разрушения) исходной ключевой информации без повреждения носителя (для обеспечения возможности его многократного использования) в соответствии с эксплуатационной и технической документацией к соответствующим шифровальным (криптографическим) средствам, а также с указаниями организации, производившей запись исходной ключевой информации;
- использование лицензиатом шифровальных (криптографических) средств иностранного производства при условии, что эти средства были ввезены на территорию Российской Федерации и распространялись в порядке, установленном нормативными правовыми актами Российской Федерации.

Лицензионными требованиями и условиями при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем, являются:

а) наличие у соискателя лицензии (лицензиата) на правах собственности или на ином законном основании помещений, технологического, испытательного, контрольно-измерительного оборудования, иных объектов и сооружений, необходимых дня осуществления лицензируемой деятельности;

б) наличие в штате у соискателя лицензии (лицензиата) следующего квалифицированного персонала:

- руководитель и (или) лицо, уполномоченное руководить работами по лицензируемой деятельности, имеющие высшее профессиональное образование и (или) профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области не менее 5 лет;

- инженерно-технические работники, имеющие высшее профессиональное образование или прошедшие переподготовку (повышение квалификации) в области информационной безопасности с получением специализации, необходимой для работы с шифровальными (криптографическими) средствами, а также стаж работы в этой области не менее 2 лет;

в) наличие у соискателя лицензии (лицензиата) допуска к проведению работ, связанных с использованием сведений, составляющих государственную тайну (только при разработке шифровальных (криптографических) средств);

г) выполнение соискателем лицензии (лицензиатом) при осуществлении лицензируемой деятельности требований и условий, устанавливаемых в соответствии со статьями 11.2 и 13 Федерального закона «О федеральной службе безопасности»;

д) реализация криптографических алгоритмов, рекомендованных лицензирующим органом, в разрабатываемых шифровальных (криптографических) средствах, применяемых в информационно-телекоммуникационных системах и сетях критически важных объектов, федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления и организаций, осуществляющих выполнение работ или оказание услуг с использованием шифровальных (криптографических) средств для государственных и муниципальных нужд;

е) обеспечение соискателем лицензии (лицензиатом) контролируемого доступа персонала к конфиденциальной информации и (или) работам с шифровальными (криптографическими) средствами, а также сохранности конфиденциальной информации и шифровальных (криптографических) средств, используемых при осуществлении лицензируемой деятельности;

ж) применение лицензиатом средств обработки информации, аттестованных в соответствии с требованиями по защите информации;

з) использование соискателем лицензии (лицензиатом) программ для электронно-вычислительных машин и баз данных на основании договора, заключенного с правообладателем в соответствии

со статьёй 14 Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных».

1.11 Сертификация средств защиты и аттестация объектов информатизации

Согласно Закону Российской Федерации «О государственной тайне» средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Кроме того, в соответствии с «Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам» (постановление Совета Министров – Правительства Российской Федерации от 15.09.1993 №912-51) информация, содержащая сведения, отнесённые к государственной или служебной тайне, должна обрабатываться с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств защиты, ***сертифицированных*** в установленном порядке. Для оценки готовности систем и средств информатизации и связи к обработке (передаче) информации, содержащей сведения, отнесённые к государственной или служебной тайне, проводится ***аттестование*** указанных систем и средств в реальных условиях эксплуатации на предмет соответствия принимаемых методов, мер и средств защиты требуемому уровню безопасности информации.

Также следует отметить, что согласно требованиям «Положения о лицензировании деятельности по технической защите конфиденциальной информации» (постановление Правительства Российской Федерации от 15.08.2006 № 504) допускается использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру ***оценки соответствия*** (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации. Кроме того, в положениях о лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств, предоставления услуг в области шифрования информации и разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем (постановление Правительства Российской Федерации от 29.12.2007 № 957) предписано применение лицензиатом средств обработки информа-

ции, ***аттестованных*** в соответствии с требованиями по защите информации. Невыполнение данных требований является грубым нарушением лицензионных требований и условий.

В «Положении об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (постановление Правительства Российской Федерации от 17.11.2007 № 781) сказано, что средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру ***оценки соответствия.***

В Указе Президента Российской Федерации от 17.03.2008 № 351 сказано, что:

- при необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке ***сертификацию*** в Федеральной службе безопасности Российской Федерации и (или) получивших ***подтверждение соответствия*** в Федеральной службе по техническому и экспортному контролю;
- государственные органы в целях защиты общедоступной информации, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, используют только средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке ***сертификацию*** в Федеральной службе безопасности Российской Федерации и (или) получившие ***подтверждение соответствия*** в Федеральной службе по техническому и экспортному контролю;
- размещение технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, осуществляется только при наличии ***сертификата,*** разрешающего эксплуатацию таких технических средств в указанных помещениях.

В постановлении Правительства Российской Федерации от 18.05.2009 № 424 сказано, что операторы федеральных государственных информационных систем, созданных или используемых в целях реализации полномочий федеральных органов исполнительной власти и содержащих сведения, указанные в перечне сведений о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательных для размещения в информационно- телекоммуникационной сети Интернет, утверждённом постановлением Правительства Российской Федерации от 12 февраля 2003 г. № 98 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» (далее – информационные системы общего пользования), при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям, доступ к которым не ограничен определённым кругом лиц, обязаны обеспечить использование при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям средств защиты информации, прошедших ***оценку соответствия*** (в том числе в установленных случаях ***сертификацию***), в порядке, установленном законодательством Российской Федерации.

В постановлении Правительства Российской Федерации от 15.05.2010 № 330 сказано, что аккредитация органа по сертификации и испытательной лаборатории (центра), выполняющих работы по подтверждению соответствия продукции (работ, услуг), указанной в пункте 2 настоящего постановления, осуществляется органом по аккредитации в установленном законодательством Российской Федерации порядке при условии наличия у органа по сертификации и испытательной лаборатории (центра): автоматизированных систем, обрабатывающих информацию ограниченного доступа, а также средств её защиты, прошедших процедуру ***оценки соответствия (аттестованных*** и (или) ***сертифицированных*** по требованиям безопасности информации) в соответствии с законодательством Российской Федерации.

В остальных случаях сертификация и аттестация носят добровольный характер *(добровольная сертификация и аттестация)* и может осуществляться по инициативе заказчика или владельца объекта информатизации.

В Федеральном законе от 27.12.2002 № 184-ФЗ **«О техническом регулировании»** даны следующие определения:

- ***оценка соответствия*** – прямое или косвенное определение соблюдения требований, предъявляемых к объекту;

- ***подтверждение соответствия*** – документальное удостоверение соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;
- ***сертификация*** – форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;
- ***декларирование соответствия*** – форма подтверждения соответствия продукции требованиям технических регламентов;
- ***технический регламент*** – документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или межправительственным соглашением, заключённым в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации, или нормативным правовым актом федерального органа исполнительной власти по техническому регулированию и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям или к связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации);
- ***форма подтверждения соответствия*** – определённый порядок документального удостоверения соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов или условиям договоров;
- ***схема подтверждения соответствия*** – перечень действий участников подтверждения соответствия, результаты которых рассматриваются ими в качестве доказательств соответствия продукции и иных объектов установленным требованиям.

Подтверждение соответствия осуществляется в целях:

- удостоверения соответствия продукции, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, работ, услуг или иных объектов техническим регламентам, стандартам, сводам правил, условиям договоров;
- содействия приобретателям в компетентном выборе продукции, работ, услуг;
- повышения конкурентоспособности продукции, работ, услуг на российском и международном рынках;
- создания условий для обеспечения свободного перемещения товаров по территории Российской Федерации, а также для осуществления международного экономического, научно-технического сотрудничества и международной торговли.

Подтверждение соответствия осуществляется на основе принципов:

- доступности информации о порядке осуществления подтверждения соответствия заинтересованным лицам;
- недопустимости применения обязательного подтверждения соответствия к объектам, в отношении которых не установлены требования технических регламентов;
- установления перечня форм и схем обязательного подтверждения соответствия в отношении определённых видов продукции в соответствующем техническом регламенте;
- уменьшения сроков осуществления обязательного подтверждения соответствия и затрат заявителя;
- недопустимости принуждения к осуществлению добровольного подтверждения соответствия, в том числе в определённой системе добровольной сертификации;
- защиты имущественных интересов заявителей, соблюдения коммерческой тайны в отношении сведений, полученных при осуществлении подтверждения соответствия;
- недопустимости подмены обязательного подтверждения соответствия добровольной сертификацией.

Подтверждение соответствия разрабатывается и применяется равным образом и в равной мере независимо от страны и (или) места происхождения продукции, осуществления процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ и оказания услуг, видов или особенностей сделок и (или) лиц, которые являются изготовителями, исполнителями, продавцами, приобретателями.

Подтверждение соответствия на территории Российской Федерации может носить добровольный или обязательный характер. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации. Обязательное подтверждение соответствия осуществляется в формах:

- принятия декларации о соответствии (далее – декларирование соответствия);
- обязательной сертификации.

Порядок применения форм обязательного подтверждения соответствия устанавливается Федеральным законом «О техническом регулировании».

В отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа; продукции (работ, услуг), сведения о которой составляют государственную тайну; продукции (работ, услуг) и объектов, для которых устанавливаются требования, связанные с обеспечением ядерной и радиационной безопасности в области использования атомной энергии; процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации, захоронения соответственно указанной продукции и указанных объектов обязательными требованиями, наряду с требованиями технических регламентов, являются требования, установленные государственными заказчиками, федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации, государственного управления использованием атомной энергии, государственного регулирования безопасности при использовании атомной энергии, и (или) государственными контрактами (договорами). Особенности оценки соответствия указанной продукции (работ, услуг) и объектов, а также соответственно процессов их проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации, захоронения устанавливаются Правительством Российской Федерации.

Технический регламент должен содержать перечень и (или) описание объектов технического регулирования, требования к этим объектам и правила их идентификации в целях применения технического регламента. Технический регламент должен содержать правила и формы оценки соответствия (в том числе в техническом регламенте

могут содержаться схемы подтверждения соответствия, порядок продления срока действия выданного сертификата соответствия), определяемые с учетом степени риска, предельные сроки оценки соответствия в отношении каждого объекта технического регулирования и (или) требования к терминологии, упаковке, маркировке или этикеткам и правилам их нанесения. Технический регламент должен содержать требования энергетической эффективности.

Оценка соответствия проводится в формах:

- государственного контроля (надзора);
- аккредитации;
- испытания;
- регистрации;
- подтверждения соответствия;
- приёмки и ввода в эксплуатацию объекта, строительство которого закончено;
- и в иной форме.

Не включённые в технические регламенты требования к продукции или к связанным с ними процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, правилам и формам оценки соответствия, правила идентификации, требования к терминологии, упаковке, маркировке или этикеткам и правилам их нанесения не могут носить обязательный характер.

Обязательное подтверждение соответствия проводится только в случаях, установленных соответствующим техническим регламентом, и исключительно на соответствие требованиям технического регламента. Объектом обязательного подтверждения соответствия может быть только продукция, выпускаемая в обращение на территории Российской Федерации.

Форма и схемы обязательного подтверждения соответствия могут устанавливаться только техническим регламентом с учётом степени риска недостижения целей технических регламентов.

Декларация о соответствии и сертификат соответствия имеют равную юридическую силу и действуют на всей территории Российской Федерации в отношении каждой единицы продукции, выпускаемой в обращение на территории Российской Федерации во время действия декларации о соответствии или сертификата соответствия, в течение срока годности или срока службы продукции, установленных в соответствии с законодательством Российской Федерации.

Работы по обязательному подтверждению соответствия подлежат оплате на основании договора с заявителем. Стоимость работ по

обязательному подтверждению соответствия продукции определяется независимо от страны и (или) места её происхождения, а также лиц, которые являются заявителями.

Декларирование соответствия осуществляется по одной из следующих схем:

- принятие декларации о соответствии на основании собственных доказательств;
- принятие декларации о соответствии на основании собственных доказательств, доказательств, полученных с участием органа по сертификации и (или) аккредитованной испытательной лаборатории (центра) (далее – третья сторона).

При декларировании соответствия заявителем может быть зарегистрированное в соответствии с законодательством Российской Федерации на её территории юридическое лицо или физическое лицо в качестве индивидуального предпринимателя, либо являющиеся изготовителем или продавцом, либо выполняющие функции иностранного изготовителя на основании договора с ним в части обеспечения соответствия поставляемой продукции требованиям технических регламентов и в части ответственности за несоответствие поставляемой продукции требованиям технических регламентов (лицо, выполняющее функции иностранного изготовителя). Круг заявителей устанавливается соответствующим техническим регламентом. Схема декларирования соответствия с участием третьей стороны устанавливается в техническом регламенте в случае, если отсутствие третьей стороны приводит к недостижению целей подтверждения соответствия.

При декларировании соответствия на основании собственных доказательств заявитель самостоятельно формирует доказательственные материалы в целях подтверждения соответствия продукции требованиям технических регламентов. В качестве доказательственных материалов используются техническая документация, результаты собственных исследований (испытаний) и измерений и (или) другие документы, послужившие мотивированным основанием для подтверждения соответствия продукции требованиям технических регламентов. Состав доказательственных материалов определяется соответствующим техническим регламентом.

При декларировании соответствия на основании собственных доказательств и полученных с участием третьей стороны доказательств заявитель по своему выбору в дополнение к собственным доказательствам:

- включает в доказательственные материалы протоколы исследований (испытаний) и измерений, проведённых в аккредитованной испытательной лаборатории (центре);
- предоставляет сертификат системы качества, в отношении которого предусматривается контроль (надзор) органа по сертификации, выдавшего данный сертификат, за объектом сертификации.

Сертификат системы качества может использоваться в составе доказательств при принятии декларации о соответствии любой продукции, за исключением случая, если для такой продукции техническими регламентами предусмотрена иная форма подтверждения соответствия.

Декларация о соответствии оформляется на русском языке и должна содержать:
- наименование и местонахождение заявителя;
- наименование и местонахождение изготовителя;
- информацию об объекте подтверждения соответствия, позволяющую идентифицировать этот объект,
- наименование технического регламента, на соответствие требованиям которого подтверждается продукция;
- указание на схему декларирования соответствия;
- заявление о безопасности продукции при её использовании в соответствии с целевым назначением и принятии заявителем мер по течению соответствия продукции требованиям технических регламентов;
- сведения о проведённых исследованиях (испытаниях) и измерениях, сертификате системы качества, а также документах, послуживших основанием для подтверждения соответствия продукции требованиям технических регламентов;
- срок действия декларации о соответствии;
- иные предусмотренные соответствующими техническими регламентами сведения.

Срок действия декларации о соответствии определяется техническим регламентом. Форма декларации о соответствии утверждается федеральным органом исполнительной власти по техническому регулированию.

Оформленная заявителем декларация о соответствии подлежит регистрации в едином реестре деклараций о соответствии в течение трех дней. Порядок формирования и ведения единого реестра деклараций о соответствии, порядок регистрации деклараций о соответствии, предоставления содержащихся в указанном реестре сведений

определяются уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

Обязательная сертификация осуществляется органом по сертификации на основании договора с заявителем. Схемы сертификации, применяемые для сертификации определённых видов продукции, устанавливаются соответствующим техническим регламентом.

Соответствие продукции требованиям технических регламентов подтверждается сертификатом соответствия, выдаваемым заявителю органом по сертификации. Сертификат соответствия включает в себя:

- наименование и местонахождение заявителя;
- наименование и местонахождение изготовителя продукции, прошедшей сертификацию;
- наименование и местонахождение органа по сертификации, выдавшего сертификат соответствия;
- информацию об объекте сертификации, позволяющую идентифицировать этот объект,
- наименование технического регламента, на соответствие требованиям которого проводилась сертификация;
- информацию о проведённых исследованиях (испытаниях) и измерениях;
- информацию о документах, представленных заявителем в орган по сертификации в качестве доказательств соответствия продукции требованиям технических регламентов;
- срок действия сертификата соответствия.

Срок действия сертификата соответствия определяется соответствующим техническим регламентом. Форма сертификата соответствия утверждается федеральным органом исполнительной власти по техническому регулированию.

Обязательная сертификация осуществляется органом по сертификации, аккредитованным в порядке, установленном Правительством Российской Федерации.

В соответствии с действующим законодательством обязательная сертификация проводится в рамках систем сертификации средств защиты информации, созданных федеральными органами исполнительной власти, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определённой для них законодательными и иными нормативными правовыми актами Российской Федерации. В качестве таких нормативных правовых актов следует отметить:

- Постановление Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации»;

- Постановление Правительства Российской Федерации от 21.04.2010 № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов её проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в Положение о сертификации средств защиты информации»;

- Постановление Правительства Российской Федерации от 15.05.2010 № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов её проектирования (включая изыскании), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг)».

Конкретные средства и меры защиты информации должны разрабатываться и применяться в зависимости от уровня конфиденциальности и ценности информации, а также от уровня возможного ущерба в случае её утечки, уничтожения, модификации или блокирования.

1.12 Основные нормативные документы по вопросам обеспечения безопасности информации

Необходимой составляющей государственной системы обеспечения информационной безопасности являются национальные (го-

сударственные стандарты) и другие руководящие, нормативно-технические и методические документы по безопасности информации, утверждённые федеральными органами исполнительной власти в соответствии с их компетенцией и определяющие нормы защищённости информации и требования в различных направлениях защиты информации.

К основным стандартам и руководящим документам по вопросам обеспечения безопасности информации, в соответствии с требованиями которых осуществляется сертификация продукции и аттестация объектов информатизации по требованиям безопасности информации, сертификация средств криптографической защиты информации, относятся:

в области защиты информации от несанкционированного доступа:

- ГОСТ Р 50922-96. Защита информации. Основные термины и определения;
- ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
- ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения;

руководящие документы Гостехкомиссии России (ФСТЭК России):

- Защита от несанкционированного доступа к информации. Термины и определения;
- Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;
- Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации;
- Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации;
- Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;

- Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации;
- Защита информации. Специальные защитные знаки. Классификация и общие требования;
- Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин автоматизированных кассовых систем и требования по защите информации;
- Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей;
- Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Часть 1, Часть 2, Часть 3);
- и другие;

в области защиты информации от утечки по техническим каналам:

- ГОСТ Р В50170-2005. Противодействие иностранной технической разведке. Термины и определения;
- ГОСТ Р 50752-95. Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний;
- ГОСТ 29339-92. Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Общие технические требования;
- ГОСТ 30373-95/ГОСТ 50414-92. Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний;

нормативно-методические документы ФСТЭК России:

- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К);
- Методические рекомендации по технической защите информации, составляющей коммерческую тайну;

- Временная методика оценки защищённости помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам;
- Временная методика оценки защищённости ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации;
- Временная методика оценки защищённости конфиденциальной информации, обрабатываемой ОТСС, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации;
- Временная методика оценки защищённости помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований;
- и другие;

в области криптографического преобразования информации при ее хранении и передаче по каналам связи:

- ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования;
- ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи;
- ГОСТ Р 34.11-94. Функция хеширования;

документы ФСБ России:

- Положение о разработке, изготовлении и обеспечении эксплуатации шифровальной техники, систем связи и комплексов вооружения, использующих шифровальную технику (ПШ-93);
- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005);
- Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну;
- и другие.

1.13 Сертификация средств защиты информации

Остановимся более детально на вопросах сертификации средств защиты. Следует отметить, что после передачи лицензирующих

подразделений ФАПСИ в ведение ФСБ России основные принципы системы лицензирования и сертификации не изменились. Все ранее выданные ФАПСИ лицензии и сертификаты оставались действительными на обозначенный в них срок.

Под ***сертификацией*** средств защиты информации по требованиям безопасности информации понимается деятельность по подтверждению их соответствия требованиям государственных стандартов или иных нормативных документов по защите информации, утверждённых уполномоченными федеральными органами исполнительной власти в пределах их компетенции.

Сертификат соответствия – документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Знак соответствия – зарегистрированный в установленном порядке знак, которым по правилам, установленным в данной системе сертификации, подтверждается соответствие маркированной им продукции установленным требованиям.

Средства защиты информации (СЗИ) – технические, криптографические, программные и другие средства, предназначенные для защиты сведений конфиденциального характера, а также средства контроля эффективности защиты информации.

Руководящий документ ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости средств вычислительной техники» устанавливает классификацию средств вычислительной техники по уровню защищённости от несанкционированного доступа к информации на базе перечня показателей защищённости и совокупности описывающих их требований.

В соответствии с этим руководящим документом возможные показатели защищённости исчерпываются 7 классами. По классу защищённости можно судить о номенклатуре используемых механизмов защиты. Наиболее защищённым является 1-й класс. Выбор класса защищённости зависит от секретности обрабатываемой информации, условий эксплуатации и расположения объектов системы (рис. 1.2). В частности, для защиты конфиденциальной информации (персональных данных, служебной тайны и др.) можно применять средства защиты 5-го и 6-го класса.

Другим важным руководящим документом ФСТЭК России является «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Класси-

фикация по уровню контроля отсутствия недекларированных возможностей», который устанавливает классификацию программного обеспечения (отечественного и импортного производства) средств защиты информации по уровню контроля отсутствия в нем недекларированных возможностей (см. рис. 1.3).

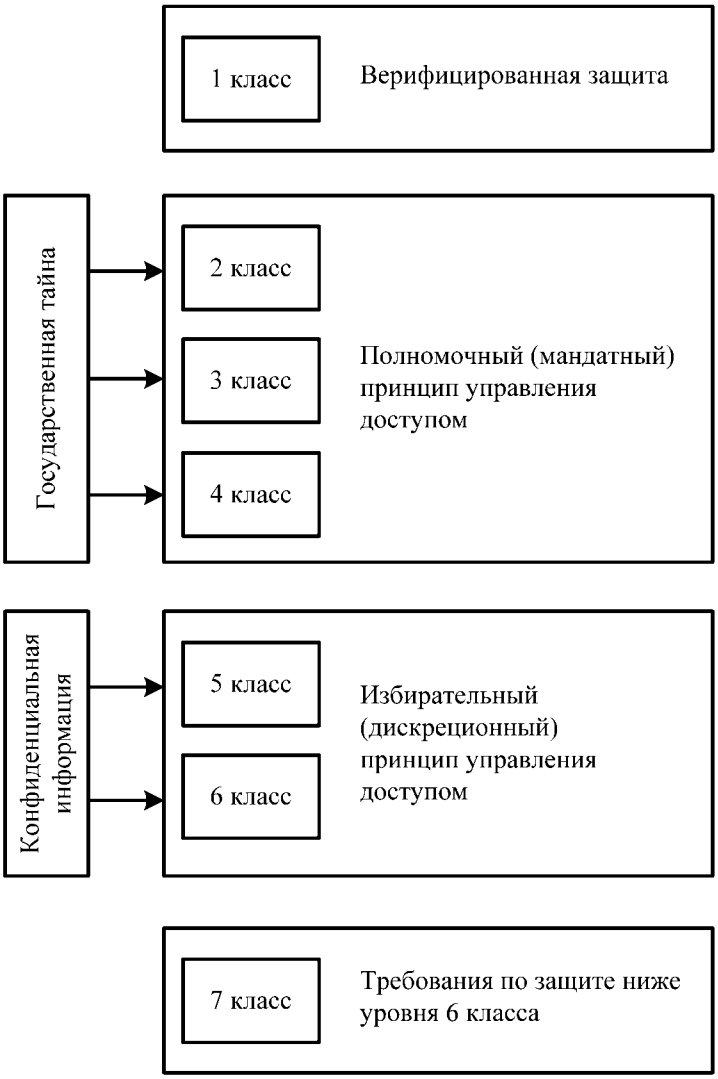

Рис. 1.2. Показатели защищённости СВТ

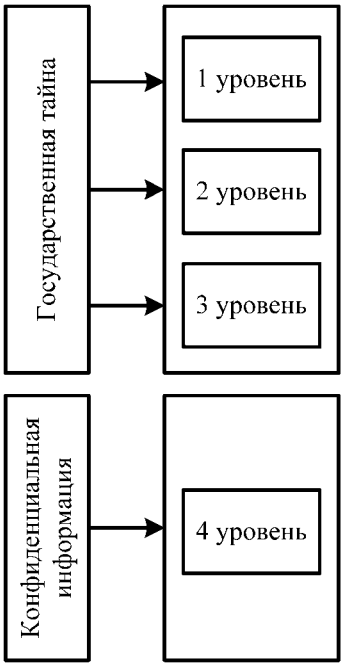

Рис. 1.3. Классификация по уровню контроля отсутствия недекларированных возможностей

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

Также следует отметить руководящий документ ФСТЭК России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации», который устанавливает классификацию межсетевых экранов (МЭ) по уровню защищённости от несанкционированного доступа к информации на базе перечня показателей защищённости и совокупности описывающих их требований (рис. 1.4).

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивающее защиту АС посредством фильтрации информации,

т.е. её анализа по совокупности критериев и принятия решения о её распространении в (из) АС.

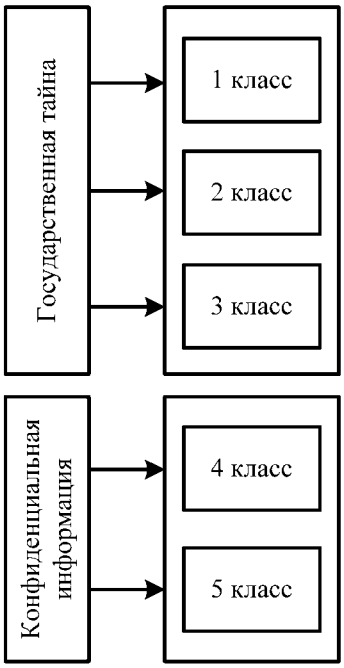

Рис. 1.4. Классификация МЭ по уровню защищённости от НСД

1.14 Аттестация объектов информатизации

При проведении работ со сведениями соответствующей степени конфиденциальности (секретности) системы информатизации должны (могут) быть *аттестованы* на соответствие требованиям по безопасности информации.

Государственная система аттестации объектов информатизации устанавливает основные принципы, организационную структуру, порядок проведения аттестации, а также порядок контроля и надзора за эксплуатацией аттестованных объектов информатизации.

Под ***объектами информатизации***, аттестуемыми по требованиям безопасности информации, понимаются автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, под-

лежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.

Система аттестации объектов информатизации по требованиям безопасности информации является составной частью единой государственной системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Деятельность системы аттестации организуют уполномоченные федеральные органы по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации.

Под ***аттестацией*** объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – ***«Аттестата соответствия»*** подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утверждённых уполномоченными федеральными органами исполнительной власти. Наличие на объекте информатизации действующего «Аттестата соответствия» даёт право обработки информации с определённым уровнем конфиденциальности и в указанный в «Аттестате соответствия» период времени.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счёт побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счёт специальных устройств, встроенных в объекты информатизации.

Аттестация проводится уполномоченными органами по аттестации объектов информатизации, аккредитованными федеральными органами исполнительной власти. Правила аккредитации определяются действующими в соответствующих системах сертификации положениями. В системе сертификации ФСТЭК России разработано и утверждено 25 ноября 1994 г. «Положением об аккредитации органов по аттестации объектов информатизации по требованиям безопасности информации». Каждый такой орган имеет лицензию на право выполнения работ в области защиты информации и Аттестат аккредитации. Виды работ, которые он может выполнять, указываются в области аккредитации, являющейся приложением к Аттестату аккредитации. В своей деятельности органы по аттестации руководствуются нормативно-методическими документами ФСТЭК России.

Аттестат соответствия утверждается руководителем органа по аттестации объектов информатизации, который и несёт юридическую и финансовую ответственность за качество проведённых работ. Кроме того, органы по аттестации несут ответственность за обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонент.

Аттестация информационных систем может производиться в соответствии с Руководящим документом ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», который вводит в рассмотрение 9 классов защищённости АС, объединённых в три группы (рис. 1.5).

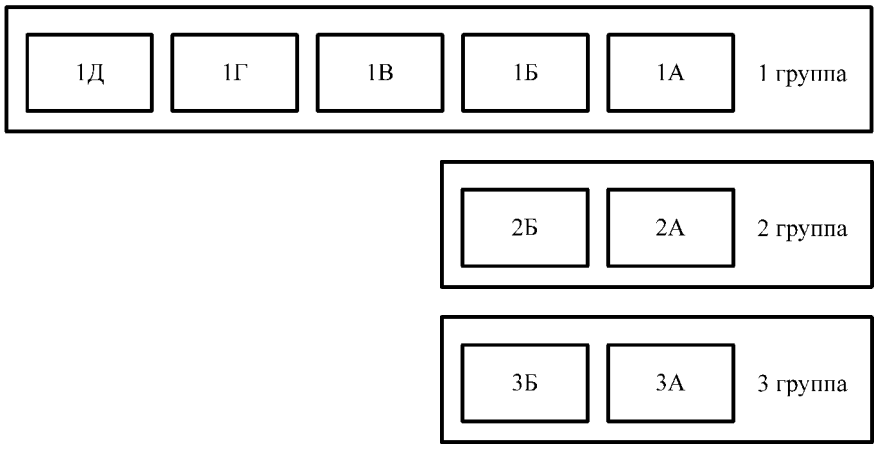

Рис. 1.5. Классы защищённости АС

Основные признаки группировки в различные классы связаны с:

- наличием в АС информации различного уровня конфиденциальности;
- уровнем полномочий субъектов доступа АС на доступ к конфиденциальной информации (одинаковый или разный);
- режимом обработки данных в АС (коллективный или индивидуальный).

