

Содержание

1.1 Понятие об информации как предмете защиты	1
1.1.1 Основные свойства информации как предмета защиты	1
1.1.2 Виды защищаемой информации	2
1.2 Демаскирующие признаки объектов защиты	3
1.2.1 Классификация демаскирующих признаков	4
1.2.2 Видовые демаскирующие признаки	5
1.2.3 Демаскирующие признаки сигналов	7
1.3 Демаскирующие признаки веществ	10
1.4 Источники и носители информации	11
1.4.1 Виды источников и носителей информации	11
1.4.2 Принципы записи и схема информации с носителя	12
1.5 Источники сигналов	13
1.5.1 Источники функциональных сигналов	13
1.5.2 Побочные излучения и наводки	14

1.1 Понятие об информации как предмете защиты

Согласно закону «Об информации, информатизации и защите информации» информация это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [1]. защите подлежит секретная и конфиденциальная информация.

К секретной относится информация, содержащая государственную тайну. Ее несанкционированное распространение может нанести ущерб интересам государственных органов, организациям, субъектам и РФ в целом.

Конфиденциальной является информация, содержащую коммерческую или иную тайну (служебную, профессиональную, промышленную), разглашение (передача, утечка) которых может нанести вред интересам собственника информации. Правовой режим защищаемой информации устанавливается ее собственником на основе законов о коммерческой, профессиональной тайне, государственной службе и других законодательных актов.

1.1.1 Основные свойства информации как предмета защиты

С точки зрения защиты информация обладает следующими основными свойствами.

1) **Информация доступна человеку**, если она содержится на материальном носителе, следовательно, **объектами защиты являются материальные носители информации**: либо источники либо переносчики либо получатели. Параметры носителя информации определяют условия и способы хранения информации. Физическая природа носителей информации (источника, переносчика, получателя) может быть как одинаковой, так и разной.

2) **Ценность информации оценивается степенью полезности ее для пользователя (собственника, владельца, получателя)**. Информация может обеспечивать ее пользователю определенные преимущества: приносить прибыль, уменьшать риск в его деятельности и т.д. Ценность информации всегда конкретна. Нет ценной информации вообще. Информация полезна или вредна для конкретного пользователя. Поэтому при защите информации, прежде всего необходимо определить, круг лиц (фирм, государств), заинтересованных в защищаемой информации. Это позволяет осуществить рациональный выбор мер по защите информации.

3) **Информацию можно рассматривать как товар**, поскольку она может покупаться и продаваться. Цена информации связана с ее ценностью. Она складывается из себестоимости и прибыли.

Себестоимость определяется расходами владельца информации на ее получение путем. Прибыль от использования информации может быть получена в самых различных формах:

за счет продажи информации на рынке;

путем материализации информации в новых свойствах продукции или технологиях, приносящих прибыли; сокращения сроков разработки новой продукции и т.д.

Денежное выражение прибыли не является самой распространенной формой. Одним из важных направлений ее использования информации является снижение риска при принятии решений.

4) **Ценность информации изменяется во времени**. Распространение информации и ее использование приводят к изменению ее ценности и цены. Характер изменения ценности во времени зависит от вида информации. Для научной информации эта зависимость часто имеет волнообразный вид.

Ценность большинства видов информации, циркулирующей в обществе, со временем уменьшается – информация стареет. Старение информации C_0 в первом приближении можно аппроксимировать выражением вида:

$$C_0(t) = C_0 \exp(-2.3t/\tau_{\text{жиз}})$$

где C_0 – ценность информации в момент ее возникновения (создания);

t – время от момента возникновения информации до момента ее использования;

$\tau_{\text{жиз}}$ – продолжительность жизненного цикла информации (от момента возникновения до момента устаревания).

За время жизненного цикла ценность информации уменьшается до 0.1 первоначальной величины.

В зависимости от продолжительности жизненного цикла коммерческая информация классифицируется следующим образом:

- оперативно-тактическая, теряющая ценность примерно по 10% в день (например, информация выдачи краткосрочного кредита, предложения по приобретению товара в срок до одного месяца и др.);
- стратегическая информация, ценность которой убывает примерно 10% в месяц (сведения о партнерах, о долгосрочном кредите, развитии и т. д.).

5. **Невозможно объективно (без учета полезности ее для потребителя, владельца, собственника) оценить количество информации**

Для определения количества информации в теории информации используется энтропийный подход, в соответствии с которым количество информации оценивается мерой уменьшения у получателя неопределенности (энтропии) выбора или ожидания событий после получения информации. Количество информации в передаваемом по каналам связи сообщении из N независимых символов определяется по формуле Шеннона [4]:

$$I = N \sum_{i=1}^n P_i \log_2 P_i$$

где P_i – вероятность появления в сообщении символа i ;

n – количество символов в алфавите языка.

Количество получаемой информации о событии тем больше, чем меньше вероятность этого события. Оно измеряемое в двоичных элементах (в битах, байтах) зависит только от количества и статистики символов, но не зависит от содержания сообщения.

Если информацию трактовать как знания, то количество информации, извлекаемой человеком из сообщения, можно оценить степенью изменения его знаний. Структурированные знания, представленные в виде понятий и отношений между ними, называются **тезаурусом**. Тезаурус имеет иерархическую структуру. Понятия и отношения, группируясь, образуют другие, более сложные понятия и отношения.

Тезаурусы человека и любой организационной структуры представляют их капитал. Поэтому они стремятся, во-первых, к сохранению (безопасности) своего тезауруса, а во-вторых, к его увеличению. Тезаурус владельца информации может быть увеличен путем получения знаний владельцем как за счет проведения собственных исследований или разработок, так и за счет их законного или незаконного приобретения.

В природе и обществе происходит процесс как увеличения тезауруса владельца в результате получения информации, так и выравнивания тезаурусов разных владельцев, путем поступления информации от тезауруса большого объема тезаурусу меньшего объема. При выравнивании тезаурусов коммерческая цена информации убывает.

6. **При копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а цена снижается**. После снятия копии с документа информация в нем не меняется. Однако при этом увеличивается число ее законных и незаконных пользователей и в соответствии с законами рынка цена информации снижается.

1.1.2 Виды защищаемой информации

По содержанию любая информация может быть отнесена к семантической (смысловой) или к информации о признаках материального объекта – признаковой.

Семантическая информация на языке национального общения представляется в виде упорядоченной последовательности знаков (букв, цифр, нероглифов) алфавита этого языка и записывается на любом материальном носителе. Сущность семантической информации не зависит от характеристик носителя. Для регистрации и консервации семантической информации изыскиваются носители, обеспечивающие все более высокую плотность записи и меньшее энергопотребление.

Признаковая информация описывает конкретный материальный объект на языке его признаков. Описание объекта содержит признаки его внешнего вида, излучаемых им полей и элементарных частей, состава и структуры веществ, из которых состоит объект. В зависимости от вида описания объекта признаковая информация делится на информацию о внешнем виде (видовых признаках), о его полях (признаках сигналов), о структуре и составе его веществ (признаках веществ).

Классификация информации по содержанию представлена на рис. 1.1.

Защищаемая информация неоднородна по содержанию, объему и ценности. Защита будет рациональной в том случае, когда уровень защиты и затраты на неё, соответствуют количеству и качеству информации. Для обеспечения

рациональной защиты необходимо структурировать конфиденциальную информацию, т. е. разделить ее на некоторые информационные элементы.

Информационный элемент представляет собой информацию на носителе с достаточно четкими границами, и удовлетворяет следующим требованиям:

- принадлежит конкретному источнику (документу, человеку, образцу продукции и т. д.);
- содержится на отдельном носителе;
- имеет конкретную цену.



Рис. 1.1. Классификация информации, защищаемой техническими средствами

Структурирование информации проводится путем последовательной многоуровневой детализации защищаемой информации. Детализация начинается с перечня сведений, содержащих тайну, и предусматривает иерархическое разделение информации в соответствии со структурой тематических вопросов, охватывающих все аспекты деятельности организации.

Пример укрупненной типовой структуры конфиденциальной информации, составляющей коммерческую тайну, приведен на рис. 1.2.



Рис. 1.2. Пример структурирования конфиденциальной информации

Защита структурированной информации является более конкретной задачей, чем защита информации вообще. Она позволяет выявить на каждом уровне иерархии, какие информационные элементы необходимо защищать, прежде всего, исходя из их ценности, кто или что является источником и носителем этого элемента. Для каждого элемента информации можно выявить возможные угрозы его безопасности и определить, какие способы и средства целесообразно применить для обеспечения его защиты.

