**ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ**

**А.А. Титов**

# ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие

Томск – 2010

Федеральное агентство по образованию

**ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)**

Кафедра радиоэлектроники и защиты информации (РЗИ)

**УТВЕРЖДАЮ**

Заведующий кафедрой РЗИ

доктор технических наук, профессор

_____ А.С. Задорин

____ _____2010 г.

# ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие для студентов специальностей
090103 – «Организация и технология защиты информации»
090104 – «Комплексная защита объектов информатизации»
090106 – «Информационная безопасность телекоммуникационных систем»

Разработчик:

Профессор кафедры РЗИ

доктор технических наук

_____А.А. Титов;

Томск – 2010

УДК 004.056

**Титов А.А.**

Инженерно-техническая защита информации: Учебное пособие для студентов специальностей «Организация и технология защиты информации», «Комплексная защита объектов информатизации» и «Информационная безопасность телекоммуникационных систем». – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2010. – 197 с.

Учебное пособие предназначено для изучения основных разделов общепрофессионального курса «Инженерно-техническая защита информации».

Для студентов высших учебных заведений специальностей «Организация и технология защиты информации», «Комплексная защита объектов информатизации» и «Информационная безопасность телекоммуникационных систем».

## ОГЛАВЛЕНИЕ

# ПРЕДИСЛОВИЕ

Изменение социально-экономических отношений в нашей стране, интегрирование в мировое экономическое сообщество повышает роль информационных ресурсов нашего государства. На этом фоне актуальными становятся вопросы обеспечения информационной безопасности Российской Федерации как неотъемлемого элемента национальной безопасности, а защита информации становится одной из приоритетных государственных задач. Основой в решении данной задачи является защита информации от технических разведок и от ее утечки по техническим каналам.

Для несанкционированного добывания информации в настоящее время используется широкий арсенал технических средств, из которых малогабаритные технические средства отражают одно из направлений в развитии современных разведывательных технологий. Выполняемые в портативном, миниатюрном и сверхминиатюрном виде, эти средства аккумулируют в себе новейшие научные, технические и технологические достижения электроники, акустики, оптики, радиотехники и других наук [1]. Такие средства находят широкое применение, как в деятельности правоохранительных органов, так и иностранных технических разведок, в подпольном информационном обеспечении незаконных экономических, финансовых и криминальных организаций. В условиях рыночной экономики появление значительного числа конкурирующих между собой различных структур естественным образом создало определенное пространство, на котором применение подобных устройств технической разведки для добывания информации различной значимости является наиболее вероятным.

В общей проблеме защиты информации от технических разведок и от ее утечки по техническим каналам, комплексное решение которой осуществляется Государственной технической комиссией при Президенте Российской Федерации, подобный класс технических средств разведки имеет свои специфические особенности, связанные с их разведывательными возможностями, факторами , ограничивающими их применение, методами перехвата информации, ее накопления и коммуникации, способами выявления и блокирования устройств и пр. Все эти и другие вопросы являются предметами пристального изучения при подготовке специалистов в области защиты информации.

В предлагаемом учебном пособии рассматриваются свойства информации как предмета защиты, демаскирующие признаки носителей информации, характеристики угроз и методы добывания информации, различные виды технических каналов утечки информации. Пособие предназначено для изучения основных разделов общепрофессионального курса «Инженерно-техническая защита информации» студентами высших учебных заведений специальностей «Организация и технология защиты информации» и «Комплексная защита объектов информатизации»

# 1. ПОНЯТИЕ ИНФОРМАЦИИ КАК ПРЕДМЕТА ЗАЩИТЫ

Термин **информация** появился в русском языке от латинского слова (**informatio** – разъяснение, изложение), и в соответствии с энциклопедическим словарем первоначально означал сведения передаваемые людьми в виде сообщений устным, письменным способом, сигналами, или техническими средствами. В соответствии с терминологией Федерального закона «Об информации, информатизации и защите информации», слово **информация** означает – сведения о лицах, предметах, фактах, событиях и процессах независимо от формы их представления. Значит информация это сведения. Согласно словарю русского языка Ожегова, **сведения – это знания**. Следовательно, в общем случае информация – это знания в самом широком значении этого слова.

Раньше считалось, что когда прекращается литься кровь, наступает мир. Сейчас войны идут постоянно. Эти войны называются информационными. Нет необходимости уничтожать людей и материальные ценности. Можно управлять человеком через информационные каналы, подчинять его себе таким образом, что это подчинение он воспримет как благо. Опасность этого оружие не только в том, что оно носит массовый характер, но и в том, что большинство людей даже не осознают факта его применения. Например, покупая рекламируемый товар, человек думает, что выбор осуществляет он, хотя реально за него это сделал рекламодатель.