Для каждого класса сформулирован определённый набор требований для подсистем:

- управления доступом;
- регистрации и учета;

- криптографической;
- обеспечения целостности.

Группа 1 классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов: **1Д, 1Г, IB, 1Б и 1А.**

Группа 2 классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса: **2Б и 2А.**

Группа 3 классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размanённой на носителях одного уровня конфиденциальности. Группа содержит два класса: **3Б и 3А.**

Соответствие классов защищённости различным уровням конфиденциальности приведено на рис. 1.6.

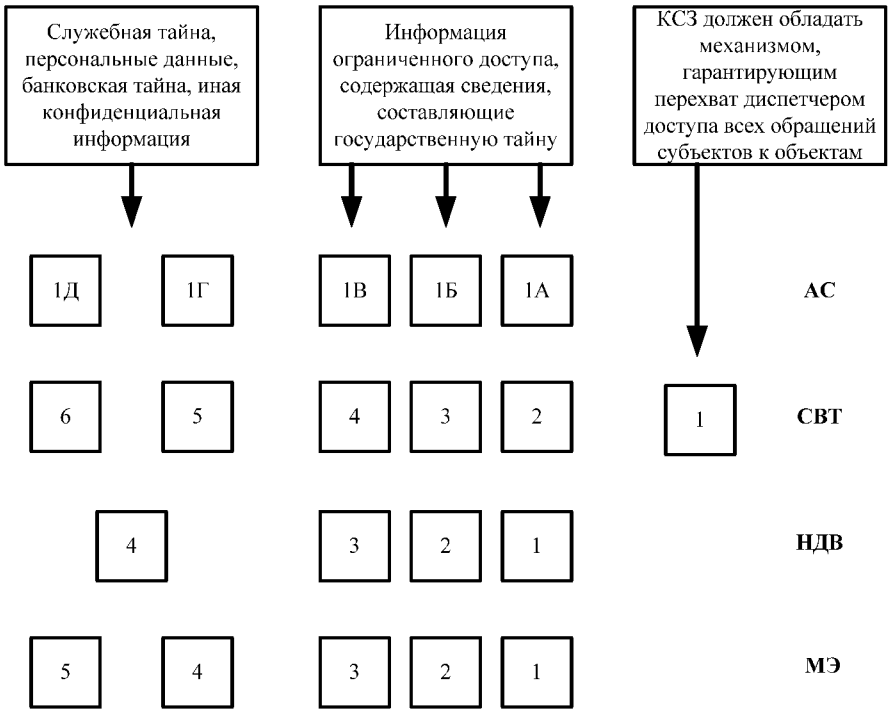

Рис. 1.6. Классы защищённости АС и категории информации ограниченного доступа

1.15 Новое поколение нормативно-технических документов (ГОСТ Р ИСО/МЭК 15408-2008)

До 2002 г. единственными нормативными документами по критериям оценки защищённости средств вычислительной техники и автоматизированных систем являлись рассмотренные выше руководящие документы ФСТЭК России.

Качественно новым этапом в развитии нормативной базы оценки безопасности ИТ послужило начало разработки и апробация (во исполнение решений Совета безопасности Российской Федерации от 26.03.2002 № 1.2 и Коллегии Гостехкомиссии России от 30.05.2002 № 9.2) нового поколения нормативных документов в системе сертификации ФСТЭК России на основе методологии ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», который содержал полный аутентичный текст Международного стандарта ISO/TEC 15408:1999 «Information Technology. Security techniques. Evaluation criteria for ГГ security», так называемые «Общие критерии».

Ещё начиная с 70-х годов службами безопасности США проводились исследования в области формальных методов оценки безопасности, связанной с использованием ИТ. Позднее, в 90-х, эта деятельность привела к разработке набора критериев TCSEC (Trusted Computer System Evaluation Criteria), более известного как «Оранжевая книга», а также «Федеральных критериев безопасности информационных технологий». Аналогичные критерии были разработаны и в других странах: «Гармонизированные критерии европейских стран» (Information Technology Security Evaluation Criteria), «Канадские критерии оценки безопасности компьютерных продуктов» и т. д.

Понимая, что национальные критерии будут препятствовать широкому распространению продуктов в области ИТ-безопасности, в 1990 году под эгидой ISO были начаты работы по унификации национальных стандартов. В 1993 году организации США, Канады, Великобритании, Франции, Германии и Нидерландов [Национальный институт стандартов и технологии, Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство национальной безопасности коммуникаций (Нидерланды), Органы исполнения Программы безопасности и сертификации ИТ (Великобритания), Центр обеспечения безопасности систем (Франция)] объединили свои усилия в рамках проекта, получившего название «Об-

щие критерии оценки безопасности информационных технологий» (Common Criteria for Information Technology Security Evaluation).

Разработка версии 1.0 «Общих критериев...» была завершена в январе 1996 года и одобрена международной организацией по стандартизации (ISO) уже в апреле 1996 года. Появление международного стандарта явилось новым этапом в развитии нормативной базы оценки информационной безопасности. Новые критерии обеспечили взаимное признание результатов стандартизованной оценки безопасности на мировом рынке ИТ. «Общие критерии...» обобщили содержание и опыт использования «Оранжевой книги», развили оценочные уровни доверия «Европейских критериев...», воплотили в реальные структуры концепцию типовых профилей защиты «Федеральных критериев...». В «Общих критериях...» проведена классификация широкого набора функциональных требований и требований доверия к безопасности, определены способы их группирования и принципы использования.

В мае 1998 года была опубликована версия 2.0 «Общих критериев...» и на её основе в июне 1999 года был принят международный стандарт ISO/1EC 15408:1999 (Information technology — Security techniques — Evaluation criteria for П security).

Практически одновременно с «Общими критериями...» разрабатывались версии «Общей методологии оценки безопасности информационных технологий». В августе 1999 года опубликована версия 1.0 «Общей методологии оценки…» (часть 2) для оценочных уровней доверия (ОУД) 1-4. В январе 2004 года опубликованы версии 2.2, а в августе 2005 г. – версии 2.3 «Общих критериев...» и «Общей методологии оценки..». Именно они легли в основу стандартов ISO/IEC 15408:2005 и ISO/IEC 18045:2005 (Information technology — Security techniques — Methodology for IT security evaluation) соответственно.

В июле 2005 года опубликованы новые версии 3.0 «Общих критериев...» и «Общей методологии оценки…», в которых предыдущие версии подверглись существенной ревизии. Однако, как показало обсуждение этих версий в международном сообществе, далеко не все предложенные авторами изменения были целесообразны и корректны. В результате, в сентябре 2006 года появились версии 3.1 «Общих критериев...» и «Общей методологии оценки…», которые и были признаны официальными. Именно эти версии с определёнными доработками легли в основу уже третьей и на данный момент последней версии стандарта КОЛЕС 15408, части которого вышли в 2008 и 2009 годах.

Надо сказать, что Россия достаточно сильно отставала от этого движения. Только в 2002 году постановлением Госстандарта России году был принят ГОСТ Р ИСО/МЭК 15408-2002, содержащий полный аутентичный текст международного стандарта КОЛЕС] 5408:1999 (введён в действие с 1 января 2004 года). Вскоре была принята вторая редакция стандарта – ГОСТ Р ИСО/МЭК 15408-2008, содержащая полный текст международного стандарта ISO/IEC 15408:2005. Однако, как уже было сказано, с 2005 по 2008 годы международный стандарт подвергся серьёзным переработкам, которые не нашли своего отражения в действующей в России версии документа.

Главная тенденция, которая прослеживается на протяжении целого ряда стандартов в области информационной безопасности – отказ от жёсткой универсальной шкалы классов безопасности и обеспечение гибкости в подходе к оценке безопасности различных типов ИТ-продуктов. Именно это стремление объясняет столь сложную на первый взгляд логическую структуру стандарта ISO/IEC 15408.

Если говорить кратко, то принципиальные черты стандарта следующие:

- чёткое разделение требований безопасности на функциональные требования и требования доверия к безопасности. Функциональные требования относятся к функциям безопасности (идентификация, аутентификация, управление доступом, аудит и т. д.), а требования доверия – к технологии разработки, тестированию, анализу уязвимостей, поставке, сопровождению, эксплуатационной документации, то есть ко всем этапам жизненного цикла изделий информационных технологий;
- систематизация и классификация требований к безопасности в рамках иерархии «класс» – «семейство» – «компонент» – «элемент»;
- ранжирование компонентов требований в семействах и классах по степени полноты и жёсткости, а также их группирование в пакеты функциональных требований и Уровни Оценки Доверия;
- гибкость и динамизм в подходе к заданию требований безопасности для различных типов изделий информационных технологий и условий их применения, обеспечиваемые путём целенаправленного формирования необходимых наборов требований в виде определённых структур (Профилей Защиты и Целевых Уровней Безопасности);
- понимание методологии является залогом эффективного использования того огромного фактического материала по требованиям безопасности ИТ, порядку их задания и оценке, который содержится в данном стандарте.

Общие критерии разработаны таким образом, чтобы удовлетворить потребности трёх групп специалистов: разработчиков, оценщиков и пользователей объекта оценки. Под объектом оценки (ОО) понимается аппаратно-программный продукт или информационная система. К таким объектам относятся, например, операционные системы, вычислительные сети, распределённые системы, прикладные программы.

К рассматриваемым в ОК аспектам безопасности относятся: защита от несанкционированного доступа, модификации или потери доступа к информации при воздействии угроз, являющихся результатом случайных или преднамеренных действий. Защищённость от этих трех типов угроз обычно называют конфиденциальностью, целостностью и доступностью.

Однако некоторые аспекты безопасности ИТ находятся вне рамок Общих критериев:

- стандарт не содержит критериев оценки безопасности, касающихся административных мер, непосредственно не относящихся к мерам безопасности ИТ. Административные меры безопасности в среде эксплуатации ОО рассматриваются в качестве предположений о безопасном использовании;
- оценка физических аспектов безопасности ИТ, таких как контроль электромагнитного изучения, специально не рассматривается, хотя многие концепции ОК применимы и в этой области;
- в ОК не рассматривается ни методология оценки, ни нормативная и правовая база, на основе которой критерии могут применяться органами оценки;
- процедуры использования результатов оценки при аттестации продуктов и систем ИТ находятся вне области действия ОК. Аттестация продукта или системы ИТ является административным актом, посредством которого компетентный орган допускает их использование в конкретных условиях эксплуатации;
- критерии для оценки специфических качеств криптографических алгоритмов в ОК не входят.

Общие критерии предполагается использовать как при задании требований к продуктам и системам ИТ, так и при оценке их безопасности на всех этапах жизненного цикла. Стандарт ГОСТ Р ИСО/МЭК 15408-2008 не меняет сложившейся в России методологии защиты, однако по уровню систематизации, полноте и степени детализации требований, универсальности и гибкости значительно превосходит действующие в настоящее время руководящие документы.

В качестве основы для разработки нормативных документов по оценке безопасности информационных технологии был принят руководящий документ (РД) «Безопасность информационных технологий. Критерии опенки безопасности информационных технологий» (введён в действие с 1 августа 2002 г. приказом председателя Гостехкомиссии России от 19.06.2002 № 187), который и применяется при проведении сертификации средств защиты информации. Самым главным недостатком РД является то, что он не был разработан на основе старой редакции ОК и не учитывает всех тех изменений, которые были внесены в ISO/IEC 15408.

Основной целью РД является повышение доверия к безопасности продуктов и систем информационных технологий. Положения руководящего документа направлены на создание продуктов и систем информационных технологий с уровнем безопасности, адекватным имеющимся по отношению к ним угрозам и проводимой политике безопасности с учётом условий применения, что должно обеспечить оптимизацию продуктов и систем ИТ по критерию «эффективность •-стоимость».

Под безопасностью информационной технологии понимается состояние ИТ, определяющее защищённость информации и ресурсов ИТ от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность ИТ выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений.

Доверие к безопасности ИТ обеспечивается как реализацией в них необходимых функциональных возможностей, так и осуществлением комплекса мер по обеспечению безопасности при разработке продуктов и систем ИТ, проведением независимых оценок их безопасности и контролем её уровня при эксплуатации.

Требования к безопасности конкретных продуктов и систем ИТ устанавливаются исходя из имеющихся и прогнозируемых угроз безопасности, проводимой политики безопасности, а также с учётом условий их применения. При формировании требований должны в максимальной степени использоваться компоненты требований, представленные в настоящем руководящем документе. Допускается также использование и других требований безопасности, при этом уровень детализации и способ выражения требований, представленных в настоящем руководящем документе, должны использоваться в качестве образца. Требования безопасности могут задаваться Заказчиком в техническом задании на разработку продуктов и систем ИТ или формироваться Разработчиком при создании им продуктов ИТ самостоятельно.

Требования безопасности, являющиеся общими для некоторого типа продуктов или систем ИТ, могут оформляться в виде представленной в настоящем руководящем документе структуры, именуемой «Профиль защиты». Профили защиты, прошедшие оценку в установленном порядке, регистрируются и помещаются в каталог оцененных профилей защиты.

Оценка и сертификация безопасности ИТ проводится на соответствие требованиям, представляемым Разработчиком продукта или системы ИТ в Задании по безопасности. Требования заданий по безопасности продуктов и систем ИТ, предназначенных для использования в областях применения, регулируемых государством, должны соответствовать требованиям установленных профилей защиты.

Руководящий документ состоит из трёх частей.

Часть 1 РД определяет виды требований безопасности (функциональные и требования доверия), основные конструкции представления требований безопасности (профиль защиты, задание по безопасности) и содержит основные методические положения по оценке безопасности ИТ.

Часть 2 РД содержит универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определённым правилам.

Часть 3 РД содержит систематизированный каталог требований доверия к безопасности и оценочные уровни доверия, определяющие меры, которые должны быть приняты на всех этапах жизненного цикла продуктов или систем ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям.

Требования безопасности, содержащиеся в настоящем руководящем документе, могут уточняться и дополняться по мере совершенствования правовой и нормативной базы, развития информационных технологий и совершенствования методов обеспечения безопасности.

В соответствии с концепцией ОК, требования к безопасности объекта оценки разделяются на две категории:

- функциональные требования;
- требования гарантированности.

В функциональных требованиях описаны те функции объекта оценки, которые обеспечивают безопасность ИТ. Имеются в виду требования идентификации, установления подлинности (аутентификации) пользователей, протоколирования и др.

Требования гарантированности отражают качества объекта оценки, дающие основание для уверенности в том, что необходимые меры безопасности объекта эффективны и корректно реализованы. Оценка гарантированности получается на основе изучения назначения, структуры и функционирования объекта оценки. Требования гарантированности включают требования к организации процесса разработки, а также требования поиска, анализа и воздействия на потенциально уязвимые с точки зрения безопасности места.

В РД функциональные требования и требования гарантированности представлены в едином стиле.

Термин «класс» используется для наиболее общей группировки требований безопасности.

Члены класса названы семействами. В семейства группируются наборы требований, которые обеспечивают выполнение определённой части целей безопасности и могут отличаться по степени жёсткости.

Члены семейства называются компонентами. Компонент описывает минимальный набор требований безопасности для включения в структуры, определённые в РД.

Компоненты построены из элементов. Элемент – самый нижний, неделимый уровень требований безопасности.

Организация требований безопасности в РД по иерархии класс – семейство – компонент – элемент помогает определить нужные компоненты после идентификации угроз безопасности объекта оценки.

Между компонентами могут существовать зависимости. Они возникают, когда компонент недостаточен для выполнения цели безопасности и необходимо наличие другого компонента. Зависимости могут существовать как между функциональными компонентами, так и компонентами гарантированности.

Назначение позволяет заполнить спецификацию идентифицированного параметра при использовании компонента. Параметр может быть признаком или правилом, которое конкретизирует требование к определённой величине или диапазону величин. Например, элемент функционального компонента может требовать, чтобы данное действие выполнялось неоднократно. В этом случае назначение обеспечивает число или диапазон чисел, которые должны использоваться в параметре.

Выбор – это выбор одного или большего количества пунктов из списка с целью конкретизации возможностей элемента.

Обработка позволяет включить дополнительные детали в элемент и предполагает интерпретацию требования, правила, константы или условия, основанную на целях безопасности. Обработка должна только ограничить набор возможных приемлемых функций или механизмов, чтобы осуществить требования, но не увеличивать их. Обработка не позволяет создавать новые требования или удалять существующие и не влияет на список зависимостей, связанных с компонентом.

РД определяют также набор структур, которые объединяет компонента требований безопасности.

Промежуточная комбинация компонентов названа пакетом. Пакет включает набор требований, которые обеспечивают выполнение многократно используемого поднабора целей безопасности.

Уровни гарантированности оценки – это предопределённые пакеты требований гарантированности.

Одной из основных структур РД является «Профиль защиты» (ПЗ), определённый как набор требований, который состоит только из компонентов или пакетов функциональных требований и одного из уровней гарантированности.. ПЗ специфицирует совокупность требований, которые являются необходимыми и достаточными для достижения поставленных целей безопасности.

Требования Профиля защиты могут быть конкретизированы и дополнены в другой структуре РД – «Задании по безопасности» (ЗБ). ЗБ содержит набор требований, которые могут быть представлены одним из ПЗ или сформулированы в явном виде. ЗБ определяет набор требований для конкретного объекта оценки. Оно включает также спецификацию объекта оценки в виде функций безопасности (ФБ), которые должны обеспечить выполнение требований безопасности и мер гарантированности оценки.

Результатом оценки безопасности должен быть общий вывод, в котором описана степень соответствия объекта оценки функциональным требованиям и требованиям гарантированности.

1.16 Специальные требования и рекомендации по технической защите конфиденциальной информации

«Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» утверждены приказом Гостехкомиссии России от 30.08.2002 № 282.

СТР-К является нормативно-методическим документом и устанавливает порядок организации работ, требования и рекомендации по обеспечению технической защиты информации с ограниченным

доступом, не содержащей сведений, составляющих государственную тайну на территории Российской Федерации.

Требования и рекомендации этого документа распространяются на защиту государственных информационных ресурсов некриптографическими методами (служебная тайна), направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и специальных воздействий на информацию в целях её уничтожения, искажения и блокирования.

При проведении работ по защите негосударственных информационных ресурсов, составляющих коммерческую тайну, банковскую тайну и т.д., требования настоящего документа носят рекомендательный характер.

Документ определяет следующие вопросы защиты конфиденциальной информации:

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

Защита информации, обрабатываемой с использованием технических средств, является составной частью работ по созданию и эксплуатации объектов информатизации различного назначения и должна осуществляться в виде системы (подсистемы) защиты информации во взаимосвязи с другими мерами по защите информации. Защите подлежит речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде ин-

формативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитооптической и иной основе.

Объектами защиты при этом являются:

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

Защита информации на объекте информатизации достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от утечки по техническим каналам, несанкционированного доступа, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе её обработки, передачи и хранения, а также работоспособности технических средств.

При защите информации в локальных вычислительных сетях (ЛВС) конфиденциальная информация может обрабатываться только в ЛВС, расположенных в пределах контролируемой зоны.

Средства защиты информации от НСД должны использоваться во всех узлах ЛВС независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС и требуют постоянного квалифицированного контроля настроек СЗИ администратором безопасности информации. Класс защищённости ЛВС определяется в соответствии с требованиями действующих руководящих документов ФСТЭК России.

Для управления, контроля защищённости ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, должны использоваться соответствующие сертифицированные по требованиям безопасности информации средства защиты.

1.17 Юридическая значимость электронных документов с электронной подписью

Вопросы юридической значимости электронных документов представлены в приведённых ниже нормативных документах.

Гражданский кодекс Российской Федерации. Часть 1. Глава 9. Статья 160. Письменная форма сделки:

2. Использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон.

Гражданский кодекс Российской Федерации. Часть 1. Глава 28. Статья 434. Форма договора:

2. Договор в письменной форме может быть заключён путём составления одного документа, подписанного сторонами, а также путём обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

Статья 11. Документирование информации

4. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

5. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

Федеральный закон от 06.04.2011 № 6В-ФЗ «Об электронной подписи» определяет основные понятия, связанные с ЭП, следующим образом:

электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой

информацией и которая используется для определения лица, подписывающего информацию;

сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат) – сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган);

владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;

ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее – проверка электронной подписи);

удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

аккредитация удостоверяющего центра – признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

средства удостоверяющего центра – программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

корпоративная информационная система – информационная система, участники электронного взаимодействия в которой составляют определённый круг лиц;

информационная система общего пользования – информационная система, участники электронного взаимодействия в которой составляют неопределённый круг лиц и в использовании которой этим лицам не может быть отказано.

2 ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

2.1 Положение о государственной системе защиты информации

Структура государственной системы защиты информации в Российской Федерации, её задачи и функции, основы организации защиты сведений, отнесённых в установленном порядке к государственной или служебной тайне, определены в «Положении о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам», утверждённом постановлением Совета Министров – Правительства Российской Федерации от 15.09.1993 №912-51.

Настоящее Положение является документом, обязательным для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную тайну, в органах (аппаратах, администрациях) представительной, исполнительной и судебной властей Российской Федерации, республик в составе Российской Федерации, автономной области, автономных округов, краёв, областей, городов Москвы и Санкт-Петербурга и в органах местного самоуправления (далее именуются – органы государственной власти), на предприятиях и в их объединениях, учреждениях и организациях независимо от их организационно-правовой формы и формы собственности (далее именуются – предприятия).

Работы по защите информации в органах государственной власти и на предприятиях проводятся на основе актов законодательства Российской Федерации.

Защита информации осуществляется путём выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путём проведения специ-

альных работ, порядок организации и выполнения которых определяется Правительством Российской Федерации.

Мероприятия по защите информации являются составной частью управленческой, научной и производственной деятельности и осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности проводимых работ.

Главными направлениями работ по защите информации являются:

- обеспечение эффективного управления системой зашиты информации;
- определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения;
- анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки сведений, подлежащих защите;
- разработка организационно-технических мероприятий по защите информации и их реализация;
- организация и проведение контроля состояния защиты информации.

Основными организационно-техническими мероприятиями по защите информации являются:

- лицензирование деятельности предприятий в области защиты информации;
- аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;
- сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении;
- разработка и внедрение технических решений и элементов защиты информации при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи;

- разработка средств защиты информации и контроля за ее эффективностью (специального и общего применения) и их использование;
- применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

Конкретные методы, приёмы и меры защиты информации разрабатываются в зависимости от степени возможного ущерба в случае её утечки, разрушения (уничтожения).

Проведение любых мероприятий и работ с использованием сведений, отнесённых к государственной или служебной тайне, без принятия необходимых мер по защите информации не допускается.

2.2 Структура государственной системы защиты информации

Основные задачи государственной системы защиты информации:
- проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;
- исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе ее обработки, передачи и хранения;
- принятие в пределах компетенции правовых актов, регулирующих отношения в области защиты информации;
- анализ состояния и прогнозирование возможностей технических средств разведки и способов их применения, формирование системы информационного обмена сведениями по осведомленности иностранных разведок;
- организация сил, создание средств защиты информации и контроля за ее эффективностью;
- контроль состояния защиты информации в органах государственной власти и на предприятиях.

Государственную систему защиты информации образуют (см. рис. 2.1):
- Федеральная служба по техническому и экспортному контролю и ее центральный аппарат;

- Федеральная служба безопасности Российской Федерации, Министерство внутренних дел Российской Федерации, Министерство обороны Российской Федерации, Федеральная служба охраны Российской Федерации, Служба внешней разведки Российской Федерации, их структурные подразделения по защите информации;
- структурные и межотраслевые подразделения по защите информации органов государственной власти;
- управления Федеральной службы по техническому и экспортному контролю по федеральным округам;
- головная научно-исследовательская организация в Российской Федерации по защите информации (ФГУП «Научно-исследовательский испытательный институт проблем технической защиты информации» Федеральной службы по техническому и экспортному контролю);
- головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские организации по защите информации органов государственной власти;
- предприятия, проводящие работы по оборонной тематике и другие работы с использованием сведений, отнесенных к государственной или служебной тайне, их подразделения по защите информации;
- предприятия, специализирующиеся на проведении работ в области защиты информации;
- высшие учебные заведения и институты повышения квалификации по подготовке и переподготовке кадров в области защиты информации.

ФСТЭК России является межведомственным коллегиальным органом и возглавляет государственную систему защиты информации.

Права и функции ФСТЭК России и её центрального аппарата определяются «Положением о Федеральной службе по техническому и экспортному контролю», утверждённым Указом Президента Российской Федерации от 16.08.2004 № 1085 и «Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам», утверждённом постановлением Совета Министров - Правительства Российской Федерации от 15.09.1993 №912-51.

Права и функции в области защиты информации Федеральной службы безопасности Российской Федерации, Министерства обороны Российской Федерации, Министерства внутренних дел Российской Федерации, Федеральной службы охраны Российской Федерации и

Службы внешней разведки Российской Федерации определяются положениями об этих органах.

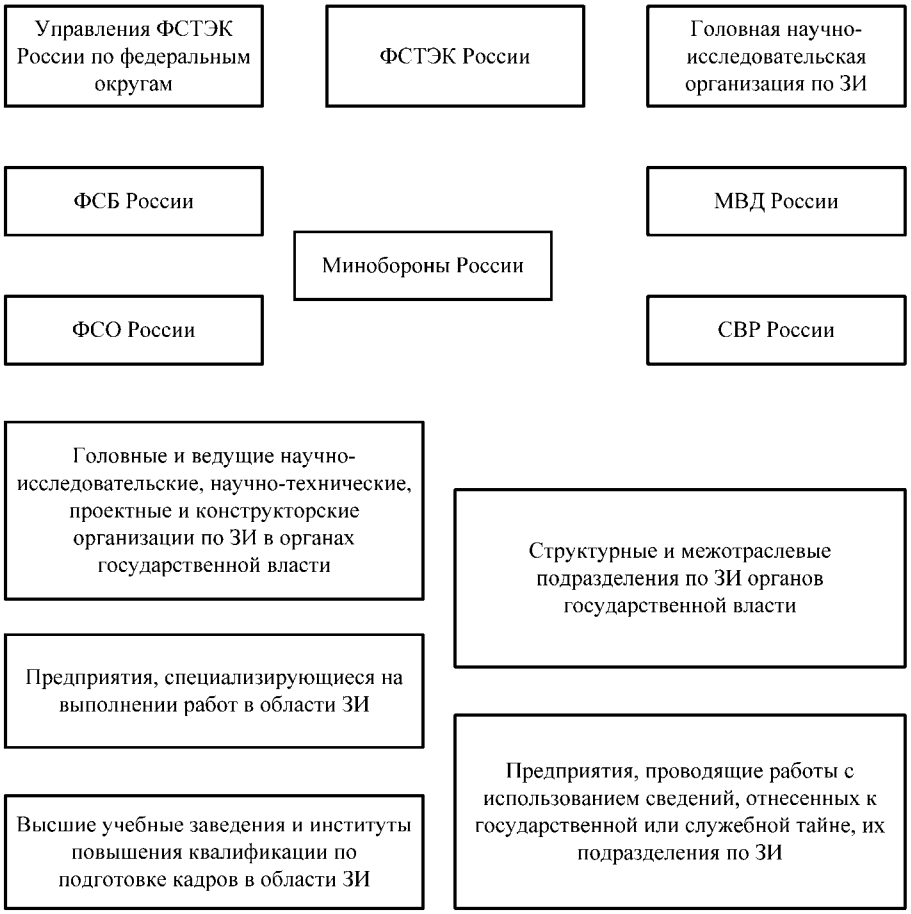

Рис. 2.1. Структура государственной системы защиты информации в Российской Федерации

Структурные и межотраслевые подразделения по защите информации органов государственной власти (в пределах их компетенции):

- проводят единую техническую политику, осуществляют координацию и методическое руководство работами по защите информации на подведомственных органу государственной власти предприятиях;

- выполняют функции заказчика по проведению научно-исследовательских и опытно-конструкторских работ по проблемам защиты информации, а также заказчика поисковых научно-исследовательских работ по этим проблемам;
- разрабатывают предложения для федеральных программ по защите информации;
- организуют аттестацию подведомственных органу государственной власти объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности, сертификацию средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам, проведение специальных проверок и специальных исследований технических средств;
- готовят рекомендации и указания по лицензированию деятельности предприятий в области защиты информации.

Непосредственное руководство работами по защите информации осуществляют руководители органов государственной власти или их заместители.

Указанные функции осуществляются подразделениями (штатными специалистами) по защите информации.

Подразделения по защите информации являются самостоятельными структурными подразделениями или входят в состав одного из главных, технических, научно-технических или специальных управлений органа государственной власти. Назначение на должности и освобождение от должности руководителей этих подразделений производятся по согласованию с ФСТЭК России.

Допускается создание при органе государственной власти в соответствии с актами законодательства Российской Федерации самостоятельных предприятий различных организационно-правовых форм и форм собственности, на которые могут быть возложены функции структурных, а также межотраслевых подразделений по защите информации.

В целях обеспечения принципа коллегиальности при рассмотрении важнейших вопросов защиты информации в органах государственной власти могут создаваться технические комиссии, межотраслевые или отраслевые советы.

Управления ФСТЭК России по федеральным округам, в пределах своих зон ответственности:

- проверяют и оценивают состояние защиты информации и оказывают методическую помощь на местах в организации и проведении мероприятий по защите информации;
- участвуют в аттестовании объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности.