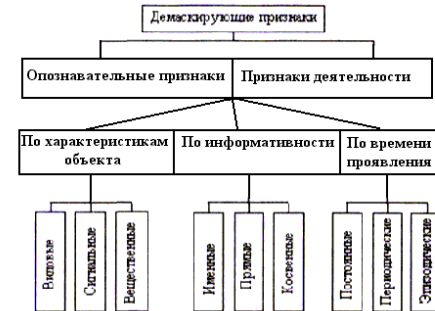
1.2 Демаскирующие признаки объектов защиты

Задача защиты признаков информации решается, прежде всего, путем предотвращения обнаружения признаков, по которым может быть распознан защищаемый объект и определены его характеристики. Признаки, позволяющие отличить один объект от другого, называются **демаскирующими**. Однотипные признаки разных объектов не относятся к демаскирующим.

1.2.1 Классификация демаскирующих признаков

В общем случае демаскирующие признаки объектов разделяются на опознавательные признаки и признаки деятельности. Опознавательные признаки описывают объекты в статическом состоянии: его назначение, принадлежность, параметры. Признаки деятельности объектов характеризуют этапы и режимы функционирования объектов, например, этапы создания новой продукции: научные исследования, подготовка к производству, изготовление новой продукции, ее испытания и т. д.

Классификация признаков приведена на рис. 1.3.



1.3. Классификация демаскирующих признаков

Совокупность демаскирующих признаков представляет собой модель объекта, описывающую его внешний вид, изучаемые им поля, внутреннюю структуру и химический состав содержащихся в нем веществ.

Демаскирующие объекты классифицируются по характеристикам на видовые, сигнальные и вещественные, по информативности на именные, прямые и косвенные, по времени проявления - постоянные, периодические и эпизодические.

Демаскирующие признаки характеристик объекта можно разделить на три группы:

- видовые признаки (форма объекта, его размеры, детали объекта, тон, цвет и структура его поверхности и др.);
- признаки сигналов (акустические, электромагнитные, световые и т.п.); их параметры, характер изменения во времени);
- признаки веществ (определенные химические элементы, характер отходов производства, потребляемые сырье и материалы, радиоактивные вещества и т.п.).

Важнейшим показателем признака является его информативность, которая значением вероятности обнаружения объекта по конкретному признаку. Чем признак более индивидуален, т. е. принадлежит меньшему числу объектов, тем он более информативен.

Признаки, принадлежащие только данному объекту, называют именными. Их информативность равна 1. Если признак может принадлежать группе объектов, его называют прямым. Информативность прямых признаков колеблется в пределах (0-1). Признаки, непосредственно не принадлежащие объекту, но отражающие свойства и состояние объекта, называются косвенными. Эти признаки являются, обычно, результатом воздействия рассматриваемого объекта на окружающую среду.

По времени проявления признаки разделяются на постоянные (не изменяющиеся в течение жизненного цикла объекта), периодические (сезонные, связанные с каким либо технологическим) и эпизодические (проявляющиеся при определенных условиях, например, при авариях).

Признаковая структура объекта представляет собой набор независимых или зависимых признаков, о которых достоверно известно, что они относятся к рассматриваемому объекту.

Каждый i -ый признак обеспечивает возможность обнаружения объекта с вероятностью P_i . Если признаковая структура содержит n независимых признаков, то вероятность обнаружения объекта хотя бы по одному из этих признаков можно найти по формуле

$$Q_n = 1 - \prod_{i=1}^n (1 - P_i).$$

Например, если $P_1=0.017$, $P_2=0.08$, $P_3=0.021$, $P_4=0.03$ и $P_5=0.015$, то вероятность обнаружения объекта хотя бы по одному из этих признаков существенно выше - более 0.14.

1.2.2 Видовые демаскирующие признаки

1) Видовые демаскирующие признаки описывают внешний вид объекта. Они выявляются в результате анализа внешнего вида модели объекта - изображения его на экране оптического приемника (сетчатке глаза человека, фотосимке, экране телевизионного приемника, прибора ночного видения, радиолокатора и т. д.). Вследствие различий модели и оригинала состав и информативность видовых демаскирующих признаков зависят от объекта наблюдения, условий наблюдения и характеристик оптического приемника.

Наибольшее количество информативных видовых демаскирующих признаков получают при визуальном-оптическом наблюдении объектов в видимом диапазоне.

2) Основные видовые демаскирующие признаки объектов в видимом свете:

- 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.

Наиболее устойчивую и информативную структуру образуют геометрические и фотометрические характеристики объектов, так как они присущи данному объекту и относятся к его прямым признакам.

Форма объекта является одним из его основных демаскирующих признаков, и прежде всего для искусственных объектов правильных геометрических форм. Размеры приобретают значение основного демаскирующего признака для объектов примерно одинаковой формы. Детали объекта (их количество, характер расположения) позволяют отличить данный объект от подобных ему по форме.

Тени объектов при прямом солнечном освещении являются важными демаскирующими признаками объекта при наблюдении его сверху. Различают два вида теней - 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.

Важнейшим свойством поверхности объекта, определяющим его цвет и яркость, является коэффициент отражения поверхности для различных длин волн в видимом, инфракрасном и радиодиапазоне. Например, коэффициент отражения листья летом в ближнем инфракрасном диапазоне в 3-5 раз выше, чем в видимом, а бетонных и асфальтовых покрытий отличаются незначительно.

Отражательные свойства объектов описываются коэффициентами (спектральными и интегральными) и индикаторной отраженности. Индикаторная отраженности 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. Поверхность считается гладкой и отражение от нее зеркальное, если отношение среднеквадратичного значения высоты неровностей h к длине волны λ менее единицы, шероховатой с диффузным отражением, если более двух. Следовательно, шероховатая поверхность в видимом свете может в ИК-диапазоне выглядеть как гладкая. Диффузное отражение присуще мелкоструктурным элементам, таким, как песок, свежесвалившийся снег. Большинство объектов земной поверхности имеют смешанную индикаторную отраженности.

3) Любые тела излучают электромагнитные волны в ИК-диапазоне. Величина энергии, излучаемая любым телом с температурой T пропорциональна в соответствии с формулой Стефана-Больцмана величине T^4 . В ближней (0.75-1.3 мкм) и средней (1.2-3.0 мкм) зонах ИК-излучения мощность (собственного) излучения объектов значительно меньше мощности отраженного от объекта потока солнечной энергии. С переходом в длинноволновую область ИК-диапазона мощность собственного излучения нагретых Солнцем объектов становится соизмеримой с мощностью отраженной ими солнечной энергии. Максимум энергии ИК-излучения тел при температуре воздуха летом находится в диапазоне 3-5 и 8-14 мкм. Чем выше температура тела, тем больше излучаемая энергия, а ее максимум смещается в сторону более коротких волн. Поэтому нагретые тела с помощью соответствующих приборов могут наблюдаться в полной, с точки зрения человека-наблюдателя, темноте.

При оценке излучений и инфракрасном диапазоне необходимо учитывать теплопроводность материалов объектов наблюдения. Нагреваясь от солнечных лучей, они добавляют к отраженному свету долю собственных излучений. В связи с этими свойствами в инфракрасном диапазоне появляется дополнительный признак - распределение температуры различных участков поверхности объекта по отношению к температуре фона.

Глаз человека не воспринимает лучи в инфракрасном диапазоне. Поэтому видовые демаскирующие признаки в этом диапазоне получают с помощью специальных приборов (ночного видения, тепловизоров). Они имеют худшее разрешение, чем глаз человека. 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.

Таким образом, к демаскирующим признакам объекта в ИК-диапазоне можно отнести геометрические характеристики внешнего вида объекта (форма, размеры, детали поверхности), а также распределение температур по поверхности объекта.

4) В радиодиапазоне наблюдается более сложная картина, чем при отражении света. Отражательные возможности поверхности в этом диапазоне зависят не только от размеров неровностей поверхности, но и ее электропроводности и конфигурации относительно направления падающей волны. Большая часть суши отражает электромагнитную волну в радиодиапазоне диффузно, спокойная водная поверхность - зеркально.