Как и в любых войнах в информационных войнах имеется нападающая сторона и обороняющаяся сторона. Оборона в этом случае ведется в двух направлениях. Это защита от информационного воздействия и защита собственной информации.

Решающее значение для исхода информационной войны имеет защита собственной информации. Среди направлений защиты информации выделяют [2]:

- организационно-правовую,
- программно-аппаратную
- инженерно-техническую защиту информации.

Организационно-правовая защита информации осуществляется путем выполнения требований и рекомендаций правовых документов.

Программно-аппаратная защита информации занимается обеспечением средств вычислительной техники и автоматизированных систем управления от несанкционированного доступа и криптографической защитой циркулирующей в них информации.

Инженерно-техническая защита информации обеспечивает защиту информации с помощью инженерных конструкций и технических средств.

Мы будем рассматривать информацию как предмет защиты. Защите подлежит **секретная** и **конфиденциальная** информация [3].

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

РФ в целом. Федеральный закон Российской Федерации от 21.07.93 № 5486–1 дает следующее определение: **государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Под **конфиденциальной** информацией понимается информация, содержащую коммерческую и иную тайну. В **Словаре терминов и определений по безопасности информации** дается следующее определение: **конфиденциальная информация** – служебная, профессиональная, промышленная, коммерческая или иная информация, правовой режим которой устанавливается ее собственником на основе законов о коммерческой, профессиональной тайне, государственной службе и других законодательных актов. Понятие коммерческой тайны предприятия определено в Федеральном законе Российской Федерации о коммерческой тайне. «Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду». К информации, составляющей коммерческую тайну относиться научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

**Особенности информации как объекта защиты:**

- она нематериальная в том смысле, что нельзя измерить ее параметры, например, массу, размеры, энергию, известными физическими методами и приборами;
- информация, записанная на материальный носитель, может храниться, обрабатываться, передаваться по различным каналам связи;
- любой материальный объект содержит информацию о самом себе или о другом объекте.

Как указывает Торокин в книге «Инженерно-техническая защита информации», без информации не может существовать жизнь в любой форме и не могут функционировать созданные человеком любые информационные системы. Без нее биологические и искусственные системы представляют груду химических элементов. Опыты по изоляции органов чувств человека, затрудняющие информационный обмен человека с окружающей средой, показали, что информационный голод (дефицит информации) по своим последствиям не менее разрушителен, чем голод физический.

Несмотря на определенные достижения прикладной области науки – информатики, занимающейся информационными процессами, достаточно четкого понимания сущности информации наука пока не имеет.

## 1.1. Виды защищаемой информации

По содержанию любая информация может быть отнесена к семантической (символьной) или к информации о признаках материального объекта – признаковой. Сущность семантической информации не зависит от характеристик носителя. Содержание текста, например, не зависит от качества бумаги, на которой он написан, или физических параметров другого носителя. **Семантическая информация – продукт абстрактного мышления человека и отображает объекты, явления, как материального мира, так и создаваемые им образы и модели с помощью символов на языках общения людей.** Языки общения включают как естественные языки национального общения, так и искусственные профессиональные языки. Языки национального общения формируются в течение длительного времени развития нации. В нем устаревшие слова постепенно отмирают, но появляются новые, вызванные развитием человечества, в том числе техническим прогрессом.

**Семантическая** информация на языке национального общения представляется в виде упорядоченной последовательности знаков (букв, цифр, иероглифов) алфавита этого языка и записывается на любом материальном носителе. В области средств регистрации и консервации семантической информации изыскиваются носители, обеспечивающие все более высокую плотность записи и меньшее энергопотребление. Профессиональные языки создаются специалистами для экономного и компактного отображения информации. Существует множество профессиональных языков: математики, музыки, радиоэлектроники, автодорожного движения, химии и т. д. Любая предметная область содержит характерные для нее понятия и условные обозначения, часто непонятные необученному этому языку человеку. Для однозначного понимания этого языка всеми специалистами областей науки, техники, искусства и др., термины и условные обозначения стандартизируются. В принципе все то, что описано на профессиональном языке, можно представить на языке общечеловеческого общения, но такая форма записи громоздка и неудобна для восприятия информации человеком.