Границы зон ответственности специальных центров определяет директор ФСТЭК России.

Головная научно-исследовательская организация в Российской Федерации по защите информации, головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские организации по защите информации органов государственной власти в пределах своей специализации разрабатывают научные основы и концепции, проекты федеральных программ, нормативно-технических и методических документов по защите информации, обобщают и анализируют информацию о силах и средствах технической разведки, прогнозируют её возможности, осуществляют разработку (корректировку) модели иностранной технической разведки и методик оценки её возможностей, проводят научные исследования и работы по созданию технических средств защиты информации и контроля за её эффективностью.

Организация работ по защите информации ***на предприятиях*** осуществляется их руководителями.

В зависимости от объёма работ по защите информации руководителем предприятия создаётся структурное подразделение по защите информации либо назначаются штатные специалисты по этим вопросам.

Подразделения по защите информации (штатные специалисты) на предприятиях осуществляют мероприятия по защите информации в ходе выполнения работ с использованием сведений, отнесённых к государственной или служебной тайне, определяют совместно с заказчиком работ основные направления комплексной защиты информации, участвуют в согласовании технических (тактико-технических) заданий на проведение работ, дают заключение о возможности проведения работ с информацией, содержащей сведения, отнесённые к государственной или служебной тайне.

Указанные подразделения (штатные специалисты) подчиняются непосредственно руководителю предприятия или его заместителю. Работники этих подразделений (штатные специалисты) приравниваются по оплате труда к соответствующим категориям работников основных структурных подразделений.

Для проведения работ по защите информации могут привлекаться на договорной основе специализированные предприятия, имеющие лицензии на право проведения работ в области защиты информации.

Предприятия, имеющие намерения заниматься деятельностью в области защиты информации, должны получить соответствующую лицензию на определённый вид этой деятельности. Лицензии выдаются ФСТЭК России и ФСБ России в соответствии со своей компетенцией по представлению органа государственной власти.

Высшие учебные заведения и институты повышения квалификации по подготовке и переподготовке кадров в области защиты информации осуществляют:

- первичную подготовку специалистов по комплексной защите информации;
- переподготовку (повышение квалификации) специалистов по защите информации органов государственной власти и предприятий;
- усовершенствование знаний руководителей органов государственной власти и предприятий в области защиты информации.

Подготовка кадров для государственной системы защиты информации осуществляется при методическом руководстве ФСТЭК России.

2.3 Организация защиты информации в системах и средствах информатизации и связи

Защита информации в системах и средствах информатизации и связи является составной частью работ по их созданию, эксплуатации и осуществляется во всех органах государственной власти и на предприятиях, располагающих информацией, содержащей сведения, отнесённые к государственной или служебной тайне.

Требования по защите информации в системах и средствах информатизации и связи определяются заказчиками совместно с разработчиками на стадии подготовки и согласования решений Правительства Российской Федерации, приказов и директив, планов и программ работ, технических и тактико-технических заданий на проведение исследовании, разработку (модернизацию), испытания, производство и эксплуатацию (применение) на основе стандартов, нормативно-технических и методических документов, разработанных Федеральной службой по техническому регулированию и метрологии, Федеральной службой по техническому и экспортному контролю и другими органами государственной власти в соответствии с их компетенцией. Указанные требования согласовываются с подразделениями по защите информации.

Организация защиты информации в системах и средствах информатизации и связи возлагается на руководителей органов государственной власти и предприятий, заказчиков и разработчиков систем и средств информатизации и связи, руководителей подразделений, эксплуатирующих эти системы и средства, а ответственность за обеспечение защиты информации – непосредственно на пользователя (потребителя) информации.

В интересах обеспечения защиты информации в системах и средствах информатизации и связи защите подлежат:

- информационные ресурсы, содержащие сведения, отнесенные к государственной или служебной тайне, представленные в виде носителей на магнитной и оптической основе, информативных физических полей, информационных массивов и баз данных;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для обработки информации, содержащей сведения, отнесенные к государственной или служебной тайне;
- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается (циркулирует) информация, содержащая сведения, отнесенные к государственной или служебной тайне, а также сами помещения, предназначенные для ведения секретных переговоров.

Целями защиты информации являются:

- предотвращение утечки информации по техническим каналам;
- предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в системах информатизации;
- соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах обработки;
- сохранение возможности управления процессом обработки и пользования информацией.

Защита информации осуществляется путём:

- предотвращения перехвата техническими средствами информации, передаваемой по каналам связи;
- предотвращения утечки обрабатываемой информации за счет побочных электромагнитных излучений н наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразований;
- исключения несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;
- предотвращения специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;
- выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);
- предотвращения перехвата техническими средствами речевой информации из помещений и объектов.

Предотвращение перехвата техническими средствами информации, передаваемой по каналам связи, достигается применением криптографических и иных методов и средств защиты, а также проведением организационно-технических и режимных мероприятий.

Предотвращение утечки обрабатываемой информации за счёт побочных электромагнитных излучений и наводок, а также электроакустических преобразований достигается применением защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами.

Исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации достигается применением специальных программно-технических средств защиты, использованием криптографических способов защиты, а также организационными и режимными мероприятиями.

Предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации, достигается применением специальных программных и аппаратных средств защиты (антивирусные процессоры, антивирусные программы), организацией системы контроля безопасности программного обеспечения.

Выявление возможно внедрённых на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) достигается проведением специальных проверок по выявлению этих устройств.

Предотвращение перехвата техническими средствами речевой информации из помещений и объектов достигается применением специальных средств защиты, проектными решениями, обеспечивающими звукоизоляцию помещений, выявлением специальных устройств подслушивания и другими организационными и режимными мероприятиями.

Информация, содержащая сведения, отнесённые к государственной или служебной тайне, должна обрабатываться с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств защиты, сертифицированных в установленном порядке.

Соответствие технического средства и его программного обеспечения требованиям защищённости подтверждается сертификатом, выдаваемым предприятием, имеющим лицензию на этот вид деятельности, по результатам сертификационных испытаний, или предписанием на эксплуатацию, оформляемым по результатам специальных исследований и специальных проверок технических средств и программного обеспечения.

Для оценки готовности систем и средств информатизации и связи к обработке (передаче) информации, содержащей сведения, отнесённые к государственной *или* служебной тайне, проводится аттестование указанных систем и средств в реальных условиях эксплуатации на предмет соответствия принимаемых методов, мер и средств защиты требуемому уровню безопасности информации.

Защита информации, передаваемой по общегосударственным и ведомственным линиям связи, обеспечивается потребителями, которые по согласованию с подразделениями ФСТЭК России и Мининформсвязи России разрабатывают инструкции по обеспечению защиты информации и определяют перечень организационных и технических мер, направленных на предотвращение утечки информации по техническим каналам.

Необходимость защиты доступных средствам радиоразведки каналов связи, по которым передаются потоки служебной информации, где отдельно взятые сведения не составляют государственную или служебную тайну, определяется решениями ФСТЭК России по согласованию с заинтересованными органами государственной власти.

2.4 Состояния защиты информации

Контроль состояния защиты информации (далее именуется – контроль) осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию.

Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты информации, решений ФСТЭК России, а также в оценке обоснованности и эффективности принятых мер защиты для обеспечения выполнения утверждённых требований и норм по защите информации.

Контроль организуется Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации, Министерством внутренних дел Российской Федерации, Министерством обороны Российской Федерации, Службой внешней разведки Российской Федерации и Федеральной службой охраны Российской Федерации, структурными и межотраслевыми подразделениями органов государственной власти, входящими в государственную систему защиты информации, и предприятиями в соответствии с их компетенцией.

Акты проверок предприятий рассылаются их руководителями в орган, проводивший проверку, и в орган государственной власти по подчинённости предприятия.

ФСТЭК России организует контроль силами центрального аппарата и управлений ФСТЭК России по федеральным округам. Она может привлекать для этих целей подразделения по защите информации органов государственной власти.

Центральный аппарат ФСТЭК России осуществляет в пределах своей компетенции контроль в органах государственной власти и на предприятиях, обеспечивает методическое руководство работами по контролю (за исключением объектов и технических средств, защита которых входит в компетенцию ФСБ России, МВД России, Минобороны России, СВР России, ФСО Росси).

Управления ФСТЭК России по федеральным округам, в пределах своей компетенции осуществляют контроль в органах государственной власти и на предприятиях, расположенных в зонах ответственности этих центров.

Органы государственной власти организуют и осуществляют контроль на подчинённых им предприятиях через свои подразделения по защите информации. Повседневный контроль за состоянием защиты информации на предприятиях проводится силами их подразделений по защите информации.

Контроль на предприятиях негосударственного сектора при выполнении работ с использованием сведений, отнесённых к государственной или служебной тайне, осуществляется органами государственной власти, ФСТЭК России, ФСБ России и заказчиком работ в соответствии с их компетенцией.

Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

Нарушения по степени важности делятся на три категории:

- первая – невыполнение требований или норм по защите информации, в результате чего имелась или имеется реальная возможность ее утечки по техническим каналам;
- вторая – невыполнение требований по защите информации, в результате чего создаются предпосылки к ее утечке по техническим каналам;
- третья – невыполнение других требований по защите информации.

При обнаружении нарушений первой категории руководители органов государственной власти и предприятий обязаны:

- немедленно прекратить работы на участке (рабочем месте), где обнаружены нарушения, и принять меры по их устранению;
- организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц;
- сообщить в ФСТЭК России, ФСБ России, руководству органа государственной власти и заказчику о вскрытых нарушениях и принятых мерах.

Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер, проводимой ФСТЭК России или по её поручению подразделениями по защите информации органов государственной власти.

При обнаружении нарушений второй и третьей категорий руководители проверяемых органов государственной власти и предприятий обязаны принять необходимые меры по их устранению в сроки, согласованные с органом, проводившим проверку, или заказчиком (представителем заказчика). Контроль за устранением этих нарушений осуществляется подразделениями по защите информации этих органов государственной власти и предприятий.

2.5 Финансирование мероприятий по защите информации

Финансирование мероприятий по защите информации, содержащей сведения, отнесённые к государственной или служебной тайне, а также подразделений по защите информации в органах государственной власти и на бюджетных предприятиях предусматривается в сметах расходов на их содержание.

Создание технических средств зашиты информации, не требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчикам на научно-исследовательские и опытно-конструкторские работы, связанные с разработкой продукции. Расходы по разработке технических средств защиты включаются в стоимость разработки образца продукции.

Создание технических средств защиты информации, требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчикам на строительство (реконструкцию) сооружений или объектов.

3 ОСНОВНЫЕ ЗАЩИТНЫЕ МЕХАНИЗМЫ, РЕАЛИЗУЕМЫЕ В РАМКАХ РАЗЛИЧНЫХ МЕР И СРЕДСТВ ЗАЩИТЫ

3.1 Основные механизмы защиты информационных систем

Для защиты компьютерных систем от неправомерного вмешательства в процессы их функционирования и НСД к информации используются следующие основные методы защиты (защитные механизмы):

- идентификация (именование и опознавание), аутентификация (подтверждение подлинности) пользователей системы;
- разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям;
- регистрация и оперативное оповещение о событиях, происходящих в системе;
- криптографическое закрытие (шифрование) хранимых и передаваемых по каналам связи данных;
- контроль целостности и аутентичности (подлинности и авторства) данных;
- резервирование и резервное копирование;
- фильтрация трафика и трансляция адресов;
- обнаружение вторжений (атак);
- выявление и нейтрализация действий компьютерных вирусов;
- затирание остаточной информации на носителях;
- выявление уязвимостей (слабых мест) системы;
- маскировка и создание ложных объектов;
- страхование рисков.

Перечисленные механизмы защиты могут применяться в конкретных технических средствах и системах защиты в различных комбинациях и вариациях. Наибольший эффект достигается при их системном использовании в комплексе с другими видами мер защиты. В дальнейшем будут рассмотрены наиболее важные защитные механизмы.

3.2 Идентификация и аутентификация пользователей

В целях обеспечения возможности разграничения доступа к ресурсам АС и возможности регистрации событий такого доступа каждый субъект (сотрудник, пользователь, процесс) и объект (ресурс) защищаемой автоматизированной системы должен быть однозначно идентифицируем. Для этого в системе должны храниться специальные признаки каждого субъекта и объекта, по которым их можно было бы однозначно опознать.

Идентификация – это, с одной стороны, присвоение индивидуальных имён, номеров (идентификаторов) субъектам и объектам системы, а с другой стороны, – это их распознавание (опознавание) по присвоенным им уникальным идентификаторам. Наличие идентификатора позволяет упростить процедуру выделения конкретного субъекта (определённый объект) из множества однотипных субъектов (объектов). Чаще всего в качестве идентификаторов применяются номера или условные обозначения в виде набора символов.

Аутентификация – это проверка (подтверждение) подлинности идентификации субъекта или объекта системы. Цель аутентификации субъекта – убедиться в том, что субъект является именно тем, кем представился (идентифицировался). Цель аутентификации объекта – убедиться, что это именно тот объект, который нужен.

Идентификация и аутентификация пользователей должна производиться при каждом их входе в систему и при возобновлении работы после кратковременного перерыва (после периода неактивности без выхода из системы или выключения компьютера).

Аутентификация пользователей может осуществляться следующим образом:

- путем проверки знания того, чего не знают другие (паролей, PIN-кодов, ключевых слов);
- путем проверки владения тем, что относительно сложно подделать (карточками, ключевыми вставками и т.п.);
- путем проверки уникальных физических характеристик и параметров (отпечатков пальцев, особенностей радужной оболочки глаз, формы кисти рук и т.п.) самих пользователей при помощи специальных биометрических устройств;
- путем проверки рекомендации (сертификата, специального билета) от доверенного посредника.

Системы аутентификации могут быть двух видов – с взаимной и односторонней аутентификацией. Примером взаимной аутентифи-

кации является аутентификация WEB-сервера, которая предполагает предъявление сертификата, доказывающего взаимодействие с нужным оборудованием, которое находится под управлением нужных физических или юридических лиц.

Простейшей формой аутентификации является парольная, при которой ввод значений идентификатора и пароля осуществляется, как правило, с клавиатуры. Считается, что эта форма аутентификации небезопасна, поскольку:

- пользователи часто применяют короткие, легко подбираемые пароли;
- во многих системах существуют многочисленные возможности перехвата паролей (серфинг на плече, запуск клавиатурных «шпионов», перехват в открытых сетях и т.д.).

В связи с этим в Международном стандарте ISO/IEC 27002 рекомендуется использовать в информационной системе сервисы, не допускающие передачу пароля в открытом виде. Именно поэтому современные защищенные информационные системы применяют, как правило, хеширование и шифрование передаваемых паролей, а также одноразовые пароли.

В качестве эффективного средства против подбора паролей могут быть использованы организационные меры в виде систематической смены пароля пользователями.

Другим важным достоинством парольной аутентификации является её интеллектуальная составляющая, т.е. связь с разумом и сознанием пользователя. В совершенных с точки зрения безопасности информационных системах пароли должны храниться исключительно в «человеческой» памяти пользователей без записи на любой материальный носитель информации.

Другой способ аутентификации связан с использованием «отчуждаемых» элементов, которыми уникально обладают пользователи (смарт-карты, дискеты, ключевые контейнеры, радиочастотные бесконтактные карточки, электронные таблетки iButton и т.п.). Как правило, подобный механизм применяется в совокупности с дополнительной парольной аутентификацией (вводом PIN-кода), образуя двухфакторную систему аутентификации. Типичным примером двухфакторной аутентификации является защита ключевых контейнеров на различных носителях (смарт-картах, е-токенов и др.) с помощью PIN-кода.

В качестве другого примера двухфакторной аутентификации можно привести технологию RSA Secure ID, показанную на рис. 3.1.

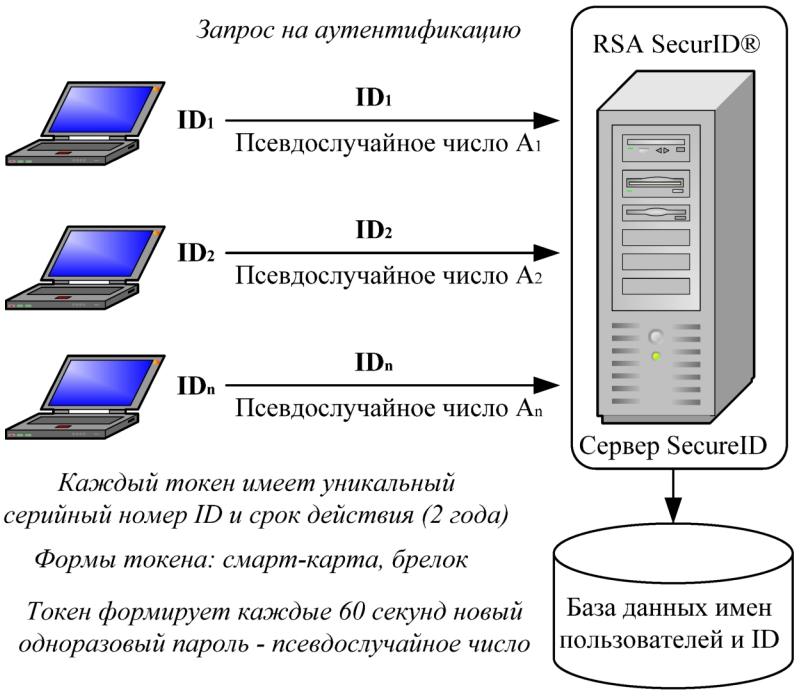

Рис. 3.1. Технология двухфакторной аутентификации RSA Secure ID

Одной из форм этого способа аутентификации является аутентификация по адресу (IP-адресу, e-mail адресу, телефонному номеру), активно применяющаяся в системах Клиент-Банк и сотовой телефонии.

Недостаток аутентификации «владения» – возможность потери (кражи) аутентификатора. Альтернативой служат биометрические технологии, которые характеризуются:

- относительной трудностью потери аутентификатора;
- высоким уровнем достоверности опознавания пользователей.

В основе работы этих систем лежит биометрическое распознавание – сравнение физиологических и психологических особенностей субъекта с его аналогичными характеристиками, хранящимися в базе данных объекта.

Биометрические технологии делятся на физиологические и психологические.

В первой из них используются постоянные физиологические (генетические) параметры субъекта: параметры пальцев (папиллярные линии, рельеф), структура глаза (сетчатки или радужной оболочки), форма ладони (отпечаток или топография), геометрические характеристики лица (2D или 3D графика), структура ДНК (сигнатура) и т.п.

Психологические технологии (индивидуальные поведенческие особенности, присущие каждому человеку) носят изменчивый характер: спектр голоса, динамические параметры письма, особенности ввода символов с клавиатуры.

Недостатками биометрической аутентификацией являются:

- проблема получения ключа из биометрических параметров;
- возможность исключения из процесса аутентификации субъектов со скомпрометированным электронным аутентификатором;
- относительно высокая стоимость реализации биометрических систем;
- возможностью ошибок распознавания первого и второго рода (пропуск или ложная тревога);
- возможность изготовления относительно дешевых муляжей для биопараметров.

Для реализации рассмотренных выше способов аутентификации необходим первоначальный контакт между субъектом и объектом, в процессе которого стороны обмениваются аутентификатором. В ряде случаев такой контакт невозможен, например, в системах электронного бизнеса B2C.

B2C – это краткосрочное взаимодействие бизнеса и конечного потребителя бизнес-продукта, сопровождаемое большим числом разовых сделок, при котором ни поставщики, ни потребители никогда ранее не имели взаимных деловых контактов. Для подобных заочных транзакций наиболее эффективна аутентификация с использованием различных форм рекомендаций от доверенного посредника, например сертификата или билета.

В частности, широко известны сертификаты X509, связывающие открытый ключ клиента и его уникальный идентификатор, которые подписаны цифровой подписью доверенного центра сертификации.

Перспективой развития технологий аутентификации является создание многофакторных систем аутентификации с комбинированным применением паролей, биопараметров, отчуждаемых элементов и сертификатов.

3.3 Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы

Разграничение (контроль) доступа к ресурсам АС – это такой порядок использования ресурсов автоматизированной системы, при котором субъекты получают доступ к объектам системы в строгом соответствии с установленными правилами.

Объект – это пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа.

Субъект – это активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.

Доступ к информации – ознакомление с информацией (чтение, копирование), её модификация (корректировка), уничтожение (удаление) и т.п.

Доступ к ресурсу – получение субъектом возможности манипулировать данным ресурсом (использовать, управлять, изменять настройки и т.п.).

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

Несанкционированный доступ (НСД) – доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

Авторизация – предоставление аутентифицированному субъекту соответствующих (предписанных установленным порядком) прав на доступ к объектам системы: какие данные и как он может использовать (какие операции с ними выполнять), какие программы может выполнять, когда, как долго и с каких терминалов может работать, какие ресурсы системы может использовать и т.п.

Авторизованный субъект доступа – субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

Авторизация пользователей осуществляется с использованием следующих основных механизмов реализации разграничения доступа:

- механизмов избирательного управления доступом, основанных на использовании атрибутных схем, списков разрешений и т.п.;

- механизмов полномочного управления доступом, основанных на использовании меток конфиденциальности ресурсов и уровней допуска пользователей;
- механизмов обеспечения замкнутой среды доверенного программного обеспечения (индивидуальных для каждого пользователя списков разрешенных для использования программ), поддерживаемых механизмами идентификации и аутентификации пользователей при их входе в систему.

Технические средства разграничения доступа к ресурсам АС должны рассматриваться как составная часть единой системы контроля доступа субъектов:
- на контролируемую территорию;
- в отдельные здания и помещения организации;
- к элементам АС и элементам системы защиты информации (физический доступ);
- к информационным и программным ресурсам АС.

Механизмы управления доступом субъектов к объектам доступа выполняют основную роль в обеспечении внутренней безопасности компьютерных систем. Их работа строится на концепции единого диспетчера доступа. Сущность этой концепции состоит в том, что диспетчер доступа (монитор ссылок) – выступает посредником-контролером при всех обращениях субъектов к объектам (см. рис. 3.2).

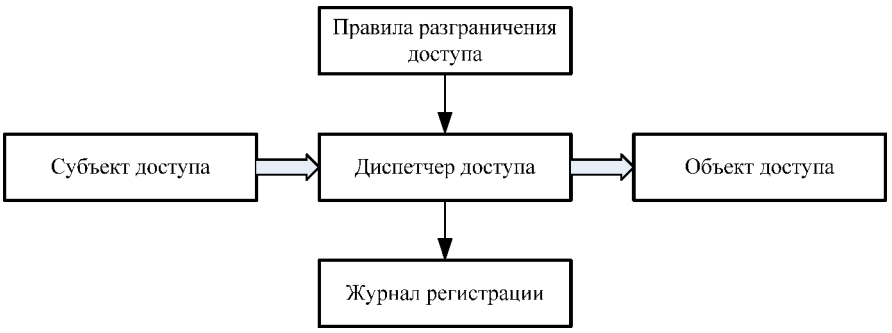

Рис. 3.2. Диспетчер доступа

Диспетчер доступа выполняет следующие основные функции:
- проверяет права доступа каждого субъекта к конкретному объекту на основании информации, содержащейся в базе данных системы защиты (правил разграничения доступа);

- разрешает (производит авторизацию) или запрещает (блокирует) доступ субъекта к объекту;
- при необходимости регистрирует факт доступа и его параметры в системном журнале (в том числе попытки несанкционированного доступа с превышением полномочий).

Основными требованиями к реализации диспетчера доступа являются:

- полнота контролируемых операций (проверке должны подвергаться все операции всех субъектов над всеми объектами системы, обход диспетчера предполагается невозможным);
- изолированность диспетчера, то есть защищенность самого диспетчера от возможных изменений субъектами доступа с целью влияния на процесс его функционирования;
- возможность формальной проверки правильности функционирования;
- минимизация используемых диспетчером ресурсов (накладных расходов).

В общем виде работа средств разграничения доступа субъектов к объектам основана на проверке сведений, хранимых в базе данных защиты.

Под ***базой данных защиты*** (security database) понимают базу данных, хранящую информацию о правах доступа субъектов к объектам.

Для внесения изменений в базу данных защиты система разграничения доступа должна включать средства для привилегированных пользователей (администраторов безопасности, владельцев объектов и т.п.) по ведению этой базы. Такие средства управления доступом должны обеспечивать возможность выполнения следующих операций:

- добавления и удаления объектов и субъектов;
- просмотра и изменения соответствующих прав доступа субъектов к объектам.

Форма представления базы данных защиты может быть различной

Основу базы данных средств разграничения доступа в общем случае составляет абстрактная ***матрица доступа*** или её реальные представления. Каждая строка этой матрицы соответствует субъекту, а столбец – объекту АС. Каждый элемент этой матрицы представляет собой кортеж (упорядоченную совокупность значений), определяющий права доступа (для всех возможных видов доступа – чтение, модификация, удаление и т.п.) определенного субъекта к определенному объекту (см. рис.3.3).

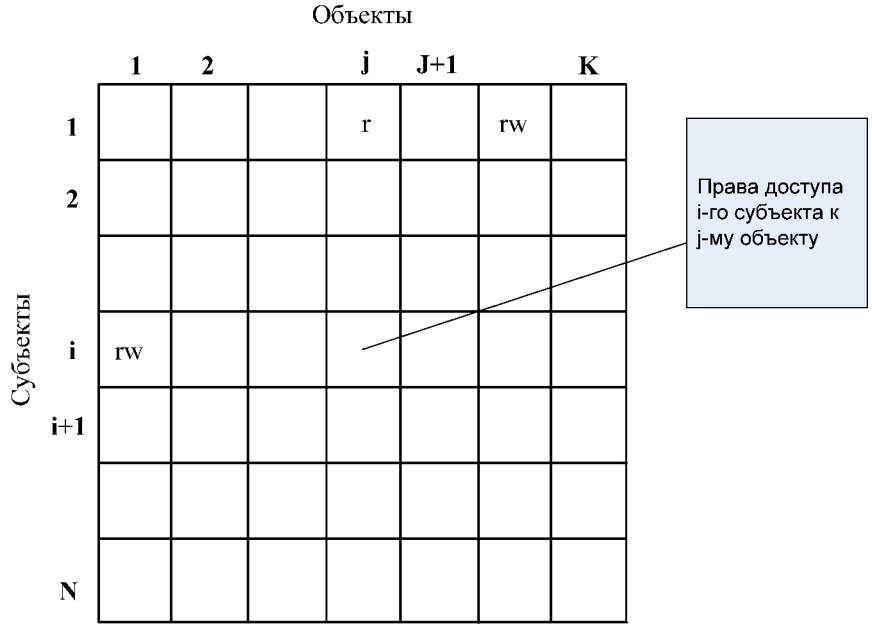

Рис. 3.3. Матрица избирательного управления доступом

Сложность управления доступом (ведения матрицы доступа) в реальных системах связана не только с большой размерностью этой матрицы (большим числом субъектов и объектов) и высоким динамизмом её корректировки, но и с необходимостью постоянного отслеживания при таких корректировках большого числа зависимостей между значениями определённых кортежей. Наличие таких зависимостей связано с объективно существующими в предметной области ограничениями и правилами наследования полномочий в иерархии объектов и субъектов.

Например, пользователь должен наследовать полномочия групп пользователей, в которые он входит. Права доступа некоторого пользователя к каталогам и файлам не должны превышать соответствующие его права по доступу к диску, на котором они размещены.

При полномочном управлении доступом (категорирование объектов и субъектов и введение ограничений по доступу установленных категорий субъектов к объектам различных категории) на матрицу доступа накладываются дополнительные зависимости между значениями прав доступа субъектов.

Ограничения и зависимости между полномочиями существенно усложняют процедуры ведения матриц доступа. Это привело к воз-

никновению большого числа способов неявного задания матрицы (списки доступа, перечисление полномочий, атрибутные схемы и т.п.).

Основные критерии оценки эффективности различных способов неявного задания матрицы доступа следующие:

- затраты памяти на хранение образа матрицы доступа;
- время на выборку (или динамическое вычисление) значений полномочий (элементов кортежей);
- удобство ведения матрицы при наличии ограничений и зависимостей между значениями ее кортежей (простота и наглядность, количество требуемых операций при добавлении/удалении субъекта или объекта, назначении/модификации полномочий и т.п.).

Рассмотрим основные способы неявного задания матрицы доступа.

Списки управления доступом к объекту

В данной схеме полномочия по доступу к объекту представляются в виде списков (цепочек) кортежей для всех субъектов, имеющих доступ к данному объекту. Это равносильно представлению матрицы по столбцам с исключением кортежей, имеющих все нулевые значения.

Такое представление матрицы доступа получило название «списка управления доступом» (access control list - ACL). Этот вид задания матрицы реализован, к примеру, в ОС Windows NT/2000/2003/XP/Vista (в NTFS).

Достоинства:

- экономия памяти, так как матрица доступа обычно сильно разрежена;
- удобство получения сведений о субъектах, имеющих какой-либо вид доступа к заданному объекту.

Недостатки:

- неудобство отслеживания ограничений и зависимостей по наследованию полномочий субъектов;
- неудобство получения сведений об объектах, к которым имеет какой-либо вид доступа данный субъект;
- так как списки управления доступом связаны с объектом, то при удалении субъекта возможно возникновение ситуации, при которой объект может быть доступен несуществующему субъекту.