Радиолокационное изображение объектов сложной формы (автомобили, 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 перестройки радиоволны внутри конструкции возвращают их к радиолокатору.

Наибольшей отражающей способностью в направлении антенны радиолокационной станции обладают конструкции в виде 2-4-х жестко связанных между собой взаимно перпендикулярных металлических или металлизированных плоскостей. Такие конструкции называются уголовыми 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».

Обобщенные результаты анализа радиолокационных изображений местности и объектов приведены в табл. 1.1 и 1.2. [15].

Таблица 1.1.

Вид отражающей поверхности	Характер отражения	Тон радиолокационного изображения
Гладкая водная	Зеркальный	Темный
Травяной покров	Диффузный, умеренной интенсивности с понижением ее при уменьшении емкостной электропроводности	Умеренно темный
Отдельные группы деревьев	Диффузный, высокой интенсивности	Светлый, с зернистой структурой
Естественные уголовые отражатели (скальные выступы, льды)	Интенсивный	Очень светлый
Сельскохозяйственные угодья	Диффузный, различной интенсивности	От умеренно-темного до светлого

Таблица 1.2.

Объекты	Интенсивность отражения	Характер радиолокационного отражения
Шоссейные дороги	Низкая	Линии с характерными изгибами мн, по тону слабо отличаются от окружающей местности
Железные дороги	Низкая	Линии с характерными изгибами
Мосты, переправы	Высокая	Короткий прямой светлый отрезок поперек реки
Промышленные объекты	Высокая	Площадь светлого тона с резкими границами
Силовые линии электропередач	Высокая (от металлических опор)	Линейное расположение светлых точек
Аэродромы, ВПП, аэродромные постройки	От поверхности аэродрома и ВПП — низкая, от построек - высокая	Площадь аэродрома умеренно-темная, ВПП и постройки - темные
Самолеты и другая техника	Высокая	Отдельные светлые точки, расположенные на местности в определенном порядке

Примечание: ВПП - взлетно-посадочная полоса аэродрома.

Основными видовыми демаскирующими признаками объектов радиолокационного наблюдения являются:

- эффективная площадь рассеяния;

- геометрические и яркостные характеристики (форма, размеры, яркость, детали);
- электропроводность, поверхность.

Отражающие свойства объекта в радиодиапазоне характеризуются эффективной площадью рассеяния (ЭПР). Эффективная площадь рассеяния равна площади плоской идеально проводящей поверхности, ориентированной перпендикулярно направлению облучения, которая создает в месте нахождения приемной антенны радиолокационной станции такую же плотность потока мощности, как и реальный объект.

Эффективная площадь рассеяния человека составляет около 0.1-0.5 м², легкового автомобиля - около 1-5 м², грузового автомобиля 3-10 м². В связи с зависимостью значений эффективной площади рассеяния от пространственного положения объекта относительно направления на радиолокационную станцию имеет место большой разброс данных для одних и тех же объектов.

Отражающая способность земной поверхности изменяется в широких пределах в зависимости от ее шероховатости, диэлектрической проницаемости материала и длины волны. Средняя удельная (деленная на геометрическую площадь облучаемой поверхности) ЭПР песчаной почвы составляет 0.003, дуга летом - 0.01, кустарника - 0.03, лесного массива - 0.05 [88].

Электромагнитная волна отражается не только от поверхности объекта, но и от более глубоких его слоев. Проникающая способность в дециметровом диапазоне для сухой почвы, например, может составлять 1-2 м.

Видовые демаскирующие признаки в радиодиапазоне могут быть получены 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.

Выводы:

а) Максимальное количество признаков внешнего вида объектов можно получить в видимом оптическом диапазоне с помощью фотоприемников с высоким разрешением (глаз человека, фотопленка).

б) В инфракрасном диапазоне и в особенности в радиодиапазоне 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. Поэтому на радиолокационном изображении будут отсутствовать многие детали объекта, наблюдаемые на его изображении в оптическом диапазоне. Однако в инфракрасном и радиодиапазонах проявляются дополнительные признаки, которые в видимом диапазоне отсутствуют.

в) Видовые демаскирующие признаки объектов образуют признаковые структуры, отличающиеся в различных диапазонах длин электромагнитных волн. Эти свойства видовых демаскирующих признаков используются при комплексном добывании информации и их необходимо учитывать при организации защиты.

г) Любим объект наблюдения можно рассматривать как сложный объект, состоящий из более простых объектов, которые могут содержать демаскирующие признаки сложного объекта. Вычленение из объекта защиты демаскирующих объектов позволяет решать вопросы защиты информации о нем путем защиты информации о демаскирующих объектах.

1.2.3 Демаскирующие признаки сигналов

В радиоэлектронике под сигналом понимается изменяющаяся физическая величина, однозначно отображающая сообщение. Сигнал, несущий информацию о физической величине, состоянии исследуемого объекта или процесса, называется информационным [112].

В задачах защиты информации **сигналом** называют распространяющийся в пространстве носитель, физические параметры которого содержат информацию об объекте защиты. Это могут быть собственные излучения объекта, отраженные от него поля и волны, разного рода поля и токи устройств обработки информации. Источники сигналов с защищаемой информацией могут рассматриваться как автономные объекты защиты, так и объекты комплексной защиты. Классификация сигналов представлена на рис. 1.4.



Рис. 1.4. Классификация сигналов

К аналоговым сигналам относятся сигналы, уровень (амплитуда) которых может принимать произвольные значения в определенном для сигнала интервале.

Большинство аналоговых сигналов имеют более сложную форму. Периодические (повторяющиеся через время T_k - период) сигналы произвольной формы могут быть представлены в соответствии с формулой Фурье в виде суммы гармонических колебаний:

$$s(t) = C_0 + \sum_{k=1}^n C_k \cos(k\omega t - \varphi_k),$$

где C_0 - постоянная составляющая сигнала;

C_k - амплитуда k -ой гармоники сигнала ($k = 1, 2, \dots, n$);

$k\omega$ и φ_k - частота и фаза k -ой гармоники сигнала.

Параметры ряда Фурье вычисляются по соответствующим формулам [70]. Ряд Фурье представляет собой математическую модель периодического сигнала, также как любой цвет может быть разложен на составляющие красный, зеленый и синий цвета.

Совокупность гармонических составляющих сигнала образуют его **спектр**.

Амплитуда каждой спектральной составляющей характеризует энергию соответствующей гармоники основной частоты сигнала. Чем выше скорость изменения амплитуды сигнала, тем больше в его спектре высокочастотных гармоник. Полоса частот, в которой сосредоточена основная часть, например, 95% энергии, называется **шириной спектра** ΔF . Графическое изображение спектра периодического сигнала представлено на рис. 1.5.

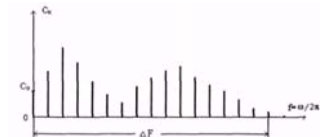


Рис. 1.5. Спектр периодического аналогового сигнала

Спектр непериодического аналогового сигнала сплошной. В соответствии с изменением амплитуды аналогового сигнала меняется его энергия или мощность (так как мощность пропорциональна квадрату амплитуды).

Энергию сигнала характеризуют средней и мгновенную мощностью. Десятичный логарифм отношения максимальной мощности сигнала к минимальной называется динамическим диапазоном сигнала.

Аналоговый сигнал описывается набором параметров, являющихся его признаками. К ним относятся:

- частота или диапазон частот;
- фаза сигнала;
- длительность сигнала;
- амплитуда или мощность сигнала;
- ширина спектра сигнала;
- динамический диапазон сигнала.

Дискретные сигналы характеризуются конечным множеством его мгновенных значений. Наиболее широко применяется двоичный (бинарный) дискретный сигнал: в ЭВМ, в телеграфии, при передаче данных. Информационные

сигналы, циркулирующие в ЭВМ IBM PC, имеют два уровня амплитуды: низкий (L-уровень, 0 В) и высокий (H-уровень, 5 В). Осциллограмма бинарного сигнала показана на рис. 1.6.

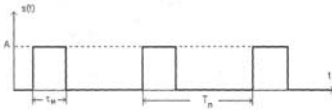


Рис. 1. 6. Осциллограмма бинарного сигнала

Дискретный сигнал характеризуется следующими параметрами: амплитудой A и мощностью P , длительностью импульса τ_n , периодом T_n или частотой $F_n = 1/T_n$ повторения импульсов (для периодических дискретных сигналов), шириной спектра сигнала ΔF_c , скважностью импульсов $\alpha = \tau_n / T_n$.