Информация **признаковая** описывает конкретный материальный объект на языке его признаков. Описание объекта содержит признаки его внешнего вида, излучаемых им полей и элементарных частиц, состава и структуры веществ, из которых состоит объект. Источниками признаковой информации являются сами объекты. К ним в первую очередь относятся интересующие зарубежную разведку или отечественного конкурента люди, новая продукция и материалы, помещения и даже здания, в которых может находиться конфиденциальная информация. 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.

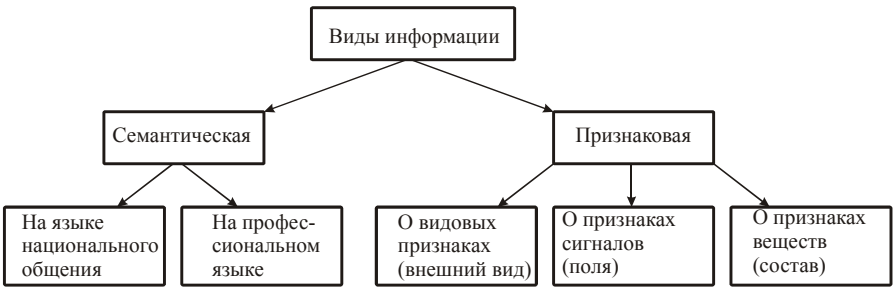



Рис. 1.1. Классификация информации, защищаемой техническими средствами

Защищаемая информация неоднородна по содержанию, объему и ценности. Следовательно, защита будет рациональной в том случае, когда уровень защиты, а следовательно, затраты, соответствуют количеству и качеству ин формации. Если затраты на защиту информации выше ее цены, то уровень защиты неоправданно велик, если существенно меньше, то повышается вероятность уничтожения, хищения или изменения информации. Для обеспечения рациональной защиты возникает необходимость структурирования конфиденциальной информации, т. е. разделения ее на так называемые 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.

Структурирование информации проводится путем последовательной детализации защищаемой информации, начиная с перечней сведений, содержащих тайну. Детализация предусматривает иерархическое разбиение информации в соответствии со структурой тематических вопросов, охватывающих все аспекты организации и деятельности частной фирмы или государственной структуры.

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

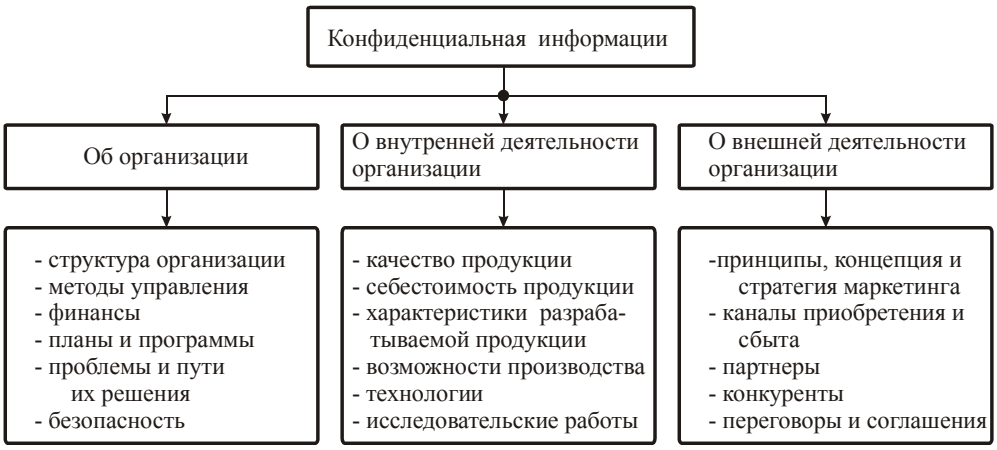



Рис. 1.2. Вариант структуры конфиденциальной информации

Обобщенный перечень сведений, составляющих коммерческую тайну (на рис. 1.2. конфиденциальная информация), относится к нулевому (исходному) уровню иерархии структуры. На 1-м уровне эта информация разделяется на 3 группы, каждая из которых соответствует темам: «об организации», «о внутренней деятельности организации», «о внешней деятельности организации». На 2-м уровне эти темы конкретизируются тематическими вопросами: структура, методы управления, качество продукции, себестоимость продукции, принципы, концепция и стратегия маркетинга и т. д. На 3-м уровне детализируются тематические вопросы 2-го уровня и т. д. Такая информация является **структурированной**.

Зашита структурированной информации принципиально отличается от защиты информации вообще. Она конкретна, так как ясно, что (какой информационный элемент) необходимо защищать, прежде всего, исходя из его ценности, кто или что являются источниками и носителями этого элемента. Для элемента информации можно выявить возможные угрозы его безопасности и определить, наконец, какие способы и средства целесообразно применять для обеспечения безопасности рассматриваемого элемента информации.