Списки полномочий субъектов

В данной модели полномочия доступа субъекта представляются в виде списков (цепочек) кортежей для всех объектов, к которым он имеет доступ (любого вида). Это равносильно представлению матрицы по строкам с исключением кортежей, имеющих нулевые значения.

Такое представление матрицы доступа называется «профилем» (profile) субъекта. Пример реализации списков полномочий субъектов – сетевая ОС Novell NetWare.

В системах с большим количеством объектов профили могут иметь большие размеры и, вследствие этого, ими трудно управлять. Изменение профилей нескольких субъектов может потребовать большого количества операций и привести к трудностям в работе системы.

Достоинства:

- экономия памяти, так как матрица доступа обычно сильно разрежена;
- удобство получения сведений об объектах, к которым имеет какой-либо вид доступа данный субъект.

Недостатки:

- неудобство отслеживания ограничений и зависимостей по наследованию полномочий доступа к объектам;
- неудобство получения сведений о субъектах, имеющих какой -либо вид доступа к заданному объекту;
- так как списки управления доступом связаны с субъектом, то при удалении объекта возможно возникновение ситуации, при которой субъект может иметь права на доступ к несуществующему объекту.

Атрибутные схемы

Так называемые атрибутные способы задания матрицы доступа основаны на присвоении субъектам и/или объектам определённых меток, содержащих значения атрибутов, на основе сопоставления которых определяются права доступа (производится авторизация субъекта). Наиболее известным примером неявного задания матрицы доступа является реализация атрибутной схемы в операционной системе UNIX.

Основными достоинствами этих схем являются:

- экономия памяти, так как элементы матрицы не хранятся, а динамически вычисляются при попытке доступа для конкретной пары субъект-объект на основе их меток или атрибутов;
- удобство корректировки базы данных защиты, то есть модификации меток и атрибутов;
- удобство отслеживания ограничений и зависимостей по наследованию полномочий субъектов, так как они в явном виде не хранятся, а формируются динамически;
- отсутствие потенциальной противоречивости при удалении отдельных субъектов или объектов.

Недостатки:

- дополнительные затраты времени на динамическое вычисление значений элементов матрицы при каждом обращении любого субъекта к любому объекту;
- затруднено задание прав доступа конкретного субъекта к конкретному объекту.

Диспетчер доступа, контролируя множество событий безопасности, происходящих в системе, тесно взаимодействует с подсистемами регистрации событий и оперативного оповещения об их наступлении. Он обеспечивает обнаружение и регистрацию до нескольких сотен типов событий. Примером таких событий могут служить:

- вход пользователя в систему;
- вход пользователя в сеть;
- неудачная попытка входа в систему или сеть (неправильный ввод имени или пароля);
- подключение к файловому серверу;
- запуск программы;
- завершение программы;
- оставление программы резидентно в памяти;
- попытка открытия файла недоступного для чтения;
- попытка открытия на запись файла недоступного для записи;
- попытка удаления файла недоступного для модификации;
- попытка изменения атрибутов файла, недоступного для модификации;
- попытка запуска программы, недоступной для запуска;
- попытка получения доступа к недоступному каталогу;
- попытка чтения/записи информации с диска, недоступного пользователю;
- попытка запуска программы с диска, недоступного пользователю;
- вывод на устройства печати документов с грифом (при полномочном управлении доступом);
- нарушение целостности программ и данных системы защиты и др.

В хорошо спроектированных системах защиты все механизмы контроля используют единый механизм регистрации. Однако в системах, где используются разнородные средства защиты разных производителей, в каждом из них используются свои механизмы и ведутся свои журналы регистрации, что создаёт дополнительные сложности в администрировании системы защиты.

Полномочное управление доступом

Механизм полномочного (меточного, мандатного) управления доступом был разработан в SO-х годах прошлого века в интересах Министерства обороны США для обработки информации с различными грифами секретности.

Полномочный метод управления доступом включает:

- присвоение каждому объекту системы метки критичности, определяющей ценность содержащейся в нем информации;
- присвоение каждому субъекту системы уровня прозрачности (уровня допуска), определяющего максимальное значение метки критичности объектов, к которым субъект имеет доступ.

При этом цель системы защиты не просто контролировать доступ пользователя к объектам АС, а контролировать его так, чтобы:

- пользователь не получил доступ к данным, более конфиденциальным, чем позволяет его форма допуска;
- не произошло копирование этих данных на носители с меньшими уровнями важности.

Можно выделить две системы присвоения меток конфиденциальности:

- иерархическая система меток (грифов) конфиденциальности;
- неиерархическая система меток конфиденциальности.

К сожалению, полномочный метод управления доступом не нашёл широкого распространения в коммерческом (негосударственном) секторе в связи со следующими причинами:

- отсутствием в коммерческой организации четкой классификации хранимой и обрабатываемой информации, аналогичной государственной;
- относительно высокой стоимостью реализации и большими накладными расходами.

Замкнутая программная среда

Механизм замкнутой программной среды предусматривает формирование жёсткого списка программ, разрешённых системе для запуска.

Однако при этом необходимо обеспечить выполнение определённых требований:

- «запрещено все, что явно не разрешено»;
- указание полных путей доступа к исполняемым файлам;
- запрет модификации (защита от подмены) файлов;
- формирование списка по журналам регистрации;
- наличие «мягкого» режима работы.

3.4 Регистрация и оперативное оповещение о событиях безопасности

Механизмы регистрации предназначены для получения и накопления (с целью последующего анализа) информации о состоянии ресурсов системы и о действиях субъектов, признанных администрацией АС потенциально опасными для системы. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, характер воздействий на систему, определить, как далеко зашло нарушение, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации.

Дополнительно, средства регистрации позволяют получать исчерпывающую статистику по использованию тех или иных ресурсов, межсетевому трафику, использованию сервисов, попыткам несанкционированного доступа, и т.п.

Кроме записи сведений об определённых событиях в специальные журналы для последующего анализа, средства регистрации событий могут обеспечивать и оперативное оповещение администраторов безопасности (при наличии соответствующих возможностей по передаче сообщений) о состоянии ресурсов, попытках НСД и других действиях пользователей, которые могут повлечь за собой нарушение политики безопасности и привести к возникновению кризисных ситуаций.

При регистрации событий безопасности в системном журнале обычно фиксируется следующая информация:

- дата и время события;
- идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;
- действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

Механизмы регистрации очень тесно связаны с другими защитными механизмами. Сигналы о происходящих событиях и детальную информацию о них механизмы регистрации получают от механизмов контроля (подсистем разграничения доступа, контроля целостности ресурсов и других).

В наиболее развитых системах защиты подсистема оповещения сопряжена с механизмами оперативного автоматического реагирования на определенные события. Могут поддерживаться следующие основные способы реагирования на обнаруженные факты НСД (возможно с участием администратора безопасности):

- подача сигнала тревоги;

- извещение администратора безопасности;
- извещение владельца информации о НСД к его данным;
- снятие программы (задания) с дальнейшего выполнения;
- отключение (блокирование работы) терминала или компьютера, с которого были осуществлены попытки НСД к информации;
- исключение нарушители из списка зарегистрированных пользователей и т.п.

3.5 Криптографические методы защиты информации

Криптографическое преобразование – это преобразование информации, основанное на некотором алгоритме, зависящем от изменяемого параметра (обычно называемого секретным ключом), и обладающее свойством невозможности восстановления исходной информации по преобразованной, без знания действующего ключа, с трудоёмкостью меньше заранее заданной.

К криптографическим средствам защиты (в соответствии с Положениями о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами, утверждёнными постановлением Правительства Российской Федерации от 29.12.2007 № 957) относятся:

- средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;
- средства имитозащиты – аппаратные, программные и аппаратно- программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;
- средства электронной цифровой подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание ЭЦП подписи с использованием закрытого ключа ЭЦП, подтверждение с использованием открытого ключа ЭЦП и подлинности ЭЦП, создание закрытых и открытых ключей ЭЦП;
- средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

- средства изготовления ключевых документов (независимо от вида носителя ключевой информации);
- ключевые документы (независимо от вида носителя ключевой информации).

Криптографические технологии защиты информации позволяют решать следующие задачи:
- аутентификация абонентов;
- контроль целостности данных;
- закрытие данных, хранимых в АС или передаваемых по каналам связи;
- разграничение ответственности на основе обеспечения аутентичности и неотказуемости.

Основным достоинством криптографических методов является то, что они обеспечивают высокую гарантированную стойкость защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей).

К числу основных недостатков криптографических методов следует отнести:
- значительные затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации;
- трудности совместного использования зашифрованной (подписанной) информации, связанные с управлением ключами (генерация, распределение и т.д.);
- высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены.

Криптография делится на два класса: криптография с симметричными ключами и криптография с открытыми ключами.

Криптография с симметричными ключами

В криптографии с симметричными ключами (классическая криптография) абоненты используют один и тот же (общий) ключ (секретный элемент) как для шифрования, так и для расшифрования данных.

Следует выделить следующие преимущества криптографии с симметричными ключами:
- относительно высокая производительность алгоритмов;
- высокая криптографическая стойкость алгоритмов на единицу длины ключа. К недостаткам криптографии с симметричными ключами следует отнести:

- необходимость использования сложного механизма распределения ключей;
- технологические трудности обеспечения неотказуемости.

Криптография с открытыми ключами

Для решения задач распределения ключей и ЭП были использованы идеи асимметричности преобразований и открытого распределения ключей Диффи и Хеллмана. В результате была создана криптография с открытыми ключами, в которой используется не один секретный, а пара ключей: открытый (публичный) ключ и секретный (личный, индивидуальный) ключ, известный только одной взаимодействующей стороне. В отличие от секретного ключа, который должен сохраняться в тайне, открытый ключ может распространяться публично.

Схема шифрования данных с использованием открытого ключа состоит из двух этапов. На первом из них производится обмен по несекретному каналу открытыми ключами. При этом необходимо обеспечить, подлинность передачи ключевой информации. На втором этапе, собственно, реализуется шифрование сообщений, при котором отправитель зашифровывает сообщение открытым ключом получателя. Зашифрованный файл может быть прочитан только владельцем секретного ключа, т.е. получателем. Схема расшифрования, реализуемая получателем сообщения, использует для этого секретный ключ получателя.

Реализация схемы ЭП связана с вычислением хэш-функции (дайджеста) данных, которая представляет собой уникальное число, полученное из исходных данных путём его сжатия (свёртки) с помощью сложного, но известного алгоритма. Хэш-функция является однонаправленной функцией, т.е. по хэш-значению невозможно восстановить исходные данные. Хэш-функция чувствительна к всевозможным искажениям данных. Кроме того, очень трудно отыскать два набора данных, обладающих одним и тем же значением хэш-функции.

Схема формирования подписи электронного документа (ЭД) его отправителем включает вычисление хэш-функции ЭД и зашифрование этого значения посредством секретного ключа отправителя. Результатом шифрования является значение ЭП ЭД (реквизит ЭД), которое пересылается вместе с самим ЭД получателю. При этом получателю сообщения должен быть предварительно передан открытый ключ отправителя сообщения.

Схема проверки (верификации) ЭП, осуществляемая получателем сообщения, состоит из следующих этапов. На первом из них произ-

водится расшифрование блока ЭП посредством открытого ключа отправителя. Затем вычисляется хэш-функция ЭД. Результат вычисления сравнивается с результатом расшифрования блока ЭП. В случае совпадения принимается решение о соответствии ЭП ЭД. Несовпадение результата расшифрования с результатом вычисления хэш-функции ЭД может объясняться следующими причинами:

- в процессе передачи по каналу связи была потеряна целостность ЭД;
- при формировании ЭП был использован не тот (поддельный) секретный ключ;
- при проверке ЭП был использован не тот открытый ключ (в процессе передачи по каналу связи или при дальнейшем его хранении открытый ключ был модифицирован или подменен).

Реализация криптографических алгоритмов с открытыми ключами требует сравнительно (с симметричными алгоритмами) больших затрат процессорного времени. Поэтому криптография с открытыми ключами обычно используется для решения задач распределения ключей и ЭП, а симметричная криптография – для шифрования.

Широко известна схема комбинированного шифрования, сочетающая высокую безопасность криптосистем с открытым ключом с преимуществами высокой скорости работы симметричных криптосистем. В этой схеме для шифрования используется случайно вырабатываемый симметричный (сеансовый) ключ, который, в свою очередь, зашифровывается посредством открытой криптосистемы для его секретной передачи по каналу в начале сеанса связи.

Доверие к открытому ключу и цифровые сертификаты

Центральным вопросом схемы открытого распределения ключей является вопрос доверия к полученному открытому ключу партнёра, который в процессе передачи или хранения может быть модифицирован или подменен. Для широкого класса практических систем (системы электронного документооборота, системы Клиент-Банк, межбанковские системы электронных расчётов), в которых возможна личная встреча партнёров до начала обмена ЭД, эта задача имеет относительно простое решение – взаимная сертификация открытых ключей.

Эта процедура заключается в том, что каждая сторона при личной встрече удостоверяет подписью уполномоченного лица и печатью бумажный документ – распечатку содержимого открытого ключа другой стороны. Этот бумажный сертификат является, во- первых, обязательством стороны использовать для проверки подписи под

входящими сообщениями данный ключ, и, во-вторых, обеспечивает юридическую значимость взаимодействия. Действительно, рассмотренные бумажные сертификаты позволяют однозначно идентифицировать мошенника среди двух партнёров, если один из них захочет подменить ключи.

Таким образом, для реализации юридически значимого электронного взаимодействия двух сторон необходимо заключить договор, предусматривающий обмен сертификатами. Сертификат представляет собой документ, связывающий личностные данные владельца и его открытый ключ. В бумажном виде он должен содержать рукописные подписи уполномоченных лиц и печати.

В системах, где отсутствует возможность предварительного личного контакта партнёров, необходимо использовать цифровые сертификаты, выданные и заверенные ЭП доверенного посредника – удостоверяющего или сертификационного центра.

На предварительном этапе каждый из партнёров лично посещает ЦС и получает личный сертификат – своеобразный электронный аналог гражданского паспорта (рис. 3.4).

После посещения ЦС каждый из партнёров становится

Этот сертификат ключа проверки ЭП подписан на «секретном» ключе ЦС, поэтому любой обладатель «открытого» ключа ЦС может проверить его подлинность. Таким образом, использование сертификата ключа проверки ЭП предполагает следующую схему электронного взаимодействия партнёров. Один из партнёров посылает другому собственный сертификат, полученный из ЦС, и сообщение, подписанное ЭП. Получатель сообщения осуществляет проверку подлинности сертификата партнёра, которая включает:

- проверку доверия эмитенту сертификата и срока его действия;
- проверку ЭП эмитента под сертификатом;
- проверку аннулирования сертификата.

В случае, если сертификат партнёра не утратил свою силу, а ЭП используется в отношениях, в которых она имеет юридическое значение, открытый ключ партнёра извлекается из сертификата. На основании этого открытого ключа может быть проверена ЭП партнёра под ЭД.

Важно отметить, что в соответствии с Федеральным законом «Об электронной подписи» подтверждением подлинности ЭП в ЭД является положительный результат проверки соответствующим сертифицированным средством ЭП с использованием сертификата ключа подписи.

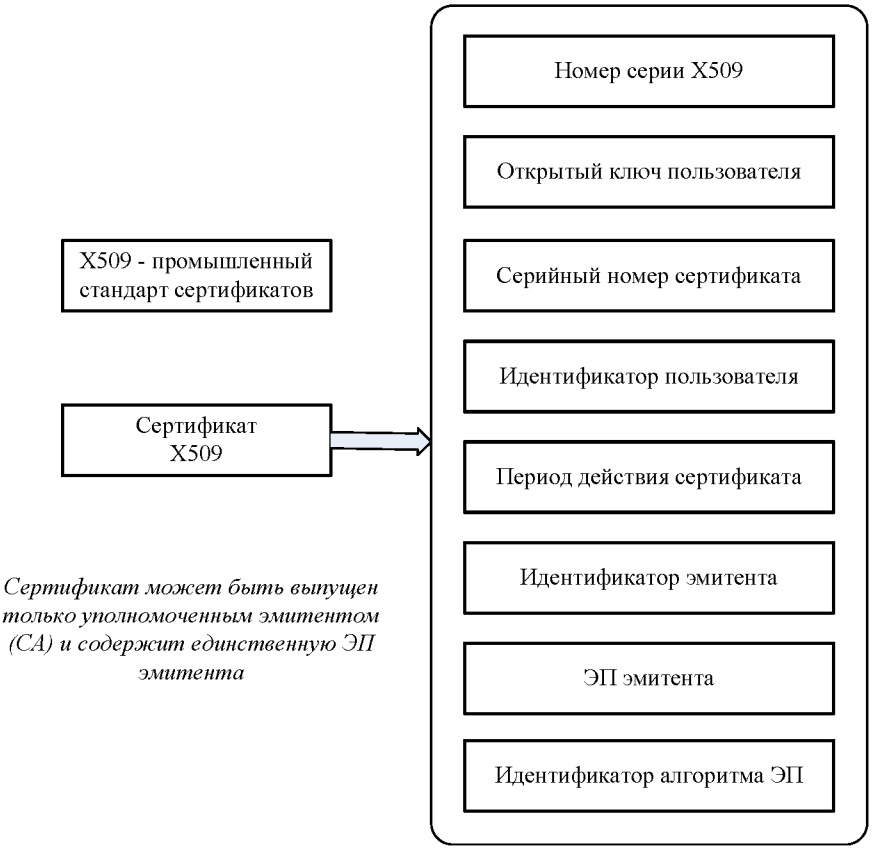

Рис. 3.4. Сертификат X509

ЦС, обеспечивая безопасность взаимодействия партнёров, выполняет следующие функции:

- создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям);
- устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;
- выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или

обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

- ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее – реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;
- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;
- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;
- осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;
- осуществляет иную связанную с использованием электронной подписи деятельность.

В ЦС создаются условия безопасного хранения секретных ключей на дорогом и хорошо защищенном оборудовании, а также условия администрирования доступа к секретным ключам.

Регистрация каждой ЭП осуществляется на основе заявления, содержащего сведения, необходимые для выдачи сертификата, а также сведения, необходимые для идентификации ЭП обладателя и передачи ему сообщений. Заявление подписывается собственноручной подписью обладателя ЭП, содержащиеся в нем сведения подтверждаются предъявлением соответствующих документов. При регистрации проверяется уникальность открытых ключей ЭП в реестре и архиве ЦС.

Важно отметить, что в соответствии с законом «Об электронной подписи» владелец сертификата проверки ключа ЭП – исключительно физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа и которое владеет соответствующим закрытым ключом ЭП.

Кроме того, сертификат ключа подписи – электронный документ с ЭП уполномоченного лица (УЛ) удостоверяющего центра. Поэтому

устойчивость всей инфраструктуры открытых ключей связана с сертификатом, выданным на уполномоченное физическое лицо. Смена работы или завершение земного пути уполномоченного лица УЦ приведёт к компрометации всех сертификатов, сформированных данным УЦ.

При регистрации в ЦС оформляются на бумажных носителях два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями обладателя ЭЦП и уполномоченного лица удостоверяющего центра и печатью удостоверяющего центра. Один экземпляр выдаётся обладателю ЭП, второй остаётся в удостоверяющем центре.

В реальных системах каждым партнёром может использоваться несколько сертификатов, выданных различными ЦС. Различные ЦС могут быть объединены инфраструктурой открытых ключей или PKI (PKI - Public Key Infrastructure). ЦС в рамках PKI обеспечивает не только хранение сертификатов, но и управление ими (выпуск, отзыв, проверку доверия). Наиболее распространённая модель PKI – иерархическая. Фундаментальное преимущество этой модели состоит в том, что проверка сертификатов требует доверия только относительно малому числу корневых ЦС. В то же время эта модель позволяет иметь различное число ЦС, выдающих сертификаты.

3.6 Контроль целостности программных и информационных ресурсов

Механизм контроля целостности ресурсов системы предназначен для своевременного обнаружения модификации ресурсов системы. Он позволяет обеспечить правильность функционирования системы защиты и целостность обрабатываемой информации.

Контроль целостности программ, обрабатываемой информации и средств защиты, с целью обеспечения неизменности программной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной корректировки информации должен обеспечиваться:

- средствами разграничения доступа, запрещающими модификацию или удаление защищаемого ресурса;
- средствами сравнения критичных ресурсов с их эталонными копиями (и восстановления в случае нарушения целостности);
- средствами подсчета контрольных сумм (сигнатур, имитовставок и т.п.);
- средствами электронной цифровой подписи.

Контролируемые ресурсы:
- файлы и каталоги;
- элементы реестра;
- сектора дисков.

Контролируемые параметры:
- содержимое ресурса;
- списки управления доступом;
- атрибуты файлов.

Алгоритмы контроля:
- сравнение с эталоном;
- вычисление контрольных сумм (сигнатур);
- формирование ЭП и имитовставок.

Время контроля:
- до загрузки ОС;
- при наступлении событий;
- по расписанию.

3.7 Обнаружение атак

Обнаружение вторжений (атак) – это процесс мониторинга событий, происходящих в АС, с целью поиска признаков нарушений безопасности.

Выше было сказано, что нарушением безопасности (просто нарушением или атакой) называется реализация угрозы безопасности (наступление соответствующего события).

Например, просматривая журнал регистрации событий и обнаружив там большое количество неудачных попыток аутентификации за короткий промежуток времени, можно сделать вывод, что произошла атака «подбор пароля». В данном случае определённое число неудачных попыток аутентификации за определённый период времени – это и есть признак нарушения безопасности.

Теоретически, поиск признаков атак может выполняться вручную (в этом случае он сводится к рассмотренному выше анализу собранной средствами регистрации информации, что, в принципе, позволяет выявить факты совершения нарушений), но суть механизма обнаружения атак состоит именно в автоматизации данного процесса. Таким образом, система (средство) обнаружения вторжений (атак) – это программное (или программно-аппаратное) обеспечение, автоматизирующее процесс обнаружения атак.

Считается, что впервые механизм обнаружения атак был «обозначен» в работе Джеймса Андерсена (James Anderson) «Computer Security Threat Monitoring and Surveillance».

3.8 Управление механизмами защиты

Конкуренция в области разработки средств защиты компьютерных систем неизбежно приводит к унификации перечня общих требований к таким средствам. Одним из пунктов в таком унифицированном списке практически всегда является требование наличия средств управления всеми имеющимися защитными механизмами. К сожалению, кроме того, что средства управления в системе должны быть, в лучшем случае для вычислительных сетей можно встретить лишь уточнение о необходимости обеспечения централизованного удалённого контроля и управления защитными механизмами. Разработчики систем защиты основное внимание уделяют реализации самих защитных механизмов, а не средств управления ими. Такое положение дел свидетельствует о незнании или непонимании и недооценке проектировщиками и разработчиками большого числа психологических и технических препятствий, возникающих при внедрении разработанных систем защиты. Успешно преодолеть эти препятствия можно только, обеспечив необходимую гибкость управления средствами защиты.

Недостаточное внимание к проблемам и пожеланиям заказчиков, к обеспечению удобства работы администраторов безопасности по управлению средствами защиты на всех этапах жизненного цикла компьютерных систем часто является основной причиной отказа от использования конкретных средств защиты.

Опыт внедрения и сопровождения систем разграничения доступа в различных организациях позволяет указать на ряд типовых проблем, возникающих при установке, вводе в строй и эксплуатации средств разграничения доступа к ресурсам компьютерных систем, а также предложить подходы к решению этих проблем.

В настоящее время в большинстве случаев установка средств защиты производится на уже реально функционирующие АС заказчика. Защищаемая АС используется для решения важных прикладных задач, часто в непрерывном технологическом цикле, и её владельцы и пользователи крайне негативно относятся к любому, даже кратковременному перерыву в её функционировании для установки и настройки средств защиты или частичной потере работоспособности АС вследствие некорректной работы средств защиты.

Внедрение средств защиты осложняется ещё и тем, что правильно настроить данные средства с первого раза обычно не представляется возможным. Это, как правило, связано с отсутствием у заказчика полного детального списка всех подлежащих защите аппаратных, программных и информационных ресурсов системы и готового непротиворечивого перечня прав и полномочий каждого пользователя АС по доступу к ресурсам системы.

Поэтому этап внедрения средств защиты информации обязательно в той или иной мере включает действия по первоначальному выявлению, итеративному уточнению и соответствующему изменению настроек средств защиты. Эти действия должны проходить для владельцев и пользователей системы как можно менее болезненно.

Очевидно, что те же самые действия неоднократно придётся повторять администратору безопасности и на этапе эксплуатации системы каждый раз при изменениях состава технических средств, программного обеспечения, персонала и пользователей и т.д. Такие изменения происходят довольно часто, поэтому средства управления системы защиты должны обеспечивать удобство осуществления необходимых при этом изменений настроек системы защиты. Такова «диалектика» применения средств защиты. Если система защиты не учитывает этой диалектики, не обладает достаточной гибкостью и не обеспечивает удобство перенастройки, то такая система очень быстро становится не помощником, а обузой для всех, в том числе и для администраторов безопасности, и обречена на отторжение.

Дня поддержки и упрощения действий по настройке средств защиты в системе защиты необходимо предусмотреть следующие возможности:

- выборочное подключение имеющихся защитных механизмов, что обеспечивает возможность реализации режима постепенного поэтапного усиления степени защищенности АС;
- так называемый «мягкий» режим функционирования средств защиты, при котором несанкционированные действия пользователей (действия с превышением полномочий) фиксируются в системном журнале обычным порядком, но не пресекаются (то есть не запрещаются системой защиты). Этот режим позволяет выявлять некорректности настроек средств защиты (и затем производить соответствующие их корректировки) без нарушения работоспособности АС и существующей технологии обработки информации;
- возможности по автоматизированному изменению полномочий пользователя с учетом информации, накопленной в системных журналах (при работе как в «мягком», так и обычном режимах).

С увеличением масштаба защищаемой АС усиливаются требования к организации удалённого управления средствами защиты. Поэтому те решения, которые приемлемы для одного автономного компьютера или небольшой сети из 10 - 15 рабочих станций, совершенно не устраивают обслуживающий персонал (в том числе и администраторов безопасности) больших сетей, объединяющих несколько сотен рабочих станций.

Для решения проблем управления средствами защиты в больших сетях в системе необходимо предусмотреть следующие возможности:

- должны поддерживаться возможности управления механизмами защиты как централизованно (удаленно, с рабочего места администратора безопасности сети), так и децентрализованно (непосредственно с конкретной рабочей станции). Причем любые изменения настроек защитных механизмов, произведенные централизованно, должны автоматически распространяться на все рабочие станции, которых они касаются (независимо от состояния рабочей станции на момент внесения изменений в центральную базу данных). Аналогично, часть изменений, произведенных децентрализованно, должна быть автоматически отражена в центральной базе данных защиты и при необходимости также разослана на все другие станции, которых они касаются. Например, при смене своего пароля пользователем, осуществленной на одной из рабочих станций, новое значение пароля этого пользователя должно быть отражено в центральной базе данных защиты сети, а также разослано на все рабочие станции, на которых данному пользователю разрешено работать;
- управление механизмами защиты конкретной станции должно осуществляться независимо от активности данной станции, то есть независимо от того, включена она в данный момент времени и работает ли на ней какой-то пользователь или нет. После включения неактивной станции все изменения настроек, касающиеся ее механизмов защиты, должны быть автоматически перенесены на нее;
- в крупных АС процедура замены версий программ средств защиты (равно как и любых других программ) требует от обслуживающего персонала больших трудозатрат и связана с необходимостью обхода всех рабочих станций для получения к ним непосредственного доступа. Проведение таких замен может быть вызвано как необходимостью устранения обнаруженных ошибок в программах, так и потребностью совершенствования и развития системы (установкой новых улучшенных версий программ);
- для больших АС особую важность приобретает оперативный контроль за состоянием рабочих станций и работой пользователей в

сети. Поэтому система защиты в свой состав должна включать подсистему оперативного контроля состояния рабочих станций сети и слежения за работой пользователей.

Увеличение количества рабочих станций и использование новых программных средств, включающих большое количество разнообразных программ (например MS Windows), приводит к существенному увеличению объёма системных журналов регистрации событий, накапливаемых системой защиты. Объем зарегистрированной информации становится настолько велик, что администратор уже физически не может полностью проанализировать все системные журналы за приемлемое время.

Для облегчения работы администратора с системными журналами в системе должны быть предусмотрены следующие возможности:

- подсистема реализации запросов, позволяющая выбирать из собранных системных журналов данные об определенных событиях (по имени пользователя, дате, времени происшедшего события, категории происшедшего события и т.п.). Естественно, такая подсистема должна опираться на системный механизм обеспечения единого времени событий;
- возможность автоматического разбиения и хранения системных журналов по месяцам и дням в пределах заданного количества последних дней. Причем во избежание переполнения дисков по истечении установленного количества дней просроченные журналы, если их не удалил администратор, должны автоматически уничтожаться;
- в системе защиты должны быть предусмотрены механизмы семантического сжатия данных в журналах регистрации, позволяющие укрупнять регистрируемые события без существенной потери их информативности. Например, заменять все многократно повторяющиеся в журнале события, связанные с выполнением командного файла autoexec.bat, одним обобщенным;
- желательно также иметь в системе средства автоматической подготовки отчетных документов установленной формы о работе станций сети и имевших место нарушениях. Такие средства позволили бы существенно снять рутинную нагрузку с администрации безопасности.