Спектр дискретного периодического сигнала содержит бесконечное количество убывающих по амплитуде гармоник. Для бинарного периодического сигнала фрагмент спектра показан на рис. 1.7.

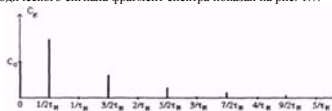


Рис. 1. 7 Спектр бинарного периодического сигнала

Он характеризуется следующими свойствами:

- форма огибающей спектра описывается функцией $|\sin x/x|$;
- амплитуда гармоник C_n имеет нулевое значение в точках k/T_n , $k=1,2,...$;
- в области частот спектра $(0-1/\tau_n)$ располагаются $\alpha - 1$ гармоник;
- постоянная составляющая сигнала равна A/α .

Большая часть энергии сигнала сосредоточена в области частот $0-1/\tau_n$, поэтому ширину спектра бинарного периодического сигнала приблизительно оценивают по формуле: $\Delta F_c \approx 1/\tau_n$.

При прохождении дискретных сигналов по электрическим цепям радиотехнических средств с ограниченной полосой пропускания их форма искажается и крутизна фронтов импульсов уменьшается. Прямоугольный импульс приобретает колоколообразную форму. В результате этого граница между формой аналогового и дискретного сигналов размывается.

Проведение $B = \Delta F_c \tau_n$ называется **базой сигнала**. Если $B \approx 1$, то сигнал узкополосный, при $B \gg 1$ - сигнал широкополосный. По ширине спектра аналогового сигнала можно судить о характере передаваемой информации, а по ширине спектра дискретного сигнала о скорости передачи информации. Например, стандартный речевой сигнал, передаваемый по телефонной линии, имеет ширину спектра 300-3400 Гц, звуковой - 16-20000 Гц, телевизионный - 6-8 МГц и т. д.

По физической природе сигналы могут быть акустическими, электрическими, магнитными, электромагнитными (в радиодиапазоне - радиосигналы), корпускулярными (в виде потоков элементарных частиц) и материально-вещными, например, пахучие добавки в газ подает сигнал об его утечке.

По виду передаваемой информации сигналы делятся на речевые, телеграфные, телекодвые, факсимильные, телевизионные, о радиоактивных излучениях и условные.

Вид информации, содержащейся в сигнале, изменяет его демаскирующие признаки: форму, ширину спектра, частотный и динамический диапазон.

По времени проявления сигналы могут быть регулярными, время появления которых получательно информации известно, например, сигналы точного времени, и случайные, когда это время неизвестно. Статистические характеристики проявления случайных сигналов во времени могут представлять собой достаточно информативные демаскирующие признаки источников, прежде всего, об их принадлежности и режимах функционирования. Например, появление в помещении радиосигнала во время ведения в нем переговоров может с достаточно высокой вероятностью служить демаскирующим признаком заданного устройства с акустическим автоматом.

По аналогии с демаскирующим объектом можно рассматривать понятие **демаскирующего сигнала**, факт обнаружения которого может служить информативным признаком объекта защиты. Например, лобовые излучения на определенной частоте конкретной радиостанции, могут служить в качестве ее прямого, а иногда именного признака.

1.3 Демаскирующие признаки вещества

Потребительские свойства продукции зависят не только от конструктивных и схемотехнических решений, но и от свойств материалов (веществ), из которых она создается. Поэтому состав, свойства и технология получения веществ с этими свойствами вызывают большой интерес у специалистов, а информация о них может быть чрезвычайно дорогой.

Для обеспечения безопасности информации о веществах с новыми свойствами важно представлять признаки, по которым злоумышленник может воссоздать вещество с новыми свойствами. Классификация основных признаков веществ представлена на рис. 1.8.



Рис.1.8. Классификация признаков веществ

По физическому составу вещества могут быть однородными твердыми (кусковыми, порошковыми), жидкими, газообразными и неоднородными, в виде взвесей, эмульсий и т. п.

По химическому составу вещества делятся на органические и неорганические. В свою очередь органические вещества - на углеводороды, кислородсодержащие и азотсодержащие, неорганические - на оксиды, кислоты, основания и соли.

Изотопный состав характеризует стабильность или нестабильность ядер веществ или, другими словами, наличие радиоактивных изотопов у рассматриваемого вещества.

Ионный состав вещества определяется при нахождении его в ионизированном состоянии, называемой плазмой и возникающем под действием высокой температуры или тазового разряда (для газообразных веществ).

Строение веществ описывают на макроскопическом, микроскопическом и субмикроскопическом уровнях, на последнем в виде кристаллической решетки, макромолекулы, молекулы, субатомных частиц и атомов.

Механические свойства веществ характеризуют их прочность на сжатие и растяжение, твердость, вязкость, плотность, пористость, пластичность, смачиваемость, непрочность и т.д.

Химические свойства вещества определяются по результатам взаимодействия его с другими веществами.

Акустические свойства определяют скорость передачи и поглощения звука в веществе.

Тепловые свойства оцениваются по температуре фазовых переходов из одного состояния в другое, теплопроводности, теплоемкости и др.

Лучистые (оптические, рентгеновские и др.) свойства вещества описываются коэффициентами и спектральными характеристиками пропускания, отражения, преломления, возможностями по дифракции, поляризации и интерференции лучей света в инфракрасном, видимом и ультрафиолетовом диапазонах, а также гамма-излучением.

Электропроводность, величины термо-э.д.с, окислительно-восстановительные потенциалы, потенциалы ионизации, диэлектрическая и магнитная проницаемости и т. п. характеризуют электрические и магнитные свойства вещества.

Ядерные свойства вещества оцениваются по массе изотопов, массе и периоду полураспада радиоактивных частиц и др.

Признаки, по которым можно обнаружить и распознать вещество, т. е. определить его состав, структуру и свойства, в смеси других веществ, являются демаскирующими. Демаскирующие признаки нового вещества и технологии его изготовления содержится не только в конечном продукте, но и в исходных и промежуточных продуктах технологического процесса получения этого вещества. Вещества, содержащие демаскирующие признаки другого вещества или технологии его изготовления, называем **демаскирующими веществами**. Например, новые духи отличаются от прототипов составом. Демаскирующими признаками новых духов являются характеристики запаха, а демаскирующими веществами - компоненты духов в определенном соотношении. Оригинальные духи отличаются от подделки также рядом признаков, в том числе стойкостью сохранения запаха. Стойкость запаху придают специальные дорогие добавки, которые являются демаскирующими веществами оригинала. Физико-химический анализ демаскирующих веществ дает информацию о составе, структуре, свойствах и технологии изготовления продукции, информация о которой составляет государственную или коммерческую тайну.

Потенциальные возможности обнаружения и распознавания демаскирующих веществ зависят от их концентрации в смеси добываемых веществ. Минимально допустимые значения концентрации демаскирующих веществ, исключающие получение злоумышленниками защищаемой информации, используются в качестве норм при обеспечении безопасности информации о признаках веществ.

1.4 Источники и носители информации

1.4.1 Виды источников и носителей информации

С точки зрения защиты информации ее **источниками** являются субъекты и объекты, от которых информация может поступить к несанкционированному получателю (злоумышленнику). Очевидно, что ценность этой информации определяется информативностью источника. Основными источниками информации являются следующие:

- люди;
- документы;
- продукция;
- измерительные датчики;
- интеллектуальные средства обработки информации;
- черновики и отходы производства;
- материалы и технологическое оборудование.

Информативность **людей** как источников информации существенно различается. Наиболее информированы руководители организаций, их заместители и ведущие специалисты. Каждый сотрудник организации владеет конфиденциальной информацией, как правило, в объеме, превышающем необходимый для выполнения его функциональных обязанностей. Распространение конфиденциальной информации между сотрудниками организации является одним из проявлений процессов выравнивания тезаурусов. В результате неформальных межличностных отношений (дружественных, приятельских) конфиденциальная информация может поступать к посторонним лицам. Тщеславные люди непреднамеренно разглашают конфиденциальные сведения в публичных выступлениях и беседах с целью продемонстрировать свою эрудицию или заинтересовать собеседника. Кроме непреднамеренного разглашения конфиденциальной информации, часть сотрудников (по американской статистике - около 25%) по различным личным мотивам готовы продать известные им секреты и ищут контактов с зарубежной разведкой или представителями конкурента.