3.9 Страхование информационных рисков

Утрата или искажение данных в результате компьютерных преступлений и мошенничества, несанкционированных действий третьих лиц, воздействия программ-вирусов, отказов и сбоев аппаратных

средств, ошибок программного обеспечения, неквалифицированных и преднамеренных действий обслуживающего персонала и других причин способны повлечь за собой значительный материальный ущерб. Одним из эффективных методов компенсации ущерба, наступившего в результате вышеназванных событий, является страхование.

В соответствии с Федеральным законом от 27.11.1992 № 4015-1 «Об организации страхового дела в Российской Федерации» страхование представляет собой отношения по защите интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов (страховых премий).

Страховой случай

К страховым случаям можно отнести уничтожение или повреждение застрахованных активов вследствие наступления следующих событий:

- действие вирусов, червей и троянских коней;
- компьютерные атаки со стороны внешних злоумышленников (хакеров);
- хищение денежных средств в электронной форме внешними злоумышленниками. Такое хищение может происходить как с помощью сфальсифицированного финансового поручения, посланного электронным способом страхователю или от имени страхователя, так и путем модификации программного обеспечения и даже путем непосредственного ввода команд;
- несанкционированные действия со стороны собственных сотрудников организации;
- сбои систем по причине ошибок при их проектировании, разработке, создании, установке, настройке и эксплуатации;
- страховым случаем также является временное прекращение деятельности вследствие любого из вышеперечисленных страховых случаев.

Принятие решения об использовании страхования

При выборе страхования как метода защиты информации проводится оценка рисков. После принятия решения об использовании страхования в качестве метода защиты информации специалист по защите информации (информационной безопасности) должен составить справку по объектам, подлежащим страхованию, рискам и возможным потерям, по вероятности реализации рисков и по размерам возможных убытков и принять решение по поводу вида страхования, типа договора, условий страхования и т.п.

После выбора вида страхования необходимо заключить договор со страховой компанией.

Процедура страхования информационных рисков

Этапами процедуры страхования информационных рисков являются:

- переговоры, определяющие условия страхования;
- разработка и согласование предложений по страхованию;
- проведение экспертизы страхователя;
- выполнение рекомендаций, полученных в результате экспертизы;
- подписание договора о страховании.

Непременным условием страхования информационных рисков является проведение специальной экспертизы по анализу рисков страхового объекта. Эта экспертиза, так называемая «сюрвей» (от английского «survey» – «осмотр»), проводится экспертами в области информационной безопасности, которые и выносят свой вердикт об уровне защищенности страхуемой компании.

Особенность этой экспертизы в том, что совершается она независимыми специалистами, не работающими ни в страхуемой, ни в страховой компании. Считается, что это позволит страховой компании получить более точную картину о страхователе, а последнему – оценить свою систему защиты с точки зрения независимого незаинтересованного эксперта. Надо помнить, что привлечение российских экспертов обходится в несколько раз дешевле их западных коллег, предпочитающих почасовую оплату труда. Половина стоимости такого сюрвея компенсируется страховой компании при заключении соответствующего договора страхования.

Параметры, влияющие на ставку страхования

К параметрам, влияющим на ставку страхования, относят:

- стоимость застрахованных ресурсов;
- используемые средства защиты. Чем известнее система защиты, тем ниже ставка страхования;
- статистика атак для аналогичных организаций отрасли.

4 ПРОГРАММНО-АППАРАТНАЯ ЗАЩИТА ИНФОРМАЦИИ

4.1 Межсетевые экраны

Межсетевой экран (МЭ), или сетевой экран – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача – не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации. Некоторые сетевые экраны также позволяют осуществлять трансляцию адресов — динамическую замену внутрисетевых (серых) адресов или портов на внешние, используемые за пределами ЛВС.

В зависимости от уровня, на котором происходит контроль доступа, существует разделение на сетевые экраны, работающие на:

- сетевом уровне, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором;
- сеансовом уровне (также известные как stateful) — отслеживающие сеансы между приложениями, не пропускающие пакеты нарушающих спецификации TCP/IP, часто используемых в злонамеренных операциях — сканировании ресурсов, взломах через неправильные реализации TCP/IP, обрыв/замедление соединений, инъекция данных;
- уровне приложений, фильтрация на основании анализа данных приложения, передаваемых внутри пакета. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации на основании политик и настроек.

Эти категории можно рассматривать как базовые компоненты реальных межсетевых экранов. Лишь немногие межсетевые экраны включают лишь одну из перечисленных категорий. Тем не менее эти

компоненты отражают ключевые возможности, отличающие межсетевые экраны друг от друга.

В зависимости от охвата контролируемых потоков данных сетевые экраны делятся на:

- традиционный сетевой (или межсетевой) экран — программа (или неотъемлемая часть операционной системы) на шлюзе (сервере, передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями;
- персональный сетевой экран — программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

МЭ поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный МЭ удобно представить в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI.

Чаще всего комплексный экран функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели. Соответственно, различают такие неделимые МЭ (рис. 4.1), как:

- фильтрующий маршрутизатор;
- шлюз сеансового уровня (экранирующий транспорт);
- шлюз прикладного уровня (экранирующий шлюз);
- шлюз уровня приложений.

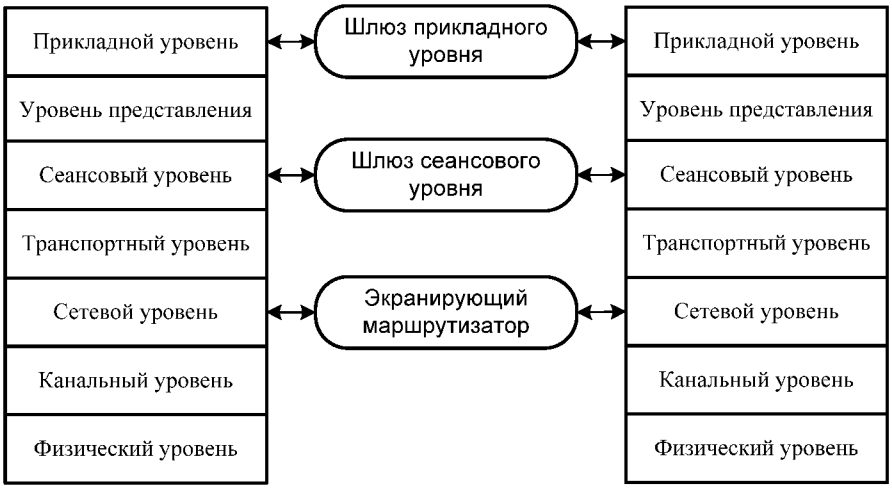

Рис. 4.1. Типы межсетевых экранов

Фильтрующий маршрутизатор представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов.

Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы следующих полей заголовка пакета:

- IP-адрес отправителя;
- IP-адрес получателя;
- порт отправителя;
- порт получателя.

Некоторые маршрутизаторы проверяют, с какого сетевого интерфейса маршрутизатора пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации.

Фильтрация может быть реализована различными способами для блокирования соединений с определенными компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех компьютеров и сетей, которые считаются враждебными или ненадежными.

Правила фильтрации пакетов формулируются сложно, к тому же обычно не существует средств для проверки их корректности, кроме медленного ручного тестирования. При этом в отсутствие фильтрующего маршрутизатора средств протоколирования (если правила фильтрации пакетов все-таки позволят опасным пакетам пройти через маршрутизатор) такие пакеты не смогут быть выявлены до обнаружения последствий проникновения. Даже если администратору сети удастся создать эффективные правила фильтрации, их возможности останутся ограниченными. Например, администратор задает правило, в соответствии с которым маршрутизатор будет отбраковывать все пакеты с неизвестным адресом отправителя. Однако в данном случае хакер для проникновения внутрь защищенной сети может осуществить атаку, которую называют подменой адреса. В таких условиях фильтрующий маршрутизатор не сумеет отличить поддельный пакет от настоящего и пропустит его.

К положительным качествам фильтрующих маршрутизаторов можно отнести следующие:

- сравнительно невысокая стоимость;
- гибкость в определении правил фильтрации;
- небольшая задержка при прохождении пакетов.

Недостатки фильтрующих маршрутизаторов:

- внутренняя сеть видна (маршрутизируется) из сети Интернет;

- правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP;
- при нарушении работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными.

Шлюз сеансового уровня представляет собой транслятор TCP-соединения. Шлюз принимает запрос авторизованного клиента на конкретные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с местом назначения (внешним хостом). После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации. Как правило, пункт назначения задается заранее, в то время как источников может быть много. Используя различные порты, можно создавать разнообразные конфигурации соединений. Данный тип шлюза позволяет создать транслятор TCP-соединения для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису и сбор статистики по его использованию.

Шлюз следит за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом, определяя, является ли запрашиваемый сеанс связи допустимым. Чтобы выявить допустимость запроса на сеанс связи, шлюз выполняет следующую процедуру. Когда авторизованный клиент запрашивает некоторый сервис, шлюз принимает этот запрос, проверяя, удовлетворяет ли данный клиент базовым критериям фильтрации. Затем, действуя от имени клиента, шлюз устанавливает соединение с внешним хостом и следит за выполнением процедуры квитирования связи по протоколу TCP. Эта процедура состоит из обмена TCP-пакетами, которые помечаются флагами SYN (синхронизировать) и ACK (подтвердить).

Первый пакет сеанса TCP, помеченный флагом SYN и содержащий произвольное число, например 500, является запросом клиента на открытие сеанса. Внешний хост, получивший этот пакет, посылает в ответ другой, помеченный флагом ACK и содержащий число на единицу большее, чем в принятом пакете (в нашем случае 501), подтверждая тем самым прием пакета SYN от клиента.

Далее осуществляется обратная процедура: хост посылает клиенту пакет SYN с исходным числом, например 700, а клиент подтверждает его получение передачей пакета ACK, содержащего число 701. На этом процесс квитирования связи завершается.

Шлюз сеансового уровня признает завершенное соединение допустимым только в том случае, если при выполнении процедуры

квитирования связи флаги SYN и ACK, а также числа, содержащиеся в TCP-пакетах, оказываются логически связанными между собой.

После того как шлюз определил, что доверенный клиент и внешний хост являются авторизованными участниками сеанса TCP, и проверил его допустимость, он устанавливает соединение. Начиная с этого момента шлюз копирует и перенаправляет пакеты туда и обратно, не проводя никакой фильтрации. Он поддерживает таблицу установленных соединений, пропуская данные, которые относятся к одному из сеансов связи, зафиксированных в данной таблице. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы и разрывает сеть, использовавшуюся в текущем сеансе.

Недостатком шлюзов сеансового уровня является отсутствие проверки содержимого передаваемых пакетов, что дает возможность нарушителю проникнуть через такой шлюз.

Шлюз прикладного уровня, называемый также *экранирующим шлюзом*, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает наиболее надежную защиту межсетевых взаимодействий. Защитные функции прикладного шлюза, как и шлюза сеансового уровня, относятся к функциям посредничества. Однако шлюз прикладного уровня, в отличие от шлюза сеансового уровня, может выполнять существенно большее количество функций защиты, к которым относятся следующие:

- идентификация и аутентификация пользователей при попытке установления соединений через МЭ;
- проверка подлинности информации, передаваемой через шлюз;
- разграничение доступа к ресурсам внутренней и внешней сетей;
- фильтрация и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;
- регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов;
- кэширование данных, запрашиваемых из внешней сети.

Поскольку функции шлюза прикладного уровня относятся к функциям посредничества, этот шлюз представляет собой универсальный компьютер, на котором функционируют программные посредники (экранирующие агенты) — по одному для каждого обслуживаемого прикладного протокола (HTTP, FTP, SMTP, NNTP и др.). Программный посредник (application proxy) каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе.

Шлюз прикладного уровня перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию, т. е. функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью (рис. 4.2).

Посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня. Во-первых, посредники прикладного шлюза связаны с конкретными приложениями (программными серверами), во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели OSI.

Шлюзы прикладного уровня используют в качестве посредников специально разработанные для этой цели программные серверы конкретных служб TCP/IP – серверы HTTP, FTP, SMTP, NNTP и др. Эти программные серверы функционируют на МЭ в резидентном режиме и реализуют функции защиты, относящиеся к соответствующим службам TCP/IP.

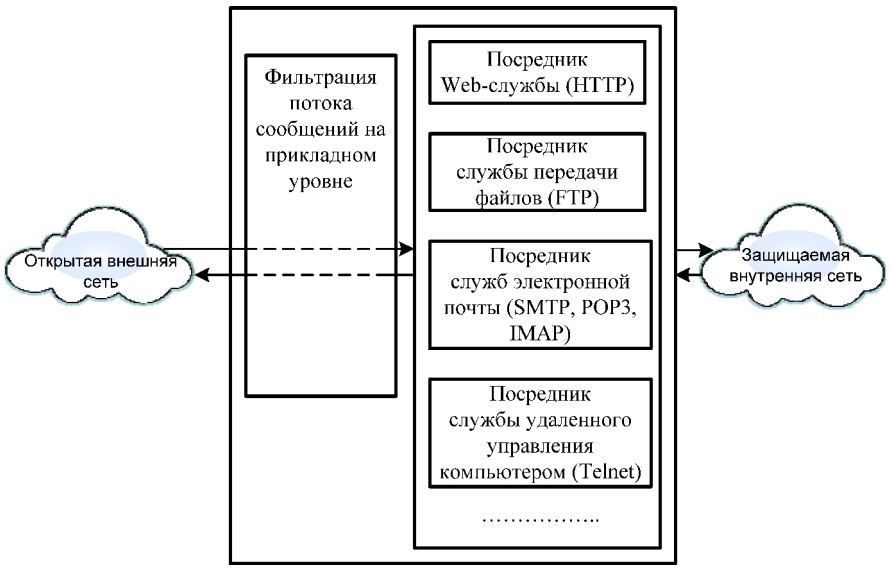

Рис. 4.2. Схема функционирования шлюза прикладного уровня

Шлюз прикладного уровня обладает следующими достоинствами:

- обеспечивает высокий уровень защиты локальной сети благодаря возможности выполнения большинства функций посредничества;

- защита на уровне приложений позволяет осуществлять большое число дополнительных проверок, уменьшая тем самым вероятность проведения успешных атак, возможных из-за недостатков программного обеспечения;
- при нарушении его работоспособности блокируется сквозное прохождение пакетов между разделяемыми сетями, в результате чего безопасность защищаемой сети не снижается из-за возникновения отказов.

К недостаткам шлюза прикладного уровня относятся:

- высокие требования к производительности и ресурсоемкости компьютерной платформы;
- отсутствие «прозрачности» для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий.

4.2 Виртуальные частные сети

Виртуальная частная сеть (англ. *Virtual Private Network* – VPN) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрованию, аутоидентификации, инфраструктуры публичных ключей, средствам для защиты от повторов и изменения передаваемых по логической сети сообщений).

По назначению VPN-сети можно разделить на:

- Intranet VPN.

Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи;

- Remote Access VPN.

Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона или интернет-киоска;

- Extranet VPN.

Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации;

- Internet VPN.

Используется для предоставления доступа к интернету провайдерами, обычно в случае если по одному физическому каналу подключаются несколько пользователей;

- Client/Server VPN.

Он обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, но, вместо разделения трафика, используется его шифрование.

VPN-соединение всегда состоит из канала типа точка-точка, также известного под названием туннель. Туннель создается в незащищенной сети, в качестве которой чаще всего выступает Интернет. Соединение точка-точка подразумевает, что оно всегда устанавливается между двумя компьютерами, которые называются узлами или peers. Каждый peer отвечает за шифрование данных до того, как они попадут в туннель, и расшифровку этих данных после того, как они туннель покинут.

Хотя VPN-туннель всегда устанавливается между двумя точками, каждый peer может устанавливать дополнительные туннели с другими узлами. Для примера, когда трем удаленным станциям необходимо связаться с одним и тем же офисом, будет создано три отдельных VPN-туннеля к этому офису. Для всех туннелей peer на стороне офиса может быть одним и тем же. Это возможно благодаря тому, что узел может шифровать и расшифровывать данные от имени всей сети, как это показано на рис. 4.3:

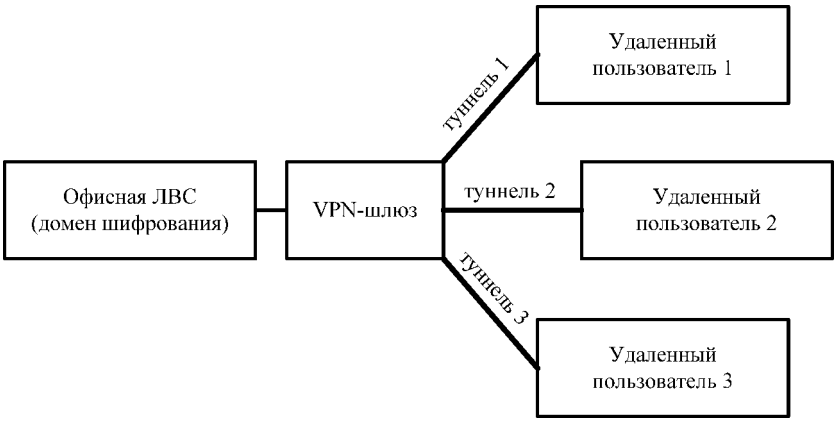

Рис. 4.3. VPN-шлюз подключения удаленных пользователей к офисной ЛВС

В этом случае VPN-узел называется VPN-шлюзом, а сеть за ним – доменом шифрования (encryption domain). Использование шлюзов удобно по нескольким причинам. Во-первых, все пользователи должны пройти через одно устройство, которое облегчает задачу управления политикой безопасности и контроля входящего и исходящего трафика сети. Во-вторых, персональные туннели к каждой рабочей станции, к которой пользователю надо получить доступ, очень быстро станут неуправляемыми (так как туннель – это канал типа точка-точка). При наличии шлюза пользователь устанавливает соединение с ним, после чего пользователю открывается доступ к сети (домену шифрования).

Интересно отметить, что внутри домена шифрования самого шифрования не происходит. Причина в том, что эта часть сети считается безопасной и находящейся под непосредственным контролем в противоположность Интернет. Это справедливо и при соединении офисов с помощью VPN-шлюзов. Таким образом гарантируется шифрование только той информации, которая передается по небезопасному каналу между офисами. Рис. 4.4. показывает VPN, соединяющую два офиса.

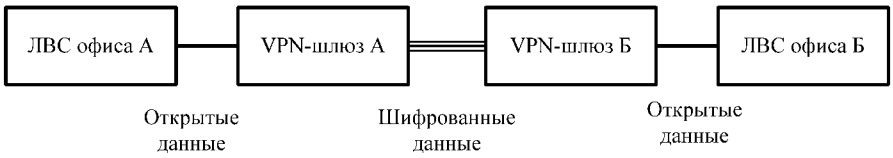

Рис. 4.4. Защищенная сеть на основе незащищенной

Сеть А считается доменом шифрования VPN-шлюза А, а сеть В – доменом шифрования VPN – шлюза В, соответственно. Когда пользователь сети А изъявляет желание отправить данные в сеть В, VPN – шлюз А зашифрует их и отошлет через VPN-туннель. VPN – шлюз В расшифрует информацию и передаст получателю в сети В.

Всякий раз, когда соединение сетей обслуживают два VPN-шлюза, они используют режим туннеля. Это означает, что шифруется весь пакет IP, после чего к нему добавляется новый IP-заголовок. Новый заголовок содержит IP-адреса двух VPN-шлюзов, которые и увидит пакетный сниффер при перехвате. Невозможно определить компьютер-источник в первом домене шифрования и компьютер-получатель во втором домене.

Посмотрите на рисунок 4.3, иллюстрирующий типичное использование VPN, которое позволяет удаленным пользователям с переносными компьютерами и пользователям, работающим из дома, иметь доступ к офисной сети. Чтобы эта схема заработала, пользователь должен иметь установленное ПО – VPN-клиент, который обеспечит создание VPN-туннеля к удаленному VPN-шлюзу. По сценарию используется режим туннеля, так как пользователь хочет получить доступ к ресурсам домена, а не самого шлюза. Единственной случай, когда включается режим транспорта – это если одному компьютеру нужно получить доступ к другому непосредственно.

Существует много вариантов VPN-шлюзов и VPN-клиентов. Это может быть аппаратное устройство или программное обеспечение, которое устанавливается на маршрутизаторах или на ПК. Скажем, ОС FreeBSD поставляется вместе с ПО для создания VPN-шлюза и для настройки VPN-клиента. Свои VPN-решения существуют и для ПО компании Microsoft.

Независимо от используемого ПО, все VPN работают по следующим принципам:

1. Каждый из узлов идентифицирует друг друга перед созданием туннеля, чтобы удостовериться, что шифрованные данные будут отправлены на нужный узел.

2. Оба узла требуют заранее настроенной политики, указывающей, какие протоколы могут использоваться для шифрования и обеспечения целостности данных.

3. Узлы сверяют политики, чтобы договориться об используемых алгоритмах; если это не получается, то туннель не устанавливается.

4. Как только достигнуто соглашение по алгоритмам, создается ключ, который будет использован в симметричном алгоритме для шифрования/расшифровки данных.

Есть несколько стандартов, регламентирующих вышеописанное взаимодействие, такие как L2TP, PPTP и IPSec. В настоящее время IPSec – наиболее широко поддерживаемый стандарт, поэтому далее он будет рассмотрен подробнее.

Стандарт IPSec был разработан для повышения безопасности IP-протокола. Это достигается за счет дополнительных протоколов, добавляющих к IP-пакету собственные заголовки. Т.к. IPSec – стандарт Интернет, то для него существуют RFC (Requests For Comments).

Приведем краткое описание каждого дополнительного протокола.

AH (Authentication Header) – протокол заголовка идентификации. Обеспечивает целостность путем проверки того, что ни один бит в защищаемой части пакета не был изменен во время передачи. Не будем вдаваться в подробности, какая часть пакета защищается и где находятся данные AH-заголовка, так как это зависит от используемого типа шифрования и в деталях, с диаграммами описывается в соответствующем RFC. Отметим лишь, что использование AH может вызвать проблемы, например, при прохождении пакета через NAT-устройство. NAT меняет IP-адрес пакета, чтобы, например, разрешить доступ в Интернет с закрытого локального адреса. Так как пакет в таком случае изменится, контрольная сумма AH станет неверной. Также стоит отметить, что AH разрабатывался только для обеспечения целостности. Он не гарантирует конфиденциальности путем шифрования содержимого пакета.

ESP (Encapsulating Security Protocol) – инкапсулирующий протокол безопасности, который обеспечивает и целостность, и конфиденциальность. В режиме транспорта ESP-заголовок находится между оригинальным IP-заголовком и заголовком TCP или UDP. В режиме туннеля заголовок ESP размещается между новым IP-заголовком и полностью зашифрованным оригинальным IP-пакетом.

Так как оба протокола – AH и ESP – добавляют собственные заголовки, они имеют свой ID протокола, по которому можно определить, что последует за заголовком IP. Каждый тип заголовка имеет собственный номер. Например, для TCP – это 6, а для UDP – 17. При работе через firewall важно не забыть настроить фильтры, чтобы пропускать пакеты с ID AH-и/или ESP-протокола. Для AH номер ID - 51, а ESP имеет ID протокола равный 50. При создании правила не перепутайте случайно ID протокола с номером порта.

Третий протокол, используемый IPSec, – это IKE или Internet Key Exchange protocol. Как следует из названия, он предназначен для обмена ключами между двумя узлами VPN. Несмотря на то, что генерировать ключи можно вручную, лучшим и более масштабируемым

вариантом будет автоматизация этого процесса с помощью IKE. Помните, что ключи должны часто меняться, и вам наверняка не хочется полагаться на свою память, чтобы найти время для совершения этой операции вручную. Главное – не забудьте настроить правило на файрволе для UDP-порта с номером 500, так как именно этот порт используется IKE.

Четвертый используемый протокол – SA (Security Association). SA можно приближенно перевести как «связь или ассоциация безопасности» – это термин IPSec для обозначения соединения. При настроенном VPN для каждого используемого протокола создается одна SA-пара (то есть одна для AH и одна для ESP). SA создаются парами, так как каждая SA – это однонаправленное соединение, а данные необходимо передавать в двух направлениях. Полученные SA-пары хранятся на каждом узле. Если ваш узел имеет SA, значит VPN-туннель был установлен успешно.

SA – это ассоциация между двумя или более узлами, которая описывает, как узлы будут использовать службы безопасности для безопасного соединения.

Так как каждый узел способен устанавливать несколько туннелей с другими узлами, каждый SA имеет уникальный номер, позволяющий определить, к какому узлу он относится. Этот номер называется SPI (Security Parameter Index) или индекс параметра безопасности.

SA хранятся в базе данных с названием – SAD (Security Association Database) или БД ассоциаций безопасности. Каждый узел IPSec также имеет вторую БД – SPD или Security Policy Database (БД политики безопасности). Она содержит настроенную вами политику узла. Большинство VPN-решений разрешают создание нескольких политик с комбинациями подходящих алгоритмов для каждого узла, с которым нужно установить соединение.

Политика включает в себя следующие настройки:

- доступные симметричные алгоритмы для шифрования/расшифровки данных;
- алгоритмы вычисления криптографических контрольных сумм для проверки целостности данных;
- способ идентификации узла (например – предустановленные ключи (pre-shared secrets) или RSA-сертификаты);
- опция использования режима туннеля или режима транспорта;
- какую использовать группу Diffie Hellman;
- как часто проводить переидентификацию узла;
- как часто менять ключ для шифрования данных;
- использовать ли PFS;

- использовать ли AH, ESP или оба вместе.

При создании политики, как правило, возможно создание упорядоченного списка алгоритмов и Diffie Hellman-групп. В таком случае будет использована первая совпавшая на обоих узлах позиция. Запомните, очень важно, чтобы все в политике безопасности позволяло добиться этого совпадения. Если за исключением одной части политики все остальное совпадает, узлы все равно не смогут установить VPN-соединение. При настройке VPN между различными системами уделите время изучению того, какие алгоритмы поддерживаются каждой стороной, чтобы иметь выбор наиболее безопасной политики из возможных.

Установка и поддержка VPN-туннеля происходит в два этапа. На первом этапе (фазе) два узла договариваются о методе идентификации, алгоритме шифрования, хэш-алгоритме и группе Diffie Hellman. Они также идентифицируют друг друга. Все это может пройти в результате обмена тремя нешифрованными пакетами (так называемый агрессивный режим) или через обмен шестью нешифрованными пакетами (стандартный режим – main mode). При успешном завершении операции создается SA первой фазы – Phase 1 SA (также называемый IKE SA) и процесс переходит к фазе два.

На втором этапе генерируются данные ключей, узлы договариваются насчет используемой политики. Этот режим, называемый быстрым режимом (quick mode), отличается от первой фазы тем, что может установиться только после первого этапа, когда все пакеты второй фазы шифруются. Такое положение дел усложняет решение проблем в случае неполадок на второй фазе при успешном завершении первой. Правильное завершение второй фазы приводит к появлению Phase 2 SA или IPSec SA, и на этом установка туннеля считается завершенной.

Когда же это все происходит? Сначала на узел прибывает пакет с адресом назначения в другом домене шифрования, и узел инициирует фазу 1 с тем узлом, который отвечает за другой домен. Допустим, туннель между узлами был успешно установлен и ожидает пакетов. Однако узлам необходимо переидентифицировать друг друга и сравнить политику через определенное время. Это время известно как время жизни Phase One, или IKE SA lifetime. Узлы также должны сменить ключ для шифрования данных через другой отрезок времени, который называется временем жизни Phase Two, или IPSec SA lifetime. Phase Two lifetime короче, чем у первой фазы, так как ключ необходимо менять чаще. Типичное время жизни Phase Two – 60 минут. Для Phase One оно равно 24 часам.

4.3 Гарантированное удаление остаточной информации

Системы гарантированного уничтожения информации (СГУ) используются для гарантированного уничтожения информации с машинных носителей. В большинстве случаев уничтожение осуществляется программной записью поверх удаляемой информации специально выбранных двоичных последовательностей.

Под гарантированным уничтожением понимается физическое удаление информации путём записи поверх неё новых данных (затирающей последовательности).

Способы уничтожения информации делятся на три основные группы:

1. Программные – удаление информации с использованием штатных средств ЭВМ. После удаления ЖД может быть использован.

2. Механические – связанные с механическим повреждением основы ЖД, на которую нанесен магнитный слой.

3. Физические – связанные с физическими принципами цифровой записи и основанные на перестройке структуры магнитного материала на ЖД.

В дальнейшем для простоты восприятия вместо термина гарантированное уничтожение информации будет использоваться термин затирание.

Все программные методы затирания информации можно по степени надежности разделить на 3 способа:

Первый, наиболее простой и часто применяемый способ уничтожения информации на магнитных дисках и полупроводниковых накопителях (твердотельная память) – вместо полной перезаписи диска в загрузочный сектор, основную и резервную таблицы разделов записывается последовательность нулей. Тем самым усложняется доступ к данным, хранящимся на диске. Сами данные не уничтожаются. Полный доступ к информации на диске легко восстанавливается с помощью посекторного чтения. Такой способ обеспечивает наибольшую скорость, но не может использоваться при обработке информации, утечка которой нежелательна.