Потому в интересах локализации ценной информации необходимо учитывать объективные процессы распространения информации внутри организации и даже за ее пределами (через родственников, друзей и приятелей, через сотрудников налоговой полиции, муниципалитетов, префектур, в арбитражном суде и т. д.). Даже эффективная защита информации, но только в пределах организации, не гарантирует ее безопасность.

Под **документом** понимается зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. К документам относятся служебная информация, научные публикации в открытой и закрытой печати, статьи в газетах и журналах о деятельности организации или ее сотрудников, реклама, отчеты сотрудников, конструкторская и технологическая документация и т. д.

Документы относятся к наиболее информативным источникам. Они содержат, как правило, достоверную информацию в отработанном виде, в частности, если документы полисаны или утверждены. Информативность публикаций изменяется в широком диапазоне оценок: от очень высокой (например, когда описывается открытие) до преуменьшенной или непреднамеренной дезинформации. К последней, например, относятся публикации с недостаточно проверенными и достоверными результатами.

Большинство технических средств сбора, обработки, хранения и передачи информации нельзя отнести к источникам информации, так как они представляют собой лишь инструмент для преобразования входной информации. Исключения составляют лишь **датчики** различных измерительных устройств и **интеллектуальные средства** обработки, генерирующие информацию.

Продукция является источником информации о признаках. Ноу-хау нового изделия могут содержаться во внешнем виде, например, в форме автомобиля, расцветке ткани, моделях одежды, узле механизма, в параметрах излучаемых полей (сигналов радиостанции или радиолокатора), в составе и структуре материала (броневой стали, ракетного топлива, духов или лекарств).

Любой творческий и производственный процесс сопровождается отходами. Научные работники создают эскизы будущих изделий или пробы веществ, при производстве (опытном или промышленном) возможен брак или технологические газообразные, жидкие или твердые отходы. Отходы производства в случае небрежного отношения с ними (сбрасывания на свалку без предварительной сортировки, сжигания или режис бумаж и т. д.) могут привести к утечке ценной информации. Такой возможности способствуют психологические предпосылки сотрудников, серьезно не воспринимających отходы как источники секретной (конфиденциальной) информации.

Информативными могут быть не только продукция и отходы ее производства, но и **исходные материалы и сырье**, а также используемое оборудование. Если среди поставляемых фирме материалов и сырья появляются новые наименования, то специалисты конкурента могут определить по ним изменения в создаваемой продукции или технологических процессах.

Как правило, передача информации от источника получателю осуществляется через посредника - **носителя информации**. Информация источника также содержится на носителе. Т.е. носителями информации являются материальные объекты, обеспечивающие ее запись, хранение и передачу в пространстве и времени. Известны четыре вида носителей информации:

- люди;
- материальные тела (макрочастицы);
- поля и волны;
- элементарные частицы (микрочастицы).

Человек как носитель информации ее запоминает и пересказывает получателю в письменном виде или устно. При этом он может полученную от источника информацию преобразовать в соответствии с собственным толкованием ее содержания, искажая смысл. Кроме того, человек может быть также носителем других носителей информации - документов, продукции и т. д.

Материальные тела являются носителями различных видов информации. Прежде всего, материальные тела содержат информацию о своем составе, структуре (строении), о воздействии на них других материальных тел. Например, по остаточным изменениям структуры бумажки восстанавливают подожженные надписи, по изменению структуры металла двигателя определяют его заводской номер, перебитый автомобильными ворами. Материальные тела (например, глиняные таблички, береста, камень, бумага) использовались людьми для консервации и хранения информации в течение всей истории человечества. И в настоящее время бумага является самым распространенным носителем семантической информации. Однако четко прослеживается тенденция замены бумаги машинными носителями (магнитными, полупроводниковыми, светочувствительными и др.), но бумага еще длительное время останется наиболее массовым и удобным носителем, прежде всего, семантической информации.

Носителями информации являются различные поля и волны. Из известных полей в качестве носителей применяются акустические, электрические, магнитные и электромагнитные (в диапазоне видимого и инфракрасного света, в радиодиапазоне). Информация содержится в значениях параметров полей. Если поля представляют собой волны, то информация содержится в амплитуде, частоте и фазе.

Из многочисленных элементарных частиц в качестве носителей информации используются электроны, образующие статические заряды и электрический ток, а также частицы (электроны и ядра легких) радиоактивных излучений. Попытки использования для переноса информации других элементарных частиц с лучшей проникающей способностью (меньшим затуханием в среде распространения), например, нейтроны, не привели пока к положительным результатам.

1.4.2 Принципы записи и съема информации с носителя

Материализация (запись) любой информации производится путем изменения параметров носителя. Запись информации на вещественные носители производится путем изменения их физической структуры и химического состава. Запись информации на носители в виде полей и электрического тока осуществляется путем изменения их параметров. Непрерывное изменение параметров сигналов в соответствии со значениями первичного сигнала называется **модуляцией**, дискретное - **манипуляцией**. Первичным является сигнал от источника информации. Если меняются значения амплитуды аналогового сигнала, то модуляция называется амплитудной (АМ), частоты - частотная (ЧМ), фазы - фазовая (ФМ). Частотная и фазовая модуляция мало различаются, поскольку при фазовой модуляции меняется непосредственно фаза, а при частотной ее первая производная по времени - частота.

При модуляции дискретных сигналов в качестве модулируемых применяются и другие параметры: длительность импульса, частота его повторения и др. С целью уплотнения информации на носителе и экономии тем самым энергии носителя применяют сложные (с использованием различных параметров сигнала) виды модуляции. Модулируемое колебание называется несущим.

В соответствии с формулой Фурье изменение формы сигнала при модуляции приводит к изменению спектра модулированного сигнала. Чем выше максимальная частота спектра модулирующего сигнала $F_{\text{сиг}}$, тем шире спектр модулированного сигнала. Количественное значение увеличения ширины спектра этого сигнала зависит от вида модуляции и ширины спектра модулирующего (первичного) сигнала. Ширина модулированного синусоидального сигнала равна:

- для АМ: $\Delta F_{\text{АМ}} = 2F_{\text{сиг}}$;
- для ЧМ: $\Delta F_{\text{ЧМ}} \gg F_{\text{сиг}}$;
- для ФМ: $\Delta F_{\text{ФМ}} \approx \Delta F_{\text{ЧМ}}$.

Для радиосвязи ширина спектра ЧМ-сигнала составляет 100-150 кГц вместо около 7 кГц для АМ речевого сигнала. Поэтому ЧМ-сигналы не применяют из-за «тесноты» в эфире в длинноволновом, средневолновом и даже коротковолновом диапазонах волн. ЧМ-вещание ведется в УКВ диапазоне. ЧМ-сигналы обладают существенно большей помехоустойчивостью, чем АМ-сигналы. Спектры ФМ и ЧМ-сигналов мало отличаются по ширине.

Выделение информации из модулированного электрического сигнала производится путем обратных преобразований - демодуляции его в детекторе (демодуляторе) приемника. Из-за влияния помех модулирующие (при передаче) и

демодулированные (при приеме) сигналы будут отличаться. В общем случае любые преобразования сигнала с воздействием на его информационные параметры изменят записанную в нем информацию. Степень изменения зависит от отношения сигнал/помеха на входе демодулятора. При достаточно большом превышении мощности сигнала над мощностью помехи искажения информации столь незначительные, что количество и качество информации практически не меняются.

Помехоустойчивость дискретных сигналов выше, чем аналоговых, так как искажения дискретных сигналов возникают в тех случаях, когда изменения параметра сигнала превышают половину величины интервала между соседними значениями параметра. Для повышения достоверности передачи информации наряду с увеличением энергии носителя информации используют другие методы защиты дискретной информации от помех, прежде всего, помехоустойчивое кодирование. При помехоустойчивом кодировании каждому элементу дискретной информации (букве, цифре, любому другому знаку) ставится в соответствие кодовая комбинация, содержащая дополнительные (избыточные) двоичные символы. Эти дополнительные символы позволяют обнаруживать искажения и исправлять в зависимости от избыточности кода ошибочные символы различной кратности. Существует большое количество видов кодов, повышающих помехоустойчивость сообщений для различных условий среды распространения носителей. Однако следует иметь, что платой за повышение помехоустойчивости кодированных сигналов является уменьшение скорости передачи информации.

Любое сообщение в общем случае можно описать с помощью трех основных параметров: динамическим диапазоном D_c , шириной спектра частот ΔF_c и длительностью передачи T_c . Произведение этих трех параметров называется **объемом сигнала** $V_c = D_c \Delta F_c T_c$. В трехмерном пространстве объем сигнала можно представить в виде параллелепипеда (рис. 1.9).

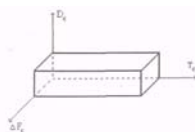


Рис. 1.9. Графическое представление объема сигнала

Для обеспечения неискаженной передачи сообщения объемом V_c , необходимо чтобы характеристики среды распространения и непосредственно приемника соответствовали ширине спектра и динамическому диапазону сигнала.

Если полоса частот среды распространения или приемника уже полосы сигнала, то для обеспечения неискаженной передачи сигнала объемом V_c уменьшают его ширину спектра. При этом для сохранения $V_c = \text{const}$ соответственно увеличивают время передачи T_c . Для неискаженной передачи сообщения в реальном масштабе времени полоса пропускания приемника должна соответствовать ширине спектра сигнала.

1.5 Источники сигналов

Объекты, излучающие сигналы, содержат источники сигналов. Источники сигналов, создаваемые и применяемые для обеспечения связи между санкционированными абонентами, называют функциональными источниками сигналов.

Существует большая группа источников, от которых могут распространяться несанкционированные сигналы с защищаемой информацией и которые возникают случайно или создаются злоумышленниками. Эти сигналы несут угрозу безопасности информации, их условно называют опасными. Условность объясняется тем обстоятельством, что сигналы функциональных источников (функциональные сигналы) при приеме их злоумышленниками также небезопасны для передаваемой информации. Но, во-первых, без функциональных сигналов невозможна связь, а, следовательно, нормальная жизнь современного общества, и, во-вторых, передача информации с их помощью может контролироваться абонентами. Функциональные сигналы становятся опасными, если не приняты меры по безопасности информации.

1.5.1 Источники функциональных сигналов

К источникам функциональных сигналов относятся

- передатчики систем связи;

- передатчики радиотехнических систем;
- излучатели акустических сигналов гидролокаторов;
- условные сигналы.

Системы и средства связи образуют наиболее многочисленную и разнообразную группу источников сигналов с семантической информацией. К системам и средствам связи относятся системы и средства радиосвязи, проводной, радиодетальной, космической и оптической связи, ионосферной, тропосферной и метеорной радиосвязи.

Источниками радиосигналов, излучаемых в окружающее пространство, являются стационарные и мобильные радиопередающие устройства систем радиосвязи, а электрических сигналов, передаваемых по проводам, - телефонные, телеграфные, факсимильные аппараты, ПЭВМ, объединенные в локальные сети организации, модемы аппаратуры передачи данных. Электрические сигналы, передаваемые по проводам кабелей, формируют телефонные, телеграфные, факсимильные аппараты, передающие телевизионные камеры кабельного телевидения, ПЭВМ, модемы аппаратуры передачи данных. Перехват сигналов средств связи представляет один из эффективных и широко распространенных методов добывания информации.

К радиотехническим системам и средствам относятся средства радиолокации, радионавигации, радиотелесметрии, радиотелеуправления, а также радиопротиводействия (радиоэлектронной борьбы).

Радиолокационные станции, предназначенные для наблюдения воздушного пространства и земной поверхности в радиодиапазоне. Возможности радиолокаторов по добыванию информации определяются в основном параметрами их сигналов и распределением их энергии в пространстве (направленности антенны).

Радио- и гидролокационные станции создают техническую основу для противоракетной, противолодочной и противолодочной обороны, поэтому параметры сигналов новейших локоаторов вызывают большой интерес у разведки других государств. Сигнальные признаки разрабатываемых радио и акустических средств интересуют также конкурентов в России и других государствах, создающих подобную технику.

Радионавигационные средства и системы предназначены для определения местоположения объектов на суше, воде, в воздухе и в космосе. Радиотелесметрические средства и системы обеспечивают измерение и передачу различных физических величин удаленных объектов, а средства и системы радиотелеуправления - управление ими.

К радиотехническим системам и средствам, характеристики сигналов которых интересуют органы добывания разведки, относятся также системы и средства радиопротиводействия (радиоэлектронной борьбы), предназначенные для нарушения систем управления войсками и оружием противника в военное время.

Передача коротких сообщений производится также условными сигналами. В качестве сигналов могут использоваться любые объекты наблюдения и излучения. Необходима только предварительная договоренность между источниками и получателями информации о содержании условного сигнала. Например, условными формами часто пользуются люди во время конфиденциального разговора по открытому телефону, условными сигналами (паролями) обмениваются незнакомые люди при конфиденциальной встрече.

1.5.2 Побочные излучения и наводки

Угрозу хищения информации путем ее утечки создают сигналы, случайно возникающие в результате побочных излучений и наводок. Если эти сигналы содержат защищаемую информацию, то они относятся к опасным.

Источниками опасных сигналов являются радио и электротехнические элементы и устройства в принципе любых радиоэлектронных и электрических устройств и приборов. В некоторых средствах звукозаписи, звукофикации и передачи информации предусматриваются дополнительные меры по безопасности информации, исключающие появление опасных сигналов. Однако технические меры по защите информации существенно повышают стоимость этих радиоэлектронных средств и делают их неконкурентными на рынке. Поэтому основной тенденцией предотвращения утечки информации из незащищенных радиоэлектронных средств является применение дополнительных средств защиты информации.

Радиоэлектронные и электрические средства и системы, содержащие потенциальные источники опасных сигналов, разделяют на основные и вспомогательные. Основные средства и системы обеспечивают обработку, хранение и передачу защищаемой информации, вспомогательные технические средства и системы (ВТСС) - остальной информации. К основным средствам и системам организации относятся:

- средства (телефонные аппараты, коммутационные щиты, кабели и провода) городской телефонной сети, размещенные на территории организации;
- внутриобъектовая автоматическая телефонная сеть;
- система оперативной телефонной связи руководства организации со структурными подразделениями;
- система диспетчерской связи для оперативного проведения совещаний;
- система громкоговорящей связи;
- вычислительная техника (ПЭВМ, принтеры, сканеры, серверы);
- аппаратура передачи данных;
- системы внутриобъектового оповещения;
- система звукофикации залов заседаний и помещений для совещаний;
- средства телеграфной и факсимильной связи;

- система объектового промышленного телевидения;
- средства аудио- и видеозаписи, используемые для документирования защищаемой информации.
- ВТСС включают:
 - городскую и объектовую радиотрансляционную сеть;
 - систему электрософистики;
 - технические средства охранной и пожарной сигнализации;
 - телевизионные средства наблюдения системы охраны объекта;
 - бытовые аудио- и видеомикрофоны;
 - бытовые радиоприемники и телевизоры;
 - средства электропитания;
 - бытовые электроприборы;
 - электронные средства оргтехники.

Назначение большинства из указанных средств и систем ясно из приведенных названий и сфер применения. Не все указанные системы и средства размещаются в любой организации, но их количество и разнообразие достаточно для самого серьезного отношения к обеспечению безопасности информации в помещениях с ними.

Средства источники опасных сигналов можно классифицировать исходя из их физической природы :

- акустоэлектрические преобразователи;
- излучатели низкочастотных сигналов;
- излучатели высокочастотных сигналов;
- паразитные связи и наводки.

К акустоэлектрическим преобразователям относятся физические устройства, элементы, детали и материалы, способные под действием переменного давления акустической волны создавать эквивалентные электрические сигналы. Свойства акустоэлектрических преобразователей используются по своему функциональному назначению для создания микрофонов различных типов. Существуют разнообразные радиоэлектронные и электрические элементы и устройства, обладающие так называемым «микрофонным эффектом», т. е. способными преобразовывать акустические сигналы в электрические. Это приводит к появлению в радио- и электрических устройствах, содержащих акустоэлектрические преобразователи, опасных сигналов, которые создают предпосылки для утечки информации.

Классификация акустоэлектрических преобразователей, создающих опасные сигналы, приведена на рис.

1.10.