Второй способ заключается в записи последовательности нулей или единиц в сектора, содержащие уничтожаемую информацию. Программный доступ к перезаписанным данным невозможен. Однако на магнитных дисках существует возможность восстановления информации после перезаписи. В ее основе лежит наличие остаточной намагниченности краевых областей дисковых дорожек, несущей информацию о предыдущих записях.

Для восстановления информации, удаленной этим методом, могут быть применены технологии магнитной силовой микроскопии.

У твердотельной памяти существует возможность записи последовательностей в так называемые «заменённые» блоки. Это обусловлено встроенными схемами контроля изношенности блоков твердотельной памяти и балансирования нагрузки ячеек памяти. Контроллер диска хранит в памяти информацию о том, сколько раз и в какие блоки были записаны данные и при необходимости «меняет» их местами. В этом случае последовательности нулей и единиц, которые должны быть записаны поверх уничтожаемой информации, могут быть записаны в другие блоки и при посекторном сканировании она может быть восстановлена.

Для восстановления также может быть использован метод считывания информации на программаторе непосредственно с микросхемы памяти.

Скорость уничтожения информации значительно ниже, чем в предыдущем способе, и определяется скоростью работы (а именно – скоростью записи) диска.

Третий способ основан на использовании нескольких циклов перезаписи информации. С увеличением числа циклов перезаписи усложняется задача восстановления удаленных данных. Это обуславливается естественным дрейфом пишущей головки магнитного диска каждого следующего цикла. Вероятность перезаписи краевых областей дорожек возрастает. У твердотельной памяти повышается вероятность перезаписи «заменённых» блоков. Следовательно, резко повышается сложность процесса восстановления уничтоженных данных.

Однако полной гарантии необратимого уничтожения информации нет и в этом случае, поскольку программно невозможно управлять траекторией движения блока головок диска и процессом перемагничивания битовых интервалов. Также уничтожение информации затруднено из-за сложности оценки факторов, оказывающих влияние на точность позиционирования головок.

У твердотельных дисков существует возможность записи информации в резервные блоки, которые при перезаписи, возможно, будут не затронуты.

Недостатком данного способа является низкая скорость уничтожения информации.

В качестве примера реализации современных алгоритмов удаления остаточной информации рассмотрим возможности программного комплекса «СГУ-2»

Программный комплекс «СГУ-2» в своей работе использует несколько методов третьего способа затирания информации и предназначен для уничтожения информации, хранимой на внешних носителях компьютера (жестких дисках, дискетах, flash-дисках). Уничтожаться могут как отдельные файлы, так и всё содержимое носителя целиком. При этом маскирующие последовательности (проходы) подбираются таким образом, чтобы перезаписать каждый битовый интервал в записи максимальное число раз. Выбор метода уничтожения зависит от метода кодирования информации, используемой на целевом носителе.

Под методом затирания понимается набор проходов, каждый из которых определяет последовательность байт, записываемую поверх затираемой информации. Проходы выполняются один за другим.

Каждый пользователь «СГУ-2» имеет возможность задавать свои собственные методы затирания, определяя последовательность проходов. При этом существует возможность не начинать формирование метода с нуля, а составить его на основе одного из встроенных или определённых пользователем ранее методов, исключив, добавив или модифицировав отдельные проходы.

Выбор конкретного метода также зависит от уровня секретности информации, подвергаемой уничтожению. Во многих странах существуют государственные стандарты, строго регламентирующие состав и количество проходов при уничтожении информации. В комплексе заранее предопределены три стандартизованных метода затирания – ГОСТ Р50739-95, US DoD и метод Гутмана.

В методе затирания, определенном по ГОСТ Р50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», говорится, что очистка внешней памяти при ее освобождении должна производиться путем записи в нее маскирующей информации. Количество и содержание проходов не уточняется. В нашем случае включает в себя два прохода, каждый из которых подразумевает запись в затираемую область последовательности нулевых байт.

Метод затирания US DoD, определенный Министерством обороны США, регламентирует троекратную перезапись информации:

1. Запись в каждый байт перезаписываемой области случайно выбранного байта.
2. Запись в каждый байт перезаписываемой области дополнения к нему.
3. Запись в перезаписываемой области последовательности случайно выбранных байт.

Данный метод носит произвольный характер и не учитывает особенностей работы конкретных носителей информации. Министерство обороны США признает этот факт и при уничтожении информации высшей категории секретности запрещает использование программных методов.

Метод Гутмана состоит из 35 проходов, ориентированных на уничтожение записей, закодированных методами MFM и различными распространенными модификациями RLL. Маскирующие последовательности подобраны таким образом, чтобы обеспечить максимально возможное число переключений знака каждого битового интервала. Это значительно затрудняет восстановление перезаписанных данных, поскольку делает нетривиальным раздельное считывание наложенных друг на друга записей.

Комплекс «СГУ-2» выполняет следующие функции:

- действительное уничтожение файлов путем записи по их физическим адресам затирающих последовательностей;
- удаление сведений об имени файла и его физическом расположении из файловой системы;
- затирание незанятых кластеров;
- затирание остаточной информации в последних кластерах файлов;
- многократное и комбинированное выполнение функций затирания;
- глобальное уничтожение информации на томах жестких дисков и гибких магнитных дисков;
- протоколирование всех действий по уничтожению информации;
- тестирование результатов очистки на наличие остаточной информации в указанных областях (в том числе поиск подстрок в кодировках ANSI, OEM, UTF16, UTF8);
- выполнение основных функций очистки или маскирования из командной строки и из контекстного меню оболочки ОС Windows.

5 ОРГАНЫ ДОБЫВАНИЯ ИНФОРМАЦИИ

5.1 Структура системы разведки

Жизненная необходимость в информации для любой государственной или коммерческой структуры вынуждает их расходовать людские, материальные и финансовые ресурсы на ее постоянное добывание. Так как любую работу эффективнее выполняют профессионалы, то эти структуры создают специализированные органы, предназначенные для добывания информации. Такими органами являются органы разведки.

Любое государство создает органы разведки, обеспечивающие руководство страны информацией для принятия им политических, экономических, военных, научно-технических решений в условиях жесткой межгосударственной конкуренции. В зависимости от целей государства, его внешней политики и возможностей структуры органов разведки существенно отличаются. Мощную разведку имеют развитые страны, прежде всего США, Россия, Англия, Германия, Франция, Израиль.

Разведка коммерческих структур (коммерческая разведка) добывает информацию в интересах их успешной деятельности на рынке в условиях острой конкурентной борьбы. Задачи органов коммерческой разведки, их состав и возможности зависят от назначения и капитала фирмы, но принципы добывания информации существенно не отличаются.

В общем случае органы разведки образуют систему разведки с многоуровневой иерархической структурой (рис. 5.1). Необходимость указанных уровней обусловлена объективными процессами добывания информации. В минимальном варианте функции системы добывания информации могут быть реализованы одним или несколькими работникам службы безопасности фирмы.

В органах планирования и управления на основе задач руководства перед разведкой формулируются конкретные задачи, планируются разведывательные операции, привлекаются необходимые силы и средства и осуществляется управление ими.

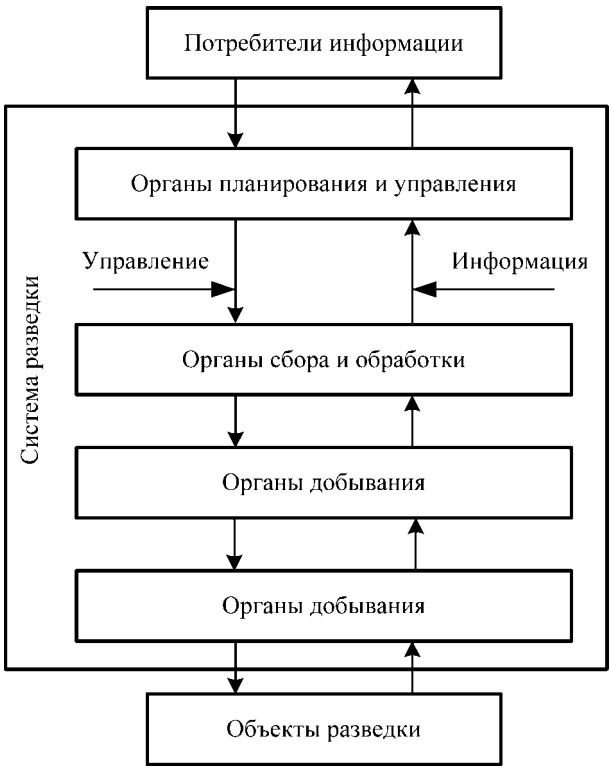

Рис. 5.1. Структура системы разведки

В соответствии с поставленными задачами и планом проведения операции органы добывания обеспечивают разведывательный контакт с источниками информации и получают от них данные и сведения. Редко органам добывания удается получить их в объеме и с качеством, достаточными для ответа на поставленные вопросы. Как правило, добываемые данные и сведения разрозненны и малоинформативны. Поэтому они собираются и обрабатываются соответствующими органами.

За свою историю разведка накопила большой опыт по добыванию информации, в том числе с использованием технических средств. Задачи по добыванию информации инициируют исследования по созданию принципиально новых способов и средств разведки. С этой целью органы разведки ведущих стран имеют мощную научно-производственную базу.

5.2 Основные направления действий разведок иностранных государств

Основными направлениями действий **разведок иностранных государств** являются:

- состояние военно-экономического и научно-технического потенциалов других государств, прежде всего потенциальных противников, и прогнозирование их развития;
- размещение военно-технических объектов, их производственные мощности, характер и распределение выпускаемой продукции:
- содержание и характер работ, ведущихся в области создания новых видов вооружения и военной техники;
- состав и дислокация группировок войск и сил флота;
- эффективность вооружения и военной техники, их тактико-технические характеристики;
- масштаб проводимых учений, состав привлекаемых на них сил и средств, содержание решаемых на учениях задач;
- принципы построения и технического оснащения систем государственного и военного управления;
- инженерное оборудование континентальных и навигационно-гидрографическое обеспечение океанских театров военных действий;
- наличие топливно-энергетических, рудных, водных, растительных и других природных ресурсов;
- метеорологические условия на территории разведываемых государств;
- выполнение условий международных договоров, прежде всего об ограничении вооружений.

Кроме этих глобальных задач, органы разведки добывают большой объем разнообразной информации, вплоть до состояния здоровья, характера, привычек, стиля мышления политических и военных руководителей зарубежных государств.

5.3 Основные направления действий разведок коммерческих структур

Разведка коммерческих структур (коммерческая разведка) добывает информацию в интересах их успешной деятельности на рынке в условиях острой конкурентной борьбы. Задачи органов коммерческой разведки, их состав и возможности зависят от назначения и капитала фирмы, но принципы добывания информации существенно не

отличаются. Основными предметными областями, представляющими интерес для коммерческой разведки, являются:

- коммерческая философия и деловая стратегия руководителей фирм-конкурентов, их личные и деловые качества;
- научно-исследовательские и конструкторские работы;
- финансовые операции фирм;
- организация производства, в том числе данные о вводе в строй новых, расширении и модернизации существующих производственных мощностей, объединение с другими фирмами;
- технологические процессы при производстве новой продукции, результаты ее испытаний;
- маркетинг фирмы, в том числе режимы поставок, сведения о заказчиках и заключаемых сделках, показатели реализации продукции.

Кроме того, коммерческая разведка занимается:

- изучением и выявлением организаций, потенциально являющихся союзниками или конкурентами;
- добыванием, сбором и обработкой сведений о деятельности потенциальных и реальных конкурентов;
- учетом и анализом попыток несанкционированного получения коммерческих секретов конкурентами;
- оценкой реальных отношений между сотрудничающими и конкурирующими организациями;
- анализом возможных каналов утечки конфиденциальной информации.

Сбор и анализ данных производится также по множеству других вопросов, в том числе изучаются с целью последующей вербовки сотрудники фирм-конкурентов, их потребности и финансовое положение, склонности и слабости.

Организация органов коммерческой разведки различных фирм может отличаться по форме. Она зависит от задач, возлагаемых на коммерческую разведку, дохода, ценности информации, расположения территории, зданий и помещений фирмы и других факторов. Однако независимо от количественного состава органы коммерческой разведки объективно должны решать задачи по информационному обеспечению руководства организации информацией, необходимой для успешной ее деятельности в условиях конкуренции. Конечно, этими вопросами занимаются руководители организации, но постоянный «информационный голод» вынуждает их привлекать к сбору и анализу информации профессионалов.

Органы коммерческой разведки входят состав в службы безопасности.

5.4 Агентурные способы разведки

В настоящее время достаточно условно разведку можно разделить на *агентурную* и *техническую*. Условность состоит в том, что добывание информации агентурными методами осуществляется с использованием технических средств, а техническую разведку ведут люди. Отличия – в преобладании человеческого или технического факторов. Агентурная разведка является наиболее древним и традиционным видом разведки. Добывание информации производится путем проникновения агента – разведчика к источнику информации на расстояние доступности его органов чувств или используемых им технических средств копирования информации и передачи ее потребителю.

Возможности разведки по добыванию информации зависят, прежде всего, от способов доступа органов ее добывания (агентов, технических средств) к источникам информации и обеспечения разведывательного контакта с ними. Эти факторы связаны между собой. Чем ближе удается приблизиться органу разведки к источнику информации, тем выше вероятность установления разведывательного контакта с ним.

Доступ к информации предполагает, что источник (или носитель информации) обнаружен и локализован и с ним потенциально возможен разведывательный контакт. Установление разведывательного контакта между злоумышленником или его техническим средством и источником информации предусматривает выполнение условий, при которых злоумышленник непосредственно или дистанционно может похитить, уничтожить или изменить информацию**. Условия разведывательного контакта** – пространственное, энергетическое и временное.

Пространственное условие предполагает такое пространственное размещение злоумышленника относительно источника информации, при котором злоумышленник «видит» источник информации.

Так как любое перемещение носителя в пространстве уменьшает его энергию, то энергетическое условие разведывательного контакта состоит в обеспечении на входе приемника злоумышленника отношения сигнал/помеха, достаточного для получения на его выходе информации с требуемым качеством. Энергетическое условие учитывает не только энергию или мощность носителя, но и уровни различного рода мешающих воздействий (помех) одинаковой с носителем информации физической природы.

Помехи присутствуют в любой среде распространения, в любых средствах приема и обработки сигналов. Они могут при недостаточной мощности носителя вызвать такие искажения информации, при которых она станет непонятной получателю или у него возникнут сомнения в достоверности, особенно цифровых данных, которые наиболее легко подвергаются трансформации под действием помех. Поэтому получатель информации (санкционированный или нет) предъявляет такие требования к качеству информации, при выполнении которых у него не возникают сомнения в достоверности получаемой информации. Качество получаемой информации оценивается относительным количеством правильно принятых или искаженных элементов сообщения (букв, цифр, звуков речи, элементов изображения) или значениями искажений признаков объектов.

Так как добывание информации является динамичным процессом, то необходима синхронизация работы всех элементов, обеспечивающих этот процесс. Необходимость функционирования органа добывания, синхронизированного с работой источника информации, составляет суть временного условия разведывательного контакта. При невыполнении его информацию не удастся получить даже в случае достаточной энергетики носителя. Действительно, если в кабинете ценного источника информации, например, руководителя фирмы, установлено закладное устройство, которое позволяет прослушивать все ведущиеся в нем разговоры, а кабинет пуст, то временное условие не выполнено.

Таким образом, для добывания информации необходимы: доступ органа разведки к источнику информации и выполнение условий разведывательного контакта.

Методы доступа к информации можно разделить на три группы:

- физическое проникновение злоумышленника к источнику информации;
- сотрудничество органа разведки или злоумышленника с работником конкурента (гражданином другого государства или фирмы), имеющего легальный или нелегальный доступ к интересующей разведку информации;
- дистанционный съем информации с носителя.

Физическое проникновение к источнику информации возможно путем скрытого или с применением силы проникновения злоумышленника к месту хранения носителя, а также в результате внедрения злоумышленника в организацию. Способ проникновения зависит от вида информации и способов ее использования.

Скрытое проникновение имеет ряд преимуществ по сравнению с остальными, но требует тщательной подготовки и информации о месте нахождения источника, системе безопасности, возможных маршрутах движения и др.

Для обеспечения регулярного доступа к информации проводится внедрение и легализация злоумышленника путем поступления его на работу в интересующую организацию. Так как при найме на работу претендент проверяется, то злоумышленник должен иметь убедительную легенду своей прошлой деятельности и соответствующие документы.

Рассмотренные способы обеспечивают скрытность добывания информации. Когда в ней нет необходимости, а цена информации очень велика, то возможно нападение на сотрудников охраны с целью хищения источника информации.

Для регулярного добывания информации органы разведки стараются привлечь к работе сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.

Основными способами привлечения таких сотрудников являются следующие:

- инициативное сотрудничество;
- подкуп;
- сотрудничество под угрозой.

Инициативное сотрудничество предполагает привлечение людей, которые ищут контакты с разведкой зарубежного государства или конкурента, к сотрудничеству с целью добывания секретной или конфиденциальной информации по месту работы. Таких людей выявляют органы разведки путем наблюдения за сотрудниками и изучения их поведения, интересов, моральных качеств, слабостей, связей, финансового положения.

Способы склонения к сотрудничеству подбираются под конкретного человека, который попал в поле зрения органов разведки и которого предполагается заставить сотрудничать (завербовать). Наиболее распространенным и менее опасным для злоумышленника способом склонения к сотрудничеству является подкуп.

Другие способы склонения к сотрудничеству связаны с насильственными действиями злоумышленников. Это – психическое воздействие, угрозы личной безопасности, безопасности родных, имущества, а также преследования и шантаж, принуждающие сотрудника фирмы нарушить свои обязательства о неразглашении тайны. Если в результате предварительного изучения личностных качеств сотрудника фирмы, его жизни и поведения выявляются компрометирующие данные, то возможен шантаж сотрудника с целью склонения его к сотрудничеству под угрозой разглашения компрометирующих сведений.

Выпытывание – способ получения информации от человека путем задавания ему вопросов. Способы выпытывания разнообразны: от скрытого выпытывания до выпытывания под пыткой. Скрытое выпытывание возможно путем задавания в ходе беседы на конференции, презентации или любом другом месте вроде бы невинных вопросов, ответы на которые для специалиста содержат конфиденциальную информацию.

6 ТЕХНИЧЕСКАЯ РАЗВЕДКА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

6.1 Классификация видов технической разведки

Развитие технической разведки связано, прежде всего, с повышением ее технических возможностей, обеспечивающих:

- снижение риска физического задержания агента органами контрразведки или службы безопасности за счет дистанционного контакта его с источником информации;
- добывание информации путем съема ее с носителей, не воздействующих на органы чувств человека.

Многообразие видов носителей информации породило множество видов технической разведки. Ее классифицируют по различным признакам (основаниям классификации). Наиболее широко применяются две классификации: по физической природе носителей информации и видам носителей технических средств добывания.

Техническая разведка (при классификации по физической природе носителя информации) состоит из следующих видов:

- оптическая (носитель – электромагнитное поле в видимом и инфракрасном диапазонах);
- радиоэлектронная (носитель – электромагнитное поле в радиодиапазоне или электрический ток);
- акустическая (носитель – акустическая волна);
- химическая (носитель – частицы вещества);
- радиационная (носитель – излучения радиоактивных веществ);
- магнитометрическая (носитель – магнитное поле).

В свою очередь оптическая, радиоэлектронная и акустическая разведка подразделяется на подвиды технической разведки. Оптическая разведка включает:

- визуально-оптическую;
- фотографическую;
- инфракрасную;
- телевизионную;
- лазерную.

Приведенная последовательность видов оптической разведки соответствует этапам развития оптической разведки по мере технического прогресса в области средств оптического наблюдения. Последние 3 вида, использующие электронную технику, образуют оптико-электронную разведку.

Радиоэлектронная разведка в зависимости от характера добываемой информации подразделяется на:

- радиоразведку;
- радиотехническую разведку;
- радиолокационную разведку;
- радиотепловую разведку;
- компьютерную разведку.

Радиоразведка добывает семантическую информацию путем перехвата радиосигналов с конфиденциальной информацией, радиотехническая – информацию о параметрах (признаках) радиотехнических сигналов, радиолокационная – о видовых признаках радиолокационного изображения объекта на экране радиолокатора, наконец, радиотепловая – о признаках, проявляющихся через собственные электромагнитные излучения объектов в радиодиапазоне. Компьютерная разведка предназначена для добывания информации из компьютеров и вычислительных сетей.

Акустическая разведка в зависимости от среды распространения акустической волны делится на воздушно-акустическую (слово «воздушная», как правило, опускается), гидроакустическую (среда распространения – вода) и сейсмическую (среда – земная поверхность).

Химическая разведка добывает информацию о составе, структуре и свойствах веществ путем взятия проб и анализа их макрочастиц.

Радиационная разведка предназначена для обнаружения, локализации, определения характеристик и измерения уровней излучений радиоактивных веществ.

Магнитометрическая разведка позволяет по изменению магнитного поля Земли обнаруживать тела, имеющие собственное магнитное поле, например, подводные лодки в погруженном состоянии.

Широко распространена классификация разведки по виду носителей средств добывания. Если средство добывания установлено на поверхности земли, в здании, на наземном транспорте, то такая разведка относится к сухопутной. На летающем аппарате (самолете, вертолете, воздушном шаре и др.) размещаются средства воздушной разведки. Добывание информации с использованием космических аппаратов осуществляет космическая разведка. Наконец, с помощью технических средств разведки, установленных на кораблях, ведется морская разведка.

6.2 Технические способы доступа к конфиденциальной информации

Дистанционное добывание информации предусматривает съем ее с носителей, распространяющихся за пределы помещения, здания, территории организации. Оно возможно в результате наблюдения, подслушивания, перехвата, сбора носителей информации в виде материальных тел (бракованных узлов, деталей, демаскирующих веществ и др.) за пределами организации.

Наблюдение предполагает получение и анализ изображения объекта наблюдения (документа, человека, предмета, пространства и др.). При наблюдении добываются, в основном, видовые признаки объектов. Но возможно добывание семантической информации, если объект наблюдения представляет собой документ, схему, чертежи т. д. Например, текст или схема конструкции прибора на столе руководителя или специалиста могут быть подсмотрены в ходе посещения. Также возможно наблюдение через окно текста и рисунков на плакатах, развешанных на стене во время проведения совещания.

Объекты могут наблюдаться непосредственно – глазами или с помощью технических средств. Различают следующие способы наблюдения с использованием технических средств:

- визуально-оптическое;
- наблюдения в ИК-диапазоне;
- наблюдение с консервацией изображения (фото- и киносъемка);
- телевизионное наблюдение, в том числе с записью изображения;
- лазерное наблюдение;
- радиолокационное наблюдение;
- радиотеплолокационное наблюдение.

Визуально-оптическое наблюдение – наиболее древний способ наблюдения со времени изобретения линзы. Современный состав приборов визуально-оптического наблюдения разнообразен – от специальных телескопов до эндоскопов, обеспечивающих наблюдение скрытых объектов через маленькие отверстия или щели.

Так как человеческий глаз не чувствителен к ИК-лучам, то для наблюдения в ИК-диапазоне применяются специальные приборы (ночного видения, тепловизоры), преобразующие невидимое изображение в видимое.

Основной недостаток визуально-оптического наблюдения в видимом и ИК-диапазонах – невозможность сохранения изображения для последующего анализа специалистами. Для консервации (сохранения)

статического изображения объекта его фотографируют, для консервации подвижных объектов производят кино- или видеосъемку.

Наблюдение объектов с одновременной передачей изображений на любое расстояние осуществляется с помощью средств телевизионного наблюдения.

Возможно так называемое лазерное наблюдение в видимом и ИК-диапазонах, в том числе с определением с высокой точностью расстояния до объекта и его координат.

Радиолокационное наблюдение позволяет получать изображение удаленного объекта в радиодиапазоне в любое время суток и в неблагоприятных климатических условиях, когда невозможны другие способы наблюдения. При радиотеплолокационном наблюдении изображение объекта соответствует распределению температуры на его поверхности.

Подслушивание – один из наиболее древних методов добывания информации. Подслушивание, как и наблюдение, бывает непосредственное и с помощью технических средств. Непосредственное подслушивание использует только слуховой аппарат человека. В силу малой мощности речевых сигналов разговаривающих людей и значительного затухания акустической волны в среде распространения непосредственное подслушивание возможно на небольшом расстоянии (единицы или в лучшем случае при отсутствии посторонних звуков – десятки метров). Поэтому для подслушивания применяются различные технические средства. Этим способом добывается в основном семантическая (речевая) информации, а также демаскирующие признаки сигналов от работающих механизмов, машин и других источников звуков.

Перехват предполагает несанкционированный прием радио- и электросигналов и извлечение из них семантической информации, демаскирующих признаков сигналов и формирование изображений объектов при перехвате телевизионных или факсимильных сигналов.

Многообразие технических средств и их комплексное применение для добывания информации порой размывает границы между рассмотренными способами. Например, при перехвате радиосигналов сотовой системы телефонной связи возможно подслушивание ведущихся между абонентами разговоров, т. е. одновременно производится и перехват, и подслушивание. Учитывая неоднозначность понятий «подслушивание» и «перехват», способы добывания акустической информации целесообразно относить к подслушиванию, а несанкционированный прием радио- и электрических сигналов – к перехвату.

6.3 Видовые демаскирующие признаки

В оптическом диапазоне

Видовые демаскирующие признаки описывают внешний вид объекта. Они объективно ему присущи, но выявляются в результате анализа внешнего вида модели объекта – изображения его на экране оптического приемника (сетчатки глаза человека, фотоснимке, экране телевизионного приемника, прибора ночного видения и т. д.). Так как модель в общем случае отличается от оригинала, то состав и значения видовых демаскирующих признаков зависят не только от объекта, но и от условий наблюдения и характеристик оптического приемника.

Наибольшее количество информативных видовых демаскирующих признаков добывается при визуально-оптическом наблюдении объектов в видимом диапазоне. Основными видовыми демаскирующими признаками объектов в видимом свете являются:

- фотометрические и геометрические характеристики объектов (форма, размеры объекта, цвет, структура, рисунок и детали его поверхности);
- тени, дым, пыль, следы на грунте, снеге, воде;
- взаимное расположение элементов группового (сложного) объекта;
- расположение защищаемого объекта относительно других известных объектов.

Геометрические и фотометрические характеристики объектов образуют наиболее устойчивую и информативную информационную структуру, так как они присущи объекту и относятся к прямым признакам. Размеры объекта наблюдения определяются по максимальному и минимальному линейным размерам, площади и периметра проекции объекта и его тени на плоскость, перпендикулярную к линии визирования (наблюдения), высоте объекта и др. Размеры приобретают значение основного демаскирующего признака для объектов примерно одинаковой формы.

Форма – один из основных демаскирующих признаков, прежде всего, искусственных объектов, поскольку для них, как правило, характерны правильные геометрические формы.

Детали объектов, их количество, характер расположения дают представление о сложном объекте и позволяют отличить его от подобных по форме.

Тени объектов возникают в условиях прямого солнечного освещения и являются важными демаскирующими признаками объекта

при наблюдении его сверху. Некоторые объекты (например, линии электропередач, антенные мачты, ограждения и т. д.) часто распознают только по тени. Различают два вида тени: собственную, от элементов объекта, которая ложится на поверхность самого объекта, и падающую, отбрасываемую объектом на фон. По падающей тени можно обнаружить объект, определить его боковые размеры, высоту, а также в ряде случаев и форму.

В инфракрасном диапазоне

Важнейшим свойством поверхности объекта, определяющим его цвет и яркость, является коэффициент отражения поверхности для различных длин волн и частот: в видимом, инфракрасном и радиодиапазоне.

Объекты по-разному отражают падающие на них лучи света. Отражательные свойства объектов описываются коэффициентами (спектральными и интегральным) и индикатрисой отражения. Индикатриса отражения характеризует распределение силы отраженного света в пространстве. Интегральный коэффициент отражения определяется в результате усреднения спектральных (на одной длине волны) коэффициентов отражения в рассматриваемом диапазоне длин волн.

В зависимости от характера поверхности различают направленное (зеркальное), рассеянное (диффузное) и смешанное отражения. Граница между ними условная и определяется соотношением величин неровностей поверхности и длины падающей волны. Следовательно, шероховатая поверхность в видимом свете может в ИК-диапазоне выглядеть как гладкая. Диффузное отражение присуще мелкоструктурным элементам, таким как песок. Большинство объектов земной поверхности имеют смешанную индикатрису отражения.

Яркость объекта, определяемая не только коэффициентами отражения объекта, но и яркостью внешнего источника освещения, относится к косвенным признакам, таким как дым, пыль, его следы на различных поверхностях.

Любые тела излучают электромагнитные волны в ИК -диапазоне. Чем выше температура тела, тем больше излучаемая энергия. Поэтому нагретые тела с помощью соответствующих приборов могут наблюдаться в полной, с точки зрения человека-наблюдателя, темноте. Зрительный анализатор человека не воспринимает лучи в инфракрасном диапазоне. Поэтому видовые демаскирующие признаки в этом диапазоне добываются с помощью специальных приборов (ночного видения, тепловизоров), имеющих худшее разрешение, чем

глаз человека. Кроме того, видимое изображение на экранах этих приборов одноцветное. Но изображение в инфракрасном диапазоне может быть получено при малой освещенности объекта или даже в полной темноте. В этом случае к демаскирующим признакам добавляются признаки, характеризующие температуру поверхности объекта.