Рис. 1.10. Классификация акустоэлектрических преобразователей

Электрические сигналы, модулированные акустическими сигналами, возникают в индуктивных акустоэлектрических преобразователях в результате перемещений под действием акустических волн индуктивностей (катушек с металлической проволокой) в полях (магнитных и электрических) или при изменениях геометрических размеров катушек и их сердечников.

Наибольшую чувствительностью обладают электродинамические акусто-электрические преобразователи в виде динамических головок громкоговорителей (см. рис. 1.12).

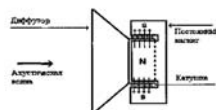


Рис. 1.11. Схема электродинамического громкоговорителя

Сущность преобразования состоит в следующем. Под давлением акустической волны соединенная с диффузором катушка в виде картонного цилиндра с намотанной на нем тонкой проволокой перемещается в магнитном поле,

создаваемом постоянным магнитом цилиндрической формы. В соответствии с законом электромагнитной индукции в катушке (контуре) возникает электродвижущая сила (ЭДС), величина которой пропорциональна громкости звука. Опасные сигналы на концах катушки достигают величин в 5–15 мВ, достаточных для их распространения за пределы помещения, здания и даже территории. Поэтому неработающие, но непосредственно подключаемые к радиотрансляционной сети громкоговорители могут выполнять функцию микрофона и передавать информацию разговоров в помещении на достаточно большое расстояние.

Аналогичный эффект возникает в электромагнитных акустоэлектрических преобразователях. К ним относятся электромагниты электромеханических звонков и калосей телефонных аппаратов, шаговые двигатели вторичных часов, кнопочные извещатели ручного вызова пожарной службы охраняемого объекта и др. Электрические сигналы индуцируются в катушках электромагнитов этих устройств в результате изменений напряженности создаваемых ими полей. Эти процессы вызваны изменениями под действием акустической волны воздушного зазора между сердечником и якорем электромагнита или статора (неподвижной части) и ротора (подвижной) части электродвигателя.

Передача бытовых радио и электроприборов, в которых возникают подобные процессы и которые устанавливаются в служебных и жилых помещениях, достаточно велика. К ним относятся: телефонные аппараты с электромеханическими звонками, вторичные электрические часы системы единого времени предприятия или организации, вентиляторы и др. Уровни опасных сигналов в этих случаях зависят от конструкции конкретного типа средства и их значения имеют значительный разброс. Например, опасные сигналы, создаваемые звонковой цепью телефонного аппарата, могут достигать значений долей и единиц мВ.

Магнитоstriction проявляется в изменении магнитных свойств ферромагнитных веществ (электротехнической стали и ее сплавов) при их деформировании (растяжении, сжатии, изгибании, кручении). Такое явление называется обратным эффектом магнитоstriction, в отличие от прямого, который заключается в изменении геометрических размеров и объема ферромагнитного тела при помещении его в магнитное поле. В результате магнитоstriction под действием акустической волны изменяется магнитная проницаемость сердечников индуктивности (контуров, дросселей, трансформаторов) радио- и электротехнических устройств, что приводит к эквивалентному изменению значений индуктивности и модуляции протекающих через них высокочастотных сигналов.

Опасные сигналы емкостных акустоэлектрических преобразователей возникают в результате механического изменения под давлением акустической волны зазоров между пластинными конденсаторами и проводниками, приводящие к эквивалентному изменению значений сосредоточенных и распределенных емкостей схем радиотехнических средств.

Широко распространены акустоэлектрические преобразователи, использующие свойства некоторых кристаллических веществ (кварца, селенитовой соли, титаната и ниобата бария и др.) создавать заряды на своей поверхности при ее деформировании, в том числе под действием акустической волны. Эти вещества применяются для создания функциональных акустоэлектрических преобразователей, например, пьезоэлектрических микрофонов. Опасные сигналы создают пьезоэлектрические вещества, в основном кварцы, применяемые в генераторах для стабилизации частоты, а также пьезоэлементы вибраторов и датчиков технических средств охраны.

Опасные сигналы на выходе акустоэлектрических преобразователей могут:

- распространяться по проводам, выходящим за пределы контролируемой зоны;
- модулировать другие, более мощные электрические сигналы, к которым возможен доступ злоумышленников.

Техническую основу для реализации первой угрозы создают, например, неработающие громкоговорители городской ретрансляционной сети и звонковая цепь телефонных аппаратов устаревших, но широко еще применяемых типов (ТА-68М, ТА-72М, ТАН-70-2, ТАН-76-3, ТА-1146, ТА-1162, ТА-1164 и др.). Головка громкоговорителя непосредственно подключается к кабелю (двухжильному проводу) при приеме первой программы городской ретрансляционной сети через согласующий трансформатор, который повышает амплитуду опасных сигналов до 30–40 мВ. Сигнал такой амплитуды может распространяться по проводам ретрансляционной сети на значительное расстояние, достаточное для создания информации злоумышленником за пределами территории организации. Однако если в радиотрансляционной сети идет передача речи или музыки, то сигналы этой передачи, имеющие существенно большую (в 100–200 раз) амплитуду и совпадающий диапазон частот, подавляют опасные сигналы. Поэтому работающие громкоговорители могут быть и мешают работе людей, но исключают утечку информации из помещений через акустоэлектрические преобразователи в громкоговорителях.

Иная ситуация с акустоэлектрическими преобразователями в телефонных аппаратах. Телефонные линии постоянно подключены к источнику тока напряжением порядка 60 В. Хотя опасные сигналы на выходе звонковой цепи составляют единицы и доли мВ, их нетрудно разделить с помощью фильтра от значительно более высокого напряжения постоянного тока в телефонной линии. Постоянный ток фильтр не пропускает, а опасные сигналы с речевой информацией от акустоэлектрических преобразователей с частотами в звуковом диапазоне проходят через фильтр с малым ослаблением, а затем усиливаются до необходимого значения.

Опасными сигналами на выходе акустоэлектрических преобразователей, имеющими даже весьма малые значения (доли милливольт) нельзя пренебрегать. Во-первых, чувствительность современных радиоприемников и усилителей электрических сигналов превышает в десятки и сотни раз уровни наиболее распространенных опасных сигналов, а, во-вторых, маломощные опасные сигналы могут модулировать более мощные опасные электрические сигналы и поля и таким образом увеличивать дальность распространения опасных сигналов. Например, если опасные сигналы попадают в цепи генераторов (гетеродинов) любого радио или телевизионного приемника, то они модулируют гармонические колебания этих генераторов по амплитуде или частоте и распространяются за пределы помещения уже в виде электромагнитной волны. Также поля опасных сигналов на выходе акустоэлектрических преобразователей, которые сами по

себе из-за малой напряженности не несут большой угрозы безопасности информации, могут наводиться в цепях рядом расположенных радиоэлектронных средств электрические сигналы с аналогичным эффектом.

Опасные поля образуются при протекании по токопроводам радиосредств (проводам индуктивности, монтажным и соединительным проводам, дорожкам печатных плат) электрического тока в звуковом диапазоне частот с конфиденциальной информацией. Источниками таких сигналов могут быть телефонные аппараты, устройства громкоговорящей связи, усилители мощности, аудио- и видеомагнитофоны.

Характер поля зависит от расстояния до его источника. В ближней зоне, в которой расстояние от источника λ поля менее длины волны его колебаний, преобладают в зависимости от вида излучателя электрические или магнитные компоненты так называемого поля индукции. Напряженность компонент поля индукции убывает пропорционально $1/r^3$ и $1/r^2$. В дальней зоне, начиная с расстояния от источника более примерно 6λ , преобладает поле излучения в виде электромагнитной волны, энергия которой делится поровну между электрической и магнитной компонентами. Напряженность электромагнитного изотропного поля убывает с расстоянием пропорционально $1/r$.

Основная часть энергии поля, частоты колебания которого относятся к звуковому диапазону, сосредоточена в ближней зоне. Однако если эти поля несут информацию, то она может быть в результате действия полей на проводники рядом расположенных средств или кабелей переписана на другой носитель, имеющий выход за пределы контролируемой зоны. При повышении частоты поля увеличивается энергия излучения в окружающее пространство.

Источниками **побочных высокочастотных колебаний** являются:

- высокочастотные генераторы, входящие в состав многих радиотехнических средств (телевизоров, радиоприемников, аудио- и видеомагнитофонов, 3-х программных абонентных громкоговорителей);
 - усилительные каскады, в которых при определенных условиях возникают паразитные высокочастотные колебания;
 - нелинейные элементы (диоды, транзисторы и другие активные радиоэлементы), на которые подаются гармонические высокочастотные колебания и электрические сигналы с речевой информацией.
- Высокочастотные генераторы выполняют в радиотехнических функциях генератор гармонических колебаний - гетеродина, необходимых для преобразования частоты, в магнитофонах они создают токи стирания и подмагничивания. Колебания этих генераторов в результате акустоэлектрических преобразований в их элементах (индуктивности, емкостях) или воздействий на генераторы электрических сигналов с информацией, могут быть промодулированы речевыми сигналами и излучаться в окружающее пространство. Например, если под действием акустической волны меняются параметры контура генератора, то происходит частотная модуляция его колебаний.

Паразитные высокочастотные колебания в усилителях возникают при образовании между выходом и входом усилителя положительной обратной связи. В этом случае при попадании через паразитные емкостные и индуктивные связи на вход усилителя сигналов с его выхода с фазой, равной фазе входного сигнала, лавинообразно нарастает амплитуда паразитного колебания на частоте, на которой выполняется равенство фаз. Если частота паразитной генерации расположена вне диапазона частот усилителя, то этот побочный режим работы усилителя может остаться незамеченным при создании и эксплуатации радиоэлектронного средства. Модуляция паразитного колебания происходит аналогично рассмотренным выше способам модуляции функциональных генераторов.

Высокочастотные колебания генерируются не только функциональными или паразитными генераторами радиоэлектронных средств, но высокочастотные колебания могут быть подведены к ним зломущением от внешнего генератора. При одновременном попадании этих высокочастотных колебаний и сигналов с речевой информацией на нелинейные элементы средств (диоды, транзисторы и др.) происходит модуляция высокочастотного колебания речевым сигналом. Наиболее просто этот вариант реализуется при подключении внешнего высокочастотного колебания к проводу телефонного аппарата, установленного в интересующем зломущенника помещении. Промодулированные высокочастотные колебания распространяются в окружающее пространство и могут быть приняты за пределами территории организации.

Многочисленные опасные сигналы создают работающие ПЭВМ, в особенности размещенные в пластмассовых нематериализованных корпусах. Ориентировочные дальности обнаружения радиоизлучений широко распространенных ПЭВМ зарубежного производства приведены в табл. 1.3.

Таблица 1.3.

Блок ПЭВМ	Дальность обнаружения полей, м	
	электромагнитного	электрического
Системный блок	2-40	1-30
Дисплей	25-120	10-55
Клавиатура	15-50	15-30
Печатающее устройство	5-35	10-80

Излучения компьютеров имеют широкий диапазон: от единиц до сотен МГц. Наиболее мощными информативными источниками электромагнитного излучения являются видеоусилитель и электронно-лучевая трубка монитора. Реальная

возможность снятия информации с опасных сигналов ПЭВМ зависит также от вида используемого кода: для последовательного кода вероятность добывания информации достаточно высокая, для параллельного - низкая.

Паразитные связи и наводки характерны для любых радиоэлектронных средств и проводов соединяющих их кабелей. Различают три вида паразитных связей:

- гальваническая;
- индуктивная;
- емкостная.

Гальваническая связь или связь через сопротивление возникает, когда по одним и тем же цепям протекают токи разных источников сигналов. В этом случае происходит проникновение сигналов в не предназначенные для них элементы схемы. Сигналы, несущие конфиденциальную информацию, за счет гальванической связи могут проникать в цепи, имеющие внешний выход. Это создает предпосылки для утечки информации.

Как между цепями относятся, прежде всего, цепи питания и заземления. Функциональный или опасный сигнал может при определенных условиях проникать через цепи питания прибора в сеть электропитания помещения и здания, далее через силовую шину в силовую кабель, по которому подается электроэнергия с подстанции. Кроме того, потребление энергии любым радиоэлектронным средством в текущий момент времени зависит от амплитуды токов, циркулирующих в нем, в том числе токов, несущих полезную информацию. Следовательно, потребляемым средством, может содержать переменную составляющую, соответствующую информационному сигналу. Существенное различие частот электронитания 50 Гц и речевого сигнала позволяет, в принципе, выделить с помощью частотных фильтров опасный сигнал чрезвычайно малой амплитуды на фоне напряжения 220 В. Хотя блок питания сглаживает колебания тока в сети электропитания, вызванные циркулирующими в технических средствах информационными сигналами, но существует реальная возможность утечки информации через цепи питания от звукоусиливающей аппаратуры.

Цепи заземления предназначены для обеспечения защиты электрических сигналов с информацией от помех и наводок путем экранирования проводов или устройств. При воздействии на экраны побочных электрических и электромагнитных полей на экранах возникают заряды, которые для эффективного экранирования необходимо удалить или нейтрализовать. С этой целью экраны «заземляют», т. е. соединяют проводом с малым сопротивлением с поверхностью Земли. В качестве «земли» применяют металлические листы или трубы, зарытые в грунт на глубину 1-2 м для обеспечения хорошего контакта с токопроводящими слоями. Протекающие по цепи заземления опасные сигналы могут перехватываться приемной аппаратурой зломущими.

Паразитные индуктивные и емкостные связи представляют собой физические факторы, характеризующие влияние электрических и магнитных полей, возникающих в цепях любого функционирующего радиоэлектронного средства, на другие цепи в этом или иных средствах.

Паразитная индуктивная связь проявляется следующим образом. В пространстве, окружающем любую цепь, по которой протекает электрический ток I возникает магнитное поле, постоянное или переменное с частотой изменения тока ω . В соседних проводниках, находящихся в переменном магнитном поле, возникает эдс $E = I\omega M$, где M - взаимная индуктивность. Величина M пропорциональна индуктивности являющихся друг на друга элементов цепей и обратно пропорциональна расстоянию между ними. Например, взаимная индуктивность двух прямых медных параллельных проводников длиной 100 м и толщиной 0,02 мм при интервале между ними 2 мм составляет 0,07 мкГн, а при интервале 10 мм - 0,04 мкГн [46].

Емкостная паразитная связь возникает между любыми элементами схемы, прежде всего, между параллельно расположенными проводами, а также точками схемы и корпусом (шасси). Емкостная связь зависит от геометрических размеров элементов цепей и расстояния между ними. Например, емкость между двумя параллельными проводами длиной 100 м и диаметром 0,1 мм уменьшается с 0,75 пф до 0,04 пф при увеличении расстояния между ними с 2 до 50 мм. Для проводов диаметром 2 мм эта емкость при тех же условиях больше и составляет 5-0,07 пф [46].

Из-за паразитных индуктивных и емкостных связей возникают паразитные наводки. Под паразитной наводкой понимается передача электрических сигналов из одного элемента радиосредства в другой, не предусмотренная его схемой и конструкцией [46]. Принципы паразитной наводки иллюстрируются рис. 1.13.

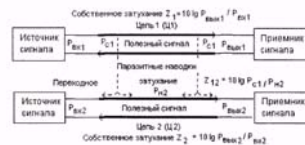


Рис. 1.12. Принципы паразитной наводки

Когда ток проходит по проводникам первой цепи (I1), вокруг них создается магнитное поле, силовые линии которого пронизывают проводники второй цепи (I2). В результате этого по цепи I2 потечет помимо основного его еще и

переходной ток, создающий помеху основному. Защищенность от взаимных помех оценивается так называемым переходным затуханием

$$Z_{12} = 10 \lg P_{c1} / P_{a2},$$

где P_{c1} и P_{a2} - мощность сигналов в 1-й цепи и наводки от них во 2-й цепи.

Переходное затухание для надежной защиты информации должно быть не менее величины $10 \lg P_c / P_{пр}$, где P_c и $P_{пр}$ - мощность сигнала с информацией и чувствительность приемника злоумышленника, перехватывающего наведенный сигнал.

Наводки создают угрозу безопасности информации в случае наводок на цепи, имеющие выход сигналов с подлежащей защите информацией за пределы территории организации. В этом отношении наибольшую угрозу создают наводки в проводах кабелей городской телефонной сети, радиотрансляции, электропитания от сигналов рядом расположенных кабелей внутренней АТС, звукофикации залов или помещений для совещаний, оперативной и диспетчерской связи. Кроме того, наводки даже очень малого уровня могут модулировать высокочастотный сигнал, распространяющийся за пределы организации в виде электромагнитной волны.