В общем случае к демаскирующим признакам объекта в ИК-диапазоне относятся следующие:

- геометрические характеристики внешнего вида объекта (форма, размеры, детали поверхности);
- температура поверхности.

Максимальное количество признаков внешнего вида объектов добывают в видимом оптическом диапазоне фотоприемники с высоким разрешением, к которым в первую очередь относятся глаз человека и фотопленка.

В инфракрасном диапазоне количество и качество признаков уменьшается. Отсутствует такой информативный признак, как цвет. С увеличением длины волны ухудшается разрешение значений признаков, например, точность оценки размеров объекта и его деталей.

В радиочастотном диапазоне

Представляет собой участок спектра электромагнитного колебания с длиной волны от 1 километра до сотых долей миллиметра.

Органы чувств человека электромагнитные поля в этом диапазоне не воспринимают, поэтому для их фиксации используют специальные технические средства.

Исследования объектов с использованием этого участка диапазона называют *радиолокацией*.

Для проведения радиолокации используют два прибора:

- передатчик, который формирует электромагнитные излучения в виде направленного луча;
- приемник, который улавливает радиоволны, отраженные от интересующего объекта.

В радиодиапазоне наблюдается более сложная картина, чем при отражении света. Отражательные возможности поверхности в этом диапазоне определяются, кроме указанных для света, ее электропроводностью и конфигурацией относительно направления падающей волны. Большая часть суши отражает электромагнитную волну в радиодиапазоне диффузно, спокойная водная поверхность – зеркально.

Радиолокационное изображение объектов сложной формы (автомобиль, самолет и др.) формируется совокупностью отдельных пятен

различной яркости, соответствующих так называемым «блестящим, точкам» объектов, отражающих сигнал в направлении радиолокационной станции (РЛС). «Блестящие точки» на экране локатора создают элементы поверхности объектов, расположенные перпендикулярно направлению облучения, а также элементы конструкции, которые после переотражений радиоволн внутри конструкции возвращают их к радиолокатору.

Наибольшей отражающей способностью в направлении антенны радиолокационной станции обладают конструкции в виде 2-4 жестко связанных между собой взаимно перпендикулярных металлических или металлизированных плоскостей. Такие конструкции называются уголковыми радиоотражателями, применяемыми для имитации ложных объектов.

Конкретный вид радиолокационного изображения зависит от положения объекта относительно направления облучения, так как при изменении ориентации меняется количество и взаимное положение «блестящих точек».

Отражательная способность объекта в радиодиапазоне характеризуется эффективной площадью рассеяния (ЭПР). Эффективная площадь рассеяния (отражения) соответствует площади плоской хорошо проводящей (металлической) поверхности, перпендикулярной направлению облучения, помещенной в место нахождения объекта и создающаей у приемной антенны радиолокационной станции такую же плотность потока мощности, как и реальный объект.

Отражающая способность земной поверхности изменяется в широких пределах в зависимости от ее шероховатости, диэлектрической проницаемости материала и длины волны.

Электромагнитная волна отражается не только от поверхности объекта, но и от более глубинных ее слоев. Проникающая способность в дециметровом диапазоне для сухой почвы может составлять 1-2 м.

К основным видовым демаскирующим признакам объектов радиолокационного наблюдения относятся:

- эффективная площадь рассеяния;
- геометрические и яркостные характеристики (форма, размеры, яркость, детали);
- электропроводность поверхности.

Видовые демаскирующие признаки в радиодиапазоне добываются также с помощью тепловой радиолокации, приемники которой способны принимать сигналы собственных электромагнитных излучений

и формировать на их основе изображения объектов. Так как возможности радиолокаторов, в особенности тепловых, весьма ограничены по разрешению, то в радиодиапазоне выявляется меньший, чем в видимом диапазоне набор демаскирующих признаков.

В ультрафиолетовом диапазоне

Ощущать ультрафиолетовое излучение человек может, особенно сильное. Оно проявляется в виде ожога сетчатки глаза.

Кроме того, ультрафиолетовые лучи сильно поглощаются в атмосфере, как и многими предметами.

Используется ультрафиолетовая часть спектра для выявления бытовых признаков. Энергия квантового излучения обратно пропорциональна длине волны. Поэтому воздействия излучения ультрафиолетового диапазона на некоторые вещества приводит к их свечению в видимой части спектра, такие вещества называют *люминофоры*.

6.4 Способы и средства наблюдения

В оптическом (видимом и инфракрасном) диапазоне информация разведкой добывается путем визуального, визуально-оптического, телевизионного наблюдения, наблюдения с использованием приборов ночного видения и тепловизоров, фото- и киносъемки.

Наибольшее количество признаков добывается в видимом диапазоне. Видимый свет как носитель информации характеризуется следующими свойствами:

- наблюдение возможно, как правило, днем или при наличии мощного внешнего источника света;
- сильная зависимость условий наблюдения от состояния атмосферы, погодных условий:
- малая проникающая способность световых лучей в видимом диапазоне, что облегчает задачу защиты информации о видовых признаках объекта.

ИК-лучи как носители информации обладают большей проникающей способностью, позволяют наблюдать объекты при малой освещенности. Но при их преобразовании в видимый свет для обеспечения возможности наблюдения объекта человеком происходит значительная потеря информации об объекте.

Эффективность обнаружения и распознавания объектов наблюдения зависит от следующих факторов:

- яркости объекта;
- контраста объект/фон;

- угловых размеров объекта;
- угловых размеров поля обзора;
- времени наблюдения объекта;
- скорости движения объекта.

Яркость объекта на входе приемника определяет мощность носителя, превышение которой над мощностью помех является необходимым условием обнаружения и распознавания объекта наблюдения.

Контрастность объекта с окружающим фоном является необходимым условием выделения демаскирующих признаков объекта и его распознавания. Контраст определяют как отношение разности яркости объекта и фона к яркости объекта или фона.

Так как физическая природа носителя информации в оптическом диапазоне одинакова, то различные средства наблюдения, применяемые для добывания информации в этом диапазоне, имеют достаточно общую структуру. Ее можно представить в виде, приведенной на рис. 6.1.

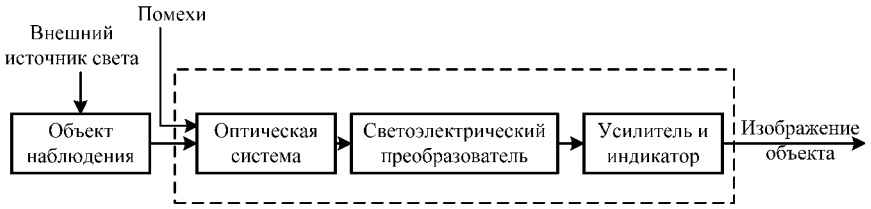

Рис. 6.1. Структурная схема средства наблюдения в оптическом диапазоне

Большинство средств наблюдения содержит оптический приемник, включающий оптическую систему, светоэлектрический преобразователь, усилитель и индикатор.

Оптическая система или объектив проецирует световой поток от объекта наблюдения на экран светоэлектрического преобразователя (сетчатку глаза, фотопленку, фотокатод, мишень оптико-электронного преобразователя). На мишени оптическое изображение преобразуется в электронное изображение, количество «свободных» электронов каждой точки которого пропорционально яркости соответствующей точки оптического изображения. Способы визуализации изображения для разных типов оптического приемника могут существенно отличаться. Изображение в виде зрительного образа формируется в мозгу человека, на фотопленке – в результате химической обработки светочувствительного слоя, на экране технического средства – путем параллельного или последовательного съема

электронов с мишени, усиления электрических сигналов и формирования под их действием видимого изображения на экране с люминофором.

6.5 Характеристики средств наблюдения

Характеристики средств наблюдения определяются, прежде всего, параметрами оптической системы и светоэлектрического преобразователя, а также они зависят от способов обработки электрических сигналов и формирования изображения при индикации. Основными из них являются:

- диапазон длин волн световых лучей, воспринимаемых светоэлектрическим преобразователем;
- чувствительность материала экрана светоэлектрического преобразователя;
- разрешающая способность, в основном пары «оптическая система - преобразователь света»;
- поле (угол) зрения и изображения.

Средства наблюдения в зависимости от назначения создаются для видимого диапазона в целом или его отдельных зон, а также для различных участков инфракрасного диапазона.

Чувствительность средства наблюдения оценивается минимальным уровнем энергии светового луча, при котором обеспечивается требуемое качество изображения объекта наблюдения. Качество изображения зависит как от яркости и контрастности проецируемого изображения, так и от помех. Помехи создают лучи света, попадающие на вход от других источников света, и шумы светоэлектрического преобразователя. На экране светоэлектрического преобразователя при посторонней внешней засветке наблюдается ухудшение контраста изображение аналогичное варианту прямого попадания на экран телевизионного приемника яркого солнечного света.

Разрешающая способность характеризуется минимальными линейными или угловыми размерами между двумя соседними точками изображения, которые наблюдаются как отдельные. Так как изображение формируется из точек, размеры которых определяются разрешающей способностью средства наблюдения, то вероятность обнаружения и распознавания объекта возрастает с повышением разрешающей способности средства наблюдения (увеличением количества точек изображения объекта).

Поле зрения – это то, что проецируется на экран оптического приемника. Угол, под которым средство «видит» предметное про-

странство, называется углом поля зрения. Часть поля зрения, удовлетворяющего требованиям к качеству изображения по его резкости, называется полем или соответственно углом поля изображения.

Характеристики зрения человека

Наиболее совершенным средством наблюдения в видимом диапазоне является зрительная система человека, включающая глаза и области мозга, осуществляющие обработку сигналов, поступающих с сетчатки глаз.

Возможности зрения человека характеризуются следующими показателями:

- глаз воспринимает световые лучи в диапазоне 0,4-0,76 мкм, причем максимум его спектральной чувствительности в светлое время суток приходится на голубой цвет (0,51 мкм), в темноте - на зеленый (0,55 мкм);
- порог угловых размеров, которые глаз различает как две раздельные точки на объекте наблюдения, составляют днем 0,5-1 угл. мин., ночью – 30 угл. мин.;
- порог контрастности различимого объекта по отношению к фону составляет днем 0,01 -0,03, ночью – 0,6;
- диапазон освещенности объектов наблюдения, к которым адаптируется глаз, чрезвычайно широк – 60-70 дБ;
- при освещенности менее 0,1 лк (в безоблачную лунную ночь) глаз перестает различать цвет.

Уникальные возможности глаз человека достигаются благодаря совершенству его оптической системы-хрусталика, выполняющей функции объектива. Совершенство хрусталика проявляется, прежде всего, в том, что его кривизна с помощью специальных глазных мышц изменяется таким образом, чтобы обеспечить на сетчатке глаза максимально четкое изображение объектов, расположенных на различных расстояниях от наблюдателя. Хотя ведутся исследования по созданию подобных искусственных объективов, но приблизиться к возможностям хрусталика глаза пока не удается.

Характеристики объективов

Объективы в силу постоянства кривизны поверхностей линз и оптической плотности стекла проецируют изображения с различного рода погрешностями. Наиболее заметны из них:

- сферическая аберрация, проявляющаяся в отсутствии резкости изображения на всем поле зрения (оно резко в центре или по краям);
- астигматизм – отсутствие одновременной резкости на краях поля изображения для вертикальных и горизонтальных линий;

- дисторсия – искривление прямых линий;
- хроматическая аберрация – появление цветных окантовок на границах световых переходов, вызванных различными коэффициентами преломления линз объектива спектральных составляющих световых лучей.

С целью уменьшения погрешностей объективы выполняются из большого (до 10 и более) количества линз с различной кривизной поверхностей. Все или отдельные группы линз склеиваются между собой.

Качество объективов описываются совокупностью параметров. Для оценки возможностей средств наблюдения основными из них являются: фокусное расстояние, угол поля зрения и изображения, светосила, разрешение, частотно-контрастная характеристика.

По величине фокусного расстояния объективы делятся на короткофокусные, с фокусным расстоянием меньшим длины диагонали кадра поля изображения d; нормальные, или среднефокусные (f=d); длиннофокусные и телеобъективы с f>d, а также с переменным фокусным расстоянием.

Объектив с переменным фокусным расстоянием (панкратический) представляет собой сложную оптическую систему, в которой предусмотрена возможность смещения оптических компонентов, за счет чего изменяется величина фокусного расстояния. Величину фокусного расстояния изменяют дискретно или плавно.

Дискретное изменение фокусного расстояния достигается применением афокальных насадок, уменьшающих или увеличивающих фокусное расстояние. Плавное изменение величины фокусного расстояния осуществляется перемещением отдельных компонент вдоль оптической оси по линейному или нелинейному закону. В зависимости от способа коррекции аберраций эти объективы подразделяют на вариообъективы и трансфокаторы.

Вариообъективы представляют собой единую оптическую схему, в которой изменение фокусного расстояния осуществляется непрерывным перемещением одного или нескольких компонентов вдоль оптической оси.

Трансфокаторы состоят из афокальной насадки с переменным, плавным увеличением и объектива с постоянным фокусным расстоянием.

Сложность оптической конструкции объективов с переменным фокусным расстоянием вызвана, прежде всего, тем, что при изменении фокусного расстояния должно автоматически сохраняться положение плоскости резкого изображения наблюдаемого объекта. Добиваются этого путем оптической компенсации (при линейном

перемещении компонентов) и механической (при нелинейном). В первом случае кратность изменения фокусного расстояния не более 3, во втором – 6-7.

По углу поля зрения (изображения) различают узкоугольные объективы, у которых величина утла не превышает 30°, среднеугольные (угол в пределах 30°-60°), широкоугольные с углом более 60° и, наконец с переменным углом поля изображения у объективов с переменным фокусным расстоянием.

Чем больше фокусное расстояние f объектива, тем больше деталей объекта можно рассмотреть на его изображении, но тем меньше угол поля зрения. Поэтому для обнаружения объекта используют коротокофокусные объективы, а для распознавания – длиннофокусные. Размеры объекта h на изображении определяются по соотношению h=fH / L в зависимости от размеров реального объекта И, расстояния от него до объектива L и фокусного расстояния объектива f.

Светосила характеризует способность объектива создавать освещенность в поле изображения в соответствии с яркостью объекта. На светосилу объектива влияют следующие факторы:

- относительное отверстие объектива;
- прозрачность (коэффициенты пропускания, поглощения, отражения) линз;
- коэффициент увеличения (масштаб получаемого изображения);
- коэффициент падения освещенности к краю поля изображения.

Светосила без учета реальных потерь света в линзах оценивается величиной геометрического относительного отверстия 1:к=1:1Ю, где D-диаметр входного отверстия объектива (апертура), или фокальным числом F=f/D. Эффективное относительное отверстие объектива меньше геометрического на величину потерь света в его линзах. По величине относительного отверстия объективы делятся на сверхсветосильные, у которых 1:к=1:2 и менее, светосильные (1:к =1:2.8-1:4) и малосветосильные с 1:к=1:5.6 и более [38]. Чем больше светосила объектива, тем выше чувствительность средства наблюдения. Однако при этом растут искажения изображения и для их уменьшения усложняют конструкцию светосильных объективов, что естественно приводит к их удорожанию.

Свет, падающий на линзу и проходящий через нее, отражается и поглощается. Количество поглощенного света зависит от толщины стекла (в среднем 1-2% на 1 см толщины). Линзы отражают 4-6% падающего на них свет. Чем больше отражающих поверхностей имеет объектив, тем больше потери света. В объективах из 5-7 линз потери света на отражение могут составлять 40-50% [38]. Уменьшают потери света просветлением линз.

Просветлением называются способы уменьшения отражения света от поверхности стекла путем нанесения на него тонкой пленки с коэффициентом преломления, меньшим преломления стекла линзы. Толщина просветляющей пленки должна составлять 1/4 длины волны падающего на линзу света. В этом случае отраженные лучи света в силу противоположности их фаз фазам падающих лучей компенсируются и, следовательно, отражение света отсутствует. Первоначально объективы просветляли для желто-зеленой части спектра, к которой наиболее чувствителен глаз человека. Просветленный объектив в отраженном свете приобретал сине-фиолетовый оттенок и назывался «голубой» оптикой. Современные технологии просветления оптики позволяют наносить на поверхность линзы 12-14 слоев просветляющих пленок и перекрывать тем самым весь спектр видимого диапазона света. Такую оптику маркируют индексами МС – многослойное покрытие. Объективы МС в отраженном свете не меняют цвет.

Возможность объектива передавать мелкие детали изображения оценивается разрешающей способностью. Она выражается максимальным числом N штрихов и промежутков между ними на 1 мм поля изображения в его центре и по краям. Наиболее высокую разрешающую способность имеют объективы для микрофотографирования в микроэлектронике. Она достигает 280-440 линий на мм по центру и 260-400 линий на мм по краям поля изображения.

Так как одним из основных факторов, определяющих вероятность обнаружения и распознавания объектов, является контрастность его изображения по отношению к фону, то важной характеристикой объектива как элемента средства наблюдения является его частотно-контрастная характеристика. Она служит мерой способности объектива передавать контраст деталей объекта и измеряется отношением контрастности деталей определенных размеров на изображении и на объекте. Уменьшение контраста мелких деталей на изображении вызвано тем, что в результате различных аберраций объектива на изображении размываются границы деталей наблюдаемых объектов.

Для количественной оценки частотно-контрастной характеристики в качестве исходного объекта используется эталонный объект наблюдения – мира в виде черно-белых линий с уменьшающейся шириной, нанесенных, например, тушью на белой бумаге. По результатам измерений контрастности n линий на проецируемом объективом изображении строится зависимость контраста K от количества линий n в одном мм. Зависимость K=f(n) определяет частотно-контрастную характеристику объектива.

В связи с большими техническими проблемами создания универсальных объективов с высокими значениями показателей, оптическая промышленность выпускает широкий набор специализированных объективов: для фото- и киносъемки, портретные, проекционные, для микрофотографирования и т. д.

Для добывания информации применяются объективы трех видов: для аэрофотосъемки, широкого применения (фото-, кино- и видеосъемки с использованием бытовых и профессиональных камер) и для скрытой съемки.

Объективы широкого применения разделяются в соответствии с размерами фотоаппаратов: для малоформатных и миниатюрных, среднеформатных и крупноформатных камер.

Для скрытого наблюдения используются:

- телеобъективы с большим фокусным расстоянием (300-4800 мм) для фотографирования на большом удалении от объекта наблюдения, например, из окна противоположного дома и далее;
- так называемые точечные объективы для фотографирования из портфеля, часов, зажигалки, через щели и отверстия. Они имеют очень малые габариты и фокусное расстояние, но большой угол поля зрения.

6.6 Способы и средства перехвата радиосигналов

Перехват носителей в виде электромагнитного, магнитного и электрического полей, а также электрических сигналов с информацией осуществляют органы добывания радио и радиотехнической разведки. При перехвате решаются следующие основные задачи:

- поиск по демаскирующим признакам сигналов с информацией в диапазоне частот, в которых они могут находиться;
- обнаружение и выделение сигналов, интересующих органы добывания;
- усиление сигналов и съем с них информации;
- анализ технических характеристик принимаемых сигналов;
- определение местонахождения (координат) источников представляющих интерес сигналов;
- обработка полученных данных с целью формирования первичных признаков источников излучения или текста перехваченного сообщения.

Упрощенная структура типового комплекса средств перехвата приведена на рис. 6.2.

Типовой комплекс включает:

- приемные антенны;

- радиоприемник;
- анализатор технических характеристик сигналов;
- радиопеленгатор;
- регистрирующее устройство/

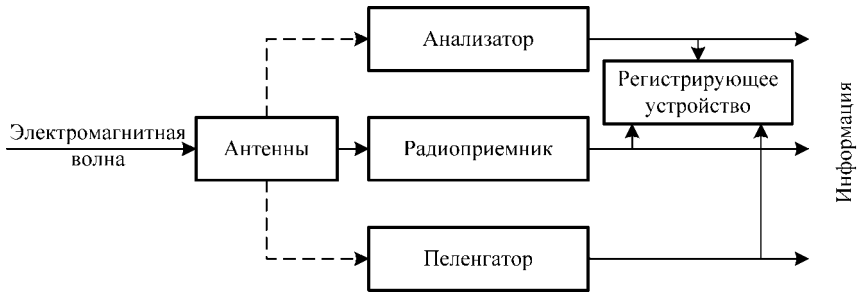

Рис. 6.2. Структура комплекса средств перехвата

1. Антенна предназначена для преобразования электромагнитной волны в электрические сигналы, амплитуда, частота и фаза которых соответствует аналогичным характеристикам электромагнитной волны.

2. В радиоприемнике производится поиск и селекция радиосигналов по частоте, усиление и демодуляция (детектирование) выделенных сигналов, усиление и обработка демодулированных (первичных) сигналов: речевых, цифровых данных, видеосигналов и т. д.

3. Для анализа радиосигналов после селекции и усиления они подаются на входы **измерительной аппаратуры** анализатора, определяющей параметры сигналов: частотные, временные, энергетические, виды модуляции, структуру кодов и др.

4. Радиопеленгатор предназначен для определения направления на источник излучения (пеленг) и его координат.

5. Регистрирующее устройство обеспечивает запись сигналов для документирования и последующей обработки.

Анализатор и пеленгатор могут иметь собственные радиоприемники (или их элементы) и антенны (на рис. 6.2 эти варианты условно показаны пунктирными линиями).

Большие возможности по перехвату радиосигналов в широком диапазоне частот предоставляют **сканирующие приемники.**

Особенностью этих радиоприемников является возможность очень быстрой (электронной) перестройки в широком диапазоне частот. Во многих приемниках предусмотрены интерфейсы сопряжения с

ПЭВМ, что позволяет автоматизировать поиск сигналов по задаваемым признакам, в том числе использующих простые виды технического закрытия.

На основе сканирующих приемников и ПЭВМ созданы **автоматизированные комплексы радиоконтроля.**

Для перехвата радиосигналов со сложной структурой, применяемых в сотовой, пейджинговой и других видах мобильной связи, создаются **специальные приемные комплексы.**

Процессы перехвата включают также регистрацию (запись, запоминание) сигналов с добытой информацией. Регистрация сигналов производится путем аудио- и видеозаписи, записи на магнитные и оптические диски, на обычной, электрохимической, термочувствительной и светочувствительной бумаге, запоминания в устройствах полупроводниковой и других видов памяти, фотографирования изображений на экранах мониторов ПЭВМ, телевизионных приемников, осциллографов, спектроанализаторов.

6.7 Виды и характеристики антенн

Антенны представляют собой конструкцию из токопроводящих элементов, размеры и конфигурация которых определяют эффективность преобразования радиосигналов в электрические. Для обеспечения эффективного излучения и приема в широком диапазоне используемых радиочастот создано большое количество видов и типов антенн, классификация которых представлена на рис. 6.3.

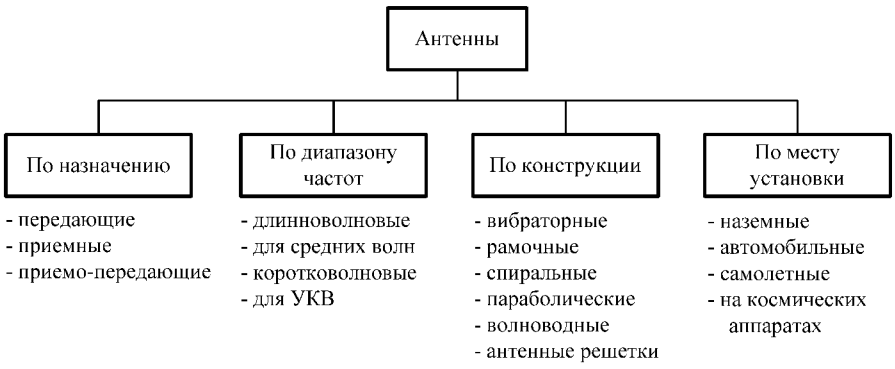

Рис. 6.3. Классификация антенн

Назначение передающих и приемных антенны ясно из их наименований. По своим основным электрическим параметрам они не отличаются. Многие из них в зависимости от схемы подключения (к передатчику или приемнику) могут использоваться как передающие или приемные. Однако если к передающей антенне подводится большая мощность, то в ней принимаются специальные меры по предотвращению пробоя между элементами антенны, находяшимися под более высоким напряжением.

Эффективность антенн зависит от согласования размеров элементов антенны с длинами излучаемых или принимаемых волн. Минимальная длина согласованной с длиной волны электромагнитного колебания штыревой антенны близка к L/4, где L – длина рабочей волны. Размеры и конструкция антенн отличаются как для различных диапазонов частот, так и внутри диапазонов.

Если для стационарных антенн требование к геометрическим размерам антенны может быть достаточно просто выполнено для коротких и ультракоротких волн, то для антенн, устанавливаемых на мобильных средствах, оно неприемлемо. Например, рациональная длина антенны для обеспечения связи на частоте 30 МГц составляет 2,5 м, что неудобно для пользователя. Поэтому применяют укороченные антенны, но при этом уменьшается их эффективность.

По конструкции антенны разделяются на проволочные (вибраторные), рупорные, параболические, рамочные, спиральные, антенные решетки и различные их комбинации.

Возможности антенн как приемных, так и передающих определяются следующими характеристиками:

- диаграммой направленности;
- коэффициентом полезного действия;
- коэффициентом направленного действия;
- коэффициентом усиления;
- полосой частот.

Диаграмма направленности представляет собой графическое изображение уровня излучаемого и принимаемого сигнала от угла поворота антенны в горизонтальной и вертикальной плоскостях. Диаграммы изображаются в прямоугольных и полярных координатах.

Диаграммы направленности могут иметь разнообразный и изрезанный характер, определяемый механической конструкцией и электрическими параметрами. Лепесток диаграммы направленности с максимумом мощности излучаемого или принимаемого электромагнитного поля называется главным или основным лепестком, остальные – боковыми и задними. Соотношение между величинами мощ-

ности основного лепестка по сравнению с остальными характеризует направленные свойства антенны. Ширина главного лепестка диаграммы измеряется углом между прямыми, проведенными из начала полярных координат до значений диаграммы, соответствующих половине максимальной мощности излучения или 0,7 напряжения электрического сигнала приемной антенны. Чем у́же ширина диаграммы направленности антенны, тем выше ее коэффициент направленного действия.

Коэффициент направленного действия (КНД) определяет величину энергетического выигрыша, который обеспечивает направленная антенна по сравнению с ненаправленной.

Потери электрической энергии в антенне оцениваются коэффициентом полезного действия (КПД), равным отношению мощности сигнала на выходе реальной антенны к мощности сигнала идеальной антенны без потерь.

Произведение этих двух коэффициентов определяет коэффициент усиления антенны (КУ).

Полоса частот, в пределах которых сохраняются заданные технические характеристики антенны, называется полосой ее пропускания.

Создание антенн с высоким коэффициентом усиления и широкой полосой пропускания представляет основную проблему в области конструирования антенн. Чем выше КУ, тем труднее обеспечить широкополосность антенны. В зависимости от полосы пропускания антенны разделяются на узкополосные, широкополосные, диапазонные и широкодиапазонные.

Узкополосные антенны обеспечивают прием сигналов в диапазоне 10% от основной частоты. У широкополосных антенн эта величина увеличивается до (10-50)%, у диапазонных антенн коэффициент перекрытия (отношение верхней частоты полосы пропускания антенны к нижней) составляет 1,5-4, а у широкодиапазонных антенн это отношение достигает значений в интервале 4-20 и более.

Совокупность однотипных антенн, расположенных определенным образом в пространстве, образует антенную решетку. Сигнал антенной решетки соответствует сумме сигналов от отдельных антенн. Различают линейные (одномерные) и плоские (двухмерные) антенные решетки. Антенные решетки, у которых можно регулировать фазы сигналов отдельных антенн, называют фазированными антенными решетками. Путем изменения фаз суммируемых сигналов можно менять диаграмму направленности в горизонтальной и вертикальной плоскостях и производить быстрый поиск сигнала по пространству и ориентацию антенны на источник излучения.

6.8 Основные характеристики радиоприемных устройств

Радиоприемник – основное техническое средство перехвата, осуществляющего поиск, селекцию, прием и обработку радиосигналов. В состав его входят устройства, выполняющие:

- перестройку частоты настройки приемника и селекцию (выделение) нужного радиосигнала;
- усиление выделенного сигнала;
- детектирование (съем информации);
- усиление видео- или низкочастотного первичного сигнала.

Различают два вида радиоприемников: прямого усиления и супергетеродинные. Появившиеся первыми приемники прямого усиления уступили супергетеродинным почти во всех радиодиапазонах, за исключением сверхвысоких частот. Такая тенденция объясняется более высокой селективностью и чувствительностью супергетеродинного радиоприемника по сравнению с приемником прямого усиления.

Возможности радиоприемника определяются следующими техническими характеристиками:

- диапазоном принимаемых частот;
- чувствительностью;
- избирательностью;
- динамическим диапазоном;
- качеством воспроизведения принимаемого сигнала;
- эксплуатационными параметрами.

Диапазон принимаемых частот определяется шириной полосы пропускания селективных элементов входных фильтров и интервалом частот гетеродина.

Чувствительность радиоприемника оценивается минимальной мощностью или напряжением сигнала на его входе, при которой уровень сигнала и отношение сигнал/шум на выходе приемника обеспечивают нормальную работу оконечных устройств (индикации и регистрации).

Избирательность приемника оценивается параметрами амплитудно-частотной характеристики (АЧХ) его селективных цепей, определяющей зависимость коэффициента усиления приемного тракта от частоты. Избирательность приемника максимальная, когда его амплитудно-частотная характеристика повторяет форму спектра принимаемого сигнала. В этом случае будут приняты все его спектральные составляющие, но не пропущены спектральные составляющие других сигналов (помех).

Избирательность реального приемника оценивается двумя основными показателями: шириной полосы пропускания и коэффициентом прямоугольности АЧХ радиоприемника, реальная форма которой имеет колоколообразный вид.

Ширина полосы пропускания выражается разностью максимальной и минимальной частот, которые может нести канал.

Так как активные элементы усилительных каскадов радиоприемника (транзисторы, диоды и др.) имеют достаточно узкий интервал значений входных сигналов, при которых обеспечивается их линейное усиление, то при обработке сигналов с амплитудой вне этих интервалов возникают их нелинейные искажения и, следовательно, искажение информации. Возможность приемника принимать радиосигналы различной мощности характеризуется его **динамическим диапазоном**. Величина динамического диапазона оценивается отношением в децибелах максимального уровня к минимальному уровню принимаемого сигнала. Для повышения динамического диапазона в современных радиоприемниках применяется устройство автоматической регулировки усиления (АРУ) приемного тракта, изменяющего его коэффициент усиления в соответствии с уровнем принимаемого сигнала.

Несоответствие амплитудно-частотной и фазовой характеристик, динамического диапазона радиоприемника текущим характеристикам сигнала приводят к его частотным, фазовым и нелинейным искажениям и потере информации.

Частотные искажения вызываются подавлением или изменениями составляющих спектра входного сигнала. Из-за частотных искажений сигнал на входе демодулятора приобретает форму, отличающуюся от входной.

Фазовые искажения сигнала возникают из-за нарушений фазовых соотношений между отдельными спектральными составляющими сигнала при прохождении его цепям тракта приемника.

Искажения, проявляющиеся в появлении в частотном спектре выходного сигнала дополнительных составляющих, отсутствующих во входном сигнале, называются нелинейные. Нелинейные искажения вызывают элементы радиоприемника, имеющие нелинейную зависимость между выходом и входом. Они возникают при превышении отношения значений максимального и минимального напряжений сигнала на входе приемника его динамическому диапазону. Эти виды искажений приводят к изменению информационных параметров сигнала на входе демодулятора и, как следствие, к искажению информации после демодуляции.

Кроме указанных электрических характеристик, возможности радиоприемников оцениваются также по их надежности, оперативности управления, видам электропитания и потребляемой мощности, массо-габаритным показателям.

Традиционные аналоговые радиоприемники постепенно вытесняются цифровыми, в которых сигнал преобразуется в цифровой вид с последующей его обработкой средствами вычислительной техники.

6.9 Особенности непосредственного подслушивания

Слуховая система человека обеспечивает прием акустических сигналов в диапазоне звуковых (20-20000 Гц) частот, границы которого для разных людей колеблются в широких пределах и изменяются с возрастом. Верхний предел слышимости у молодых людей составляет 16-20 кГц, для пожилых людей он снижается в среднем до 12 кГц. Диапазон интенсивности воспринимаемых ухом звуков очень велик. На частоте 1000 Гц наиболее громкий звук, который человек может вынести, примерно в 10^{12} интенсивнее самого слабого воспринимаемого звука. Интенсивность звука при таком большом интервале уровней измеряют относительной мерой в дБ, определяемой относительно порога слышимости человеком звука на частоте 1000 Гц. Интенсивность звука человек оценивает как его громкость. Между психологическим восприятием громкости и физической интенсивностью звука нет прямого соответствия. Громкость звука зависит не только от его интенсивности, но и от частоты. При постоянной интенсивности звуки очень высокой и очень низкой частоты кажутся более тихими, чем звуки средней частоты. Порог слышимости слуховой системы на частоте 20 Гц выше порога в диапазоне 2000-5000 Гц примерно на 70 дБ, а на частоте 10000 Гц приблизительно на 15 дБ. Следовательно, максимальная дальность непосредственного подслушивания изменяется в широких пределах в зависимости от спектра звуков говорящего человека.

Уши человека плохо приспособлены для восприятия структурных звуков, распространяющихся в твердой среде. С этой целью используются устройства – стетоскопы, которые передают колебания поверхности твердой среды распространения в слуховые проходы ушей человека. Стетоскопы широко применяются в медицинской практике для прослушивания звуков в теле человека. Они представляет собой один или два гибких звукопровода в виде резиновых или из других синтетических материалов трубок, соединенных с контактной площадкой и передающих звуковое колебание от поверхности твердого тела к ушам человека. Эти звукопроводы локализуют и направляют

звуковую волну к ушам человека, а также изолируют ее от акустических помех в окружающем пространстве. Для добывания информации применяются стетоскопы, у которых площадка, контактирующая с твердой поверхностью твердой среды распространения, соединена с мембраной микрофона. Для прослушивания структурных звуков подобный акустоэлектрический преобразователь (датчик) стетоскопа прижимают или приклеивают к поверхности стены или трубы.

6.10 Технические способы и средства подслушивания

При непосредственном подслушивании акустические сигналы, распространяющиеся от источника звука прямолинейно в воздухе, по воздухопроводам или через различные ограждения (двери, стены, окна и др.) и экраны, принимаются слуховой системой злоумышленника.

Основной недостаток непосредственного подслушивания – малая дальность, составляющая для речи средней (нормальной) громкости единицы и десятки метров в зависимости от уровня шума. На улице города дальность слышимости днем составляет всего несколько метров.

Подслушивание с помощью технических средств осуществляется путем:

- приема и прослушивания акустических сигналов, распространяющихся в воздухе, воде и твердых телах;
- прослушивания речи, выделяемой из перехваченных радио- и электрических сигналов функциональных каналов связи и из сигналов побочных излучений и наводок;
- применения лазерных систем подслушивания:
- использования закладных устройств;
- высокочастотного навязывания.

Конкретный метод подслушивания реализуется с использованием соответствующего технического средства. Для подслушивания применяют следующие технические средства:

- акустические приемники, в том числе с направленными микрофонами;
- приемники опасных сигналов;
- акустические закладные устройства;
- лазерные системы подслушивания;
- устройства подслушивания путем высокочастотного навязывания.

Акустические приемники обеспечивают селекцию акустических сигналов, распространяющихся в атмосфере, воде, твердых телах,

преобразуют их в электрические сигналы, усиливают и обрабатывают электрические сигналы и преобразуют их в акустическую волну для восприятия информации слуховой системой человека. Кроме того, электрические сигналы с выхода приемника подаются на аудиомагнитофон для регистрации акустической информации. Типовая структура акустического приемника приведена на рис. 6.4.

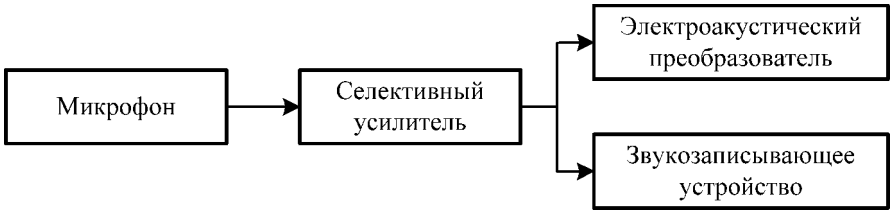

Рис. 6.4. Структурная схема акустического приемника

7 ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

7.1 Задачи инженерно-технической защиты информации

Инженерно-техническая защита информации – одна из основных компонент комплекса мер по защите информации, составляющей государственную, служебную, коммерческую и личную тайну. Этот комплекс включает нормативно-правовые документы, организационные и технические меры, направленные на обеспечение безопасности секретной и конфиденциальной информации. С возрастанием роли информации в обществе повышаются требования ко всем аспектам ее защиты и, прежде всего, к инженерно-технической защите.

Инженерно-техническая защита информации включает комплекс организационных и технических мер по обеспечению безопасности информации техническими средствами. Она решает следующие задачи:

1. Предотвращение проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или изменения.

2. Защита носителей информации от уничтожения в результате воздействия стихийных сил и прежде всего пожара и воды (пены) при его тушении.

3. Предотвращение утечки информации по различным техническим каналам.

Способы и средства решения первых двух задач не отличаются от способов и средств защиты любых материальных ценностей, третья задача решается исключительно способами и средствами инженерно-технической защиты информации.

Инженерно-техническая защита информации представляет собой достаточно быстро развивающуюся область науки и техники на стыке теории систем, физики, оптики, акустики, радиоэлектроники, радиотехники, электро- и радиоизмерений и других дисциплин. Круг вопросов, которыми вынуждена заниматься инженерно-техническая защита, широк и обусловлен многообразием источников и носителей информации, способов и средств ее добывания, а следовательно, и защиты. Для обеспечения эффективной инженерно-технической защиты информации необходимо определить:

- что защищать техническими средствами в конкретной организации, здании, помещении;
- каким угрозам подвергается защищаемая информация со стороны злоумышленников и их технических средств;
- какие способы и средства целесообразно применять для обеспечения безопасности информации с учетом как величины угрозы, так и затрат на ее предотвращение;
- как организовать и реализовать техническую защиту информации в организации.

При решении задач защиты информации объективно существует необходимость учета большого числа различных факторов, что не удается, как правило, сделать на основе здравого смысла. Поэтому основы инженерно-технической защиты должны содержать как теоретические знания, так и методические рекомендации, обеспечивающие решение этих задач.

7.2 Принципы инженерно-технической защиты информации

Так как органам безопасности, занимающимся защитой информации, противостоит разведка с мощным аппаратом и средствами, находящимися на острие научно-технического прогресса, то возможности способов и средств защиты не должны, по крайней мере, уступать возможностям разведки. Исходя их этих исходных положений в основу защиты должны быть положены следующие принципы, аналогичные принципам добывания, а именно:

- непрерывность защиты информации, характеризующая постоянную готовность системы защиты к отражению угроз безопасности информации в любое время;
- активность, предусматривающая прогнозирование действий злоумышленника, разработку и реализацию опережающих мер по защите;
- скрытность, исключающая ознакомление посторонних лиц со средствами и технологией защиты информации;
- целеустремленность, предполагающая сосредоточение усилий по предотвращению угроз утечки наиболее ценной информации;
- комплексное использование различных способов и средств защиты информации, позволяющее компенсировать недостатки одних достоинствами других.

Эти принципы хотя и не содержат конкретных рекомендаций, однако определяют общие требования к способам и средствам защиты информации.

Следующая группа принципов характеризует основные профессиональные подходы к организации защиты информации, обеспечивает рациональный уровень ее защиты и позволяет сократить затраты. Эта группа включает следующие принципы:

- соответствие уровня защиты ценности информации;
- гибкость защиты;
- многозональность защиты, предусматривающая размещение источников информации в зонах с контролируемым уровнем ее безопасности;
- многорубежность зашиты информации на пути движения злоумышленника или распространения носителя.

Первый принцип определяет экономическую целесообразность применения тех или иных мер защиты. Он заключается в том, что затраты на защиту не должны превышать цену защищаемой информации. В противном случае защита нерентабельна.

Так как цена информации – величина переменная, зависящая как от источника информации, так и времени, то во избежание неоправданных расходов защита должна быть гибкой. Гибкость защиты проявляется в возможности изменения степени защищенности в соответствии с изменившимися требованиями к безопасности информации. Степень защищенности информации определяет уровень безопасности информации.

7.3 Методы защиты информации техническими средствами

В общем случае защита информации техническими средствами обеспечивается в следующих вариантах:

- источник и носитель информации локализованы в пределах границ объекта защиты и обеспечена механическая преграда от контакта с ними злоумышленника или дистанционного воздействия на них полей технических средств добывания;
- соотношение энергии носителя и помех на выходе приемника канала утечки такое, что злоумышленнику не удается снять информацию с носителя с необходимым для ее использования качеством;
- злоумышленник не может обнаружить источник или носитель информации;
- вместо истинной информации злоумышленник получает ложную, которую он принимает как истинную.

Эти варианты реализуют следующие методы защиты:

- воспрепятствование непосредственному проникновению злоумышленника к источнику информации с помощью инженерных конструкций и технических средств охраны;

- скрытие достоверной информации;
- «подсовывание» злоумышленнику ложной информации.

Классификация методов защиты представлена на рис. 7.1.

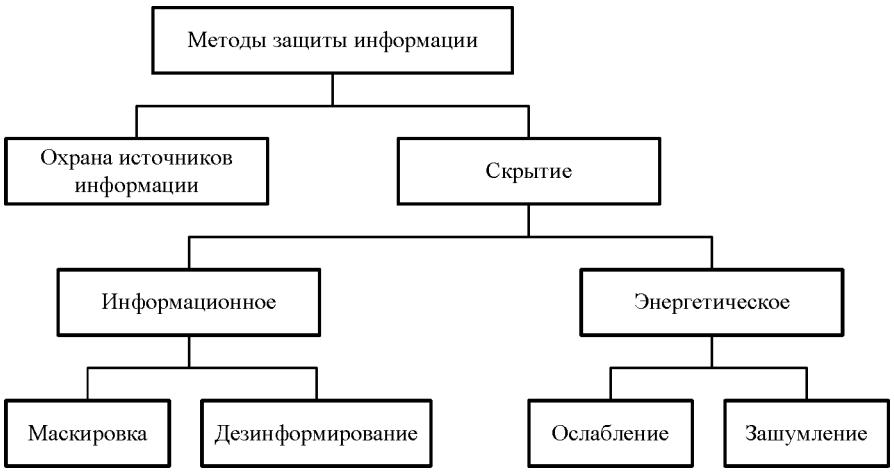

Рис. 7.1. Классификация методов защиты информации

Применение инженерных конструкций и охрана – наиболее древний метод защиты людей и материальных ценностей. Способы защиты на основе инженерных конструкций в сочетании с техническими средствами охраны также распространены в настоящее время. Совокупность этих способов образуют так называемую физическую защиту. Но этот термин нельзя считать удачным, так как иные методы защиты информации с помощью технических средств также основываются на физических законах. Учитывая, что основу рассматриваемого метода составляют инженерные конструкции и технические средства охраны, целесообразно его определить как инженерная защита и техническая охрана объектов (ИЗТОО).

Основной задачей ИЗТОО является недопущение (предотвращение) непосредственного контакта злоумышленника или сил природы с объектами защиты. Под объектами защиты понимаются как люди и материальные ценности, так и носители информации, локализованные в пространстве. К таким носителям относятся бумага, машинные носители, фото- и кинопленка, продукция, материалы и т. д., то есть все, что имеет четкие размеры и вес. Носители информации в виде электромагнитных и акустических полей, электрического тока не

имеют четких границ и для защиты информации на этих носителях методы инженерной защиты не приемлемы – поле с информацией нельзя хранить, например, в сейфе. Для защиты информации на таких носителях применяют методы скрытия информации.

Скрытие информации предусматривает такие изменения структуры и энергии носителей, при которых злоумышленник не может непосредственно или с помощью технических средств выделить информацию с качеством, достаточным для использования ее в собственных интересах.

Различают информационное и энергетическое скрытие. Информационное скрытие достигается изменением или созданием ложного информационного портрета семантического сообщения, физического объекта или сигнала.

Информационным портретом можно назвать совокупность элементов и связей между ними, отображающих смысл сообщения (речевого или данных), признаки объекта или сигнала. Элементами дискретного семантического сообщения, например, являются буквы, цифры или другие знаки, а связи между ними определяют их последовательность. Информационными портретами объектов наблюдения, сигналов и веществ являются их эталонные признаковые структуры.

Возможны следующие способы изменения информационного портрета:

- удаление части элементов и связей, образующих информационный узел (наиболее информативную часть) портрета;
- изменение части элементов информационного портрета при сохранении неизменности связей между оставшимися элементами;
- удаление или изменение связей между элементами информационного портрета при сохранении их количества.

Изменение информационного портрета объекта вызывает изменение изображения его внешнего вида (видовых демаскирующих признаков), характеристик излучаемых им полей или электрических сигналов (признаков сигналов), структуры и свойств веществ. Эти изменения направлены на сближение признаковых структур объекта и окружающего его фона, в результате чего снижается контрастность изображения объекта по отношению к фону и ухудшаются возможности его обнаружения и распознавания.

Но при изменении информационного портрета информация не воспринимается не только злоумышленником, но и ее санкционированным получателем. Следовательно, для санкционированного по-

лучателя информационный портрет должен быть восстановлен путем дополнительной передачи ему удаленных элементов и связей или алгоритма (ключа) этих изменений

В условиях рынка, когда производитель вынужден рекламировать свой товар, наиболее целесообразным способом информационного скрытия является исключение из рекламы или открытых публикаций наиболее информативных сведений или признаков – информационных узлов, содержащих охраняемую тайну.

К информационным узлам относятся принципиально новые технические, технологические и изобразительные решения и другие достижения, которые составляют ноу-хау. Изъятие из технической документации информационных узлов не позволит конкуренту воспользоваться информацией, содержащейся в рекламе или публикациях.

Этот широко применяемый способ позволяет:

- существенно уменьшить объем защищаемой информации и тем самым упростить проблему защиты информации;
- использовать в рекламе новой продукции сведения о ней, не опасаясь разглашения.

Например, вместо защиты информации, содержащейся в сотнях и тысячах листов технической документации, разрабатываемой для производства новой продукции, защите подлежат всего несколько десятков листов с информационными узлами.

Другой метод информационного скрытия заключается в трансформации исходного информационного портрета в новый, соответствующий ложной семантической информации или ложной признаковой структуре, и «навязывании» нового портрета органу разведки или злоумышленнику. Такой метод защиты называется дезинформированием.

Принципиальное отличие информационного скрытия путем изменения информационного портрета от дезинформирования состоит в том, что первый метод направлен на затруднение обнаружения объекта с информацией среди других объектов (фона), а второй — на создании на этом фоне признаков ложного объекта.

Дезинформирование относится к числу наиболее эффективных способов защиты информации по следующим причинам:

- создает у владельца защищаемой информации запас времени, обусловленный проверкой разведкой достоверности полученной информации;

- последствия принятых конкурентом на основе ложной информации решений могут быть для него худшими по сравнению с решениями, принимаемыми при отсутствии добываемой информации.

Однако этот метод защиты практически сложно реализовать. Основная проблема заключается в обеспечении достоверности ложного информационного портрета. Дезинформирование только в том случае достигнет цели, когда у разведки (злоумышленника) не возникнут сомнения в истинности подсовываемой ему ложной информации. В противном случае может быть получен противоположный эффект, так как при раскрытии разведкой факта дезинформирования полученная ложная информация сузит область поиска истинной информации. Поэтому к организации дезинформирования необходимо относиться очень серьезно, с учетом того что потребители информации отчетливо представляют ущерб от дезинформации и при малейших сомнениях будут перепроверять информацию с использованием других источников.

Дезинформирование осуществляется путем подгонки признаков информационного портрета защищаемого объекта под признаки информационного портрета ложного объекта, соответствующего заранее разработанной версии. От тщательности подготовки версии и безукоризненности ее реализации во многом зависит правдоподобность дезинформации. Версия должна предусматривать комплекс распределенных во времени и в пространстве мер, направленных на имитацию признаков ложного объекта. Причем чем меньше при дезинформации используется ложных сведений и признаков, тем труднее вскрыть ее ложный характер.

Различают следующие способы дезинформирования:

- замена реквизитов защищаемых информационных портретов в том случае, когда информационный портрет объекта защиты похож на информационные портреты других «открытых» объектов и не имеет специфических информативных признаков. В этом случае ограничиваются разработкой и поддержанием версии о другом объекте, выдавая в качестве его признаков признаки защищаемого объекта. Например, в настоящее время большое внимание уделяется разработкам продукции двойного применения: военного и гражданского. Распространение информации о производстве продукции сугубо гражданского использования является надежным прикрытием для вариантов военного назначения;

- поддержание версии с признаками, заимствованными из разных информационных портретов реальных объектов. Применяется в тех случаях, когда в организации одновременно выполняется несколько закрытых тем. Путем различных сочетаний признаков, относящихся к

различным темам, можно навязать противоположной стороне ложное представление о ведущихся работах без имитации дополнительных признаков;

- сочетание истинных и ложных признаков, причем ложными заменяется незначительная, но самая ценная часть информации, относящейся к защищаемому объекту;
- изменение только информационных узлов с сохранением неизменной остальной части информационного портрета.

Как правило, используются различные комбинации этих вариантов.

Другим эффективным методом скрытия информации является энергетическое скрытие. Оно заключается в применении способов и средств защиты информации, исключающих или затрудняющих выполнение энергетического условия разведывательного контакта.

Энергетическое скрытие достигается уменьшением отношения энергии (мощности) сигналов, т. е. носителей (электромагнитного или акустического полей и электрического тока) с информацией, и помех. Уменьшение отношения сигнал/помеха (слово «мощность», как правило, опускается) возможно двумя методами: снижением мощности сигнала или увеличением мощности помехи на входе приемника.

Воздействие помех приводит к изменению информационных параметров носителей: амплитуды, частоты, фазы. Если носителем информации является амплитудно-модулированная электромагнитная волна, а в среде распространения канала присутствует помеха в виде электромагнитной волны, имеющая одинаковую с носителем частоту, но случайную амплитуду и фазу, то происходит интерференция этих волн. В результате этого значения информационного параметра (амплитуды суммарного сигнала) случайным образом изменяются и информация искажается. Чем меньше отношение мощностей, а следовательно, амплитуд, сигнала и помехи, тем значительнее значения амплитуды суммарного сигнала будут отличаться от исходных (устанавливаемых при модуляции) и тем больше будет искажаться информация.

Атмосферные и промышленные помехи, которые постоянно присутствуют в среде распространения носителя информации, оказывают наибольшее влияние на амплитуду сигнала, в меньшей степени – на его частоту. Но ЧМ-сигналы имеют более широкий спектр частот. Поэтому в функциональных каналах, допускающих передачу более широкополосных сигналов, например, в УКВ диапазоне, передачу информации осуществляют, как правило. ЧМ сигналами как более помехоустойчивыми, а в узкополосных ДВ, СВ и КВ диапазонах – АМ сигналами.

В общем случае качество принимаемой информации ухудшается с уменьшением отношения сигнал/помеха.

Наиболее жесткие требования к качеству информации предъявляются при передаче данных (межмашинном обмене): вероятность ошибки знака по плановым задачам, задачам статистического и бухгалтерского учета оценивается порядка- 100-10"6, по денежным данным -10"8-1(У . Для сравнения, в телефонных каналах хорошая слоговая разборчивость речи обеспечивается при 60-80%, т. е. требования к качеству принимаемой информации существенно менее жесткие. Это различие обусловлено избыточностью речи, которая позволяет при пропуске отдельных звуков и даже слогов восстанавливать речевое сообщение. Вероятность ошибки знака 10° достигается при его передаче двоичным АМ сигналом и отношении мощности сигнала к мощности флуктуационного шума на входе приемника приблизительно 20, при передаче ЧМ сигналом – около 10. Для обеспечения разборчивости речи порядка 85% превышение амплитуды сигнала над шумом должно составлять около 10 дБ, для получения удовлетворительного качества факсимильного изображения – приблизительно 35 дБ, качественного телевизионного изображения – более 40 дБ.

В общем случае при уменьшении отношения сигнал/помеха до единицы и менее качество информации настолько ухудшается, что она не может практически использоваться. Для конкретных видов информации и модуляции сигнала существуют граничные значения отношения сигнал/помеха, ниже которых обеспечивается энергетическое скрытие информации.

Так как разведывательный приемник в принципе может быть приближен к границам контролируемой зоны организации, то значения отношения сигнал/помеха измеряются, прежде всего, на границе этой зоны. Обеспечение на границе зоны значений отношения сигнал/помеха ниже минимально допустимой величины гарантирует безопасность защищаемой информации от утечки за пределами контролируемой зоны.

7.4 Классификация каналов утечки информации

Канал утечки информации отличается от функционального канала передачи получателем информации. Если получатель санкционированный, то канал функциональный, в противном случае – канал утечки. Классификация каналов утечки информации дана на рис. 7.2.

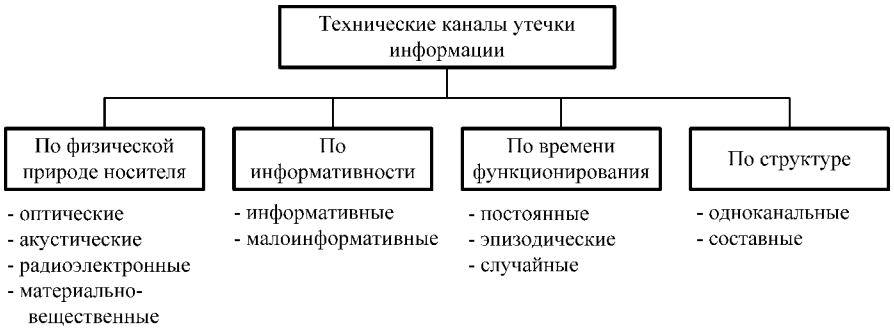

Рис. 7.2. Классификация каналов утечки информации

Основным классификационным признаком технических каналов утечки информации является физическая природа носителя. По этому признаку они делятся на:

- оптические;
- радиоэлектронные;
- акустические;
- материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле в диапазоне 0,46-0,76 мкм (видимый свет) и 0,76-13 мкм (инфракрасные излучения).

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон колебаний носителя этого вида чрезвычайно велик: от звукового диапазона до десятков ГГц.

В соответствии с видами носителей информации радиоэлектронный канал целесообразно разделить на 2 подвида: электромагнитный, носителями информации в котором являются электрическое, магнитное и электромагнитное поля, и электрический канал, носитель информации в котором – электрический ток.

Носителями информации в акустическом канале являются механические упругие акустические волны в инфразвуковом (менее 16 Гц), звуковом (16 Гц -20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот, распространяющиеся в атмосфере, воде и твердой среде.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы организации вещественных носителей с защищаемой информацией,

прежде всего, выбрасываемых черновиков документов и использованной копировальной бумаги, забракованных деталей и узлов, демаскирующих веществ. Последние в виде твердых, жидких и газообразных отходов или промежуточных продуктов содержат вещества, по которым в принципе можно определить состав, структуру и свойства новых материалов или восстановить технологию их получения.

По информативности каналы утечки делятся на информативные и неинформативные. Информативность канала оценивается ценностью информации, которая передается по каналу.

По времени проявления каналы делятся на постоянные, периодические и эпизодические. В постоянном канале утечка информации носит достаточно регулярный характер. Например, наличие в кабинете источника опасного сигнала может привести к передаче из кабинета речевой информации до момента обнаружения этого источника. Периодический канал утечки может возникнуть при условии, например, размещения во дворе неукрытой продукции, демаскирующие признаки о которой составляют тайну, во время пролетов разведывательных космических аппаратов. К эпизодическим каналам относятся каналы, утечка информации в которых имеет случайный разовый характер.

Канал утечки информации, состоящий из передатчика, среды распространения и приемника, является одноканальным. Однако возможны варианты, когда утечка информации происходит более сложным путем – по нескольким последовательным или параллельным каналам. При этом используется свойство информации переписываться с одного носителя на другой. Например, если в кабинете ведется конфиденциальный разговор, то утечка возможна не только по акустическому каналу через стены, двери, окна, но и по оптическому – путем съема информации лазерным лучом со стекла окна или по радиоэлектронному с использованием установленной в кабинете радиозакладки. В двух последних вариантах образуется составной канал, образованный из последовательно соединенных акустического и оптического (на лазерном луче) или акустического и радиоэлектронного (радиозакладка – среда распространения – радиоприемник) каналов. Для повышения дальности канала утечки может также использоваться ретранслятор, совмещающий функции приемника одного канала утечки информации и передатчика следующего канала. Например, для повышения дальности подслушивания с использованием радиозакладки можно разместить ретранслятор в портфеле, сдаваемом якобы на хранение в камеру хранения закрытого предприятия.

Как любой канал связи, канал утечки информации характеризуется следующими основными показателями:

- пропускной способностью;
- дальностью передачи информации.

Пропускная способность канала связи оценивается количеством информации, передаваемой по каналу в единицу времени с определенным качеством.

По ширине полосы частот пропускания каналы делятся на узкополосные и широкополосные. Стандартный телефонный канал для передачи речевой информации имеет полосу 300-3400 Гц и относится к узкополосным, шириной 8 МГц для передачи телевизионных сигналов – к широкополосным. Чем шире канал, тем больше информации можно передать за единицу времени. Так как для добывания информации с требуемым качеством необходимо обеспечить на входе приемника канала минимально допустимое для каждого вида информации и носителя отношение сигнал/помеха, то это отношение достигается на различном удалении от источника сигнала, в зависимости от мощности сигнала и помехи, а также величины (коэффициента) ослабления (затухания) сигнала в канале. Носители информации существенно отличаются по величине затухания в среде распространения: в наибольшей степени уменьшается энергия акустической волны, в наименьшей – электромагнитная волна в длинноволновом диапазоне частот.

Учебное издание

Александр Иванович Моисеев
Денис Борисович Жмуров

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебник

Редактор Ю.Н. Литвинова
Компьютерная доверстка А.В. Ярославцева

Подписано в печать 05.04.2013 г. Формат 60x84 1/16.
Бумага офсетная. Печать офсетная. Печ. л. 11,25.
Тираж 20 экз. Заказ . Арт. – 7/2013.

Самарский государственный
аэрокосмический университет.
443086 Самара, Московское шоссе, 34.

Изд-во Самарского государственного
аэрокосмического университета.
443086 Самара, Московское шоссе, 34.