## 1.2. Свойства информации как предмета защиты

Для обеспечения эффективной защиты информации необходимо знать ее свойства. Она как предмет защиты обладает рядом свойств, основные из которых следующие:

**1.** Нематериальная информация может храниться, передаваться, обрабатываться, если она содержится на материальном носителе. Так как с помощью материальных средств можно защищать только материальный объект, **то объектами защиты являются материальные носители информации.** Различают носители — источники информации, носители — переносчики информации и носители — получатели информации. Например, чертеж является источником информации, а бумага, на которой он нарисован, — носитель информации. Физическая природа источника и носителя в этом примере одна и та же — бумага. Однако между ними существует разница. Бумага без нанесенного на ней текста или рисунка является источником информации о ее физических и химических свойствах. Когда бумага содержит семантическую информацию, то она становится документом — источником семантической информации.

Но независимо от вида информации, содержащейся на бумаге или ином другом носителе, защищать от хищения, изменения и уничтожения информации можно материальный объект — листы бумаги, которые имеют определенные размеры, вес, механическую прочность, устойчивость краски или чернил к внешним воздействиям и т. д., или иные носители. Параметры носителя определяют условия и способы хранения информации. Бумагу для обеспечения безопасности содержащейся на ней информации хранят в сейфе. Другие носители, например, поля, не имеют четких границ в пространстве и

их трудно запереть в шкаф. Но в любом случае характеристики материального носителя контролируемы органами чувств человека или его технических средств.

**2. Информация может быть для ее для пользователя (собственника, владельца, получателя) достоверной и ложной, полезной и вредной.** Информация, отражающие объективные факты, события, явления и процессы, является **достоверной,** а не соответствующая им — **ложной.** Границу между достоверной и ложной информацией часто трудно провести. Достоверная информация в процессе передачи может трансформироваться в свою противоположность. Преднамеренно создаваемая и распространяемая ложная информация называется **дезинформацией.**

В естественных областях науки достоверной информацией считается та, которую может получить не только ее автор, но и другие ученые. Если результаты научного исследования не удается повторить, то информация считается недостоверной. Например, сенсационное сообщение английских физиков о получении ими «холодной» (при обычной температуре) термоядерной реакции сначала вызвало большой интерес в мире, но после неудачных попыток повторить эксперимент другими учеными, это сообщение было забыто.

**Полезная** информация приносит прибыль ее владельцу или пользователю, уменьшает риск в его деятельности в результате принятия более обоснованных решений, улучшает его психическое состояние и т. д. Достоверная информация, как правило, является полезной, так как обеспечивает принятие более правильного решения. Но в отдельных случаях такая зависимость подвергается сомнению. Например, американские врачи сообщают больному о его неизлечимой болезни, так как считают, что такая информация позволяет больному принять более обоснованное решение о своих дальнейших действиях. Наши врачи часто скрывают правду, полагая, что такая информация может «добить» больного. Истина, как считают в таких случаях, посредине. Сильному человеку горькая правда полезна, так как она мобилизует его силы для борьбы с недугом, слабому более полезна «сладкая ложь», так как она поддерживает его жизненный тонус.

**Вредной** является информация, в результате использования которой ее получателю наносится моральный или материальный ущерб. Часто вредная информация создается в результате целенаправленной или случайной модификации ее при переносе с одного носителя на другой. Такая информация распространяется в виде слухов. Из этого не следует, что слухи содержат только ложную и вредную информации. Иногда власти допускают утечку достоверной информации с целью выявить реакцию общественности на готовящиеся непопулярные меры, а «звезды», особенно шоу-бизнеса, распускают слухи о себе для поддержания имиджа.

К вредной также относится информация, содержание которой является нейтральной для ее пользователя, но засоряет так называемое информационное пространство. Засоренность каналов связи и документов нейтральной информацией затрудняет и существенно увеличивает время добывания полезной. Многие по собственному опыту знают, как иногда трудно найти нужный

документ в кипах других, от которых и пользы-то мало, но выбросить жалко. Кроме того, носитель с нейтральной для конкретного получателя информацией может оказывать вредное воздействие на другой носитель с полезной информацией, если близки по значениям параметры носителей, например частоты колебаний электромагнитных полей разных источников. Носители информации, оказывающее воздействие на другой носитель, представляют собой **помехи.** То, что для одного получателя является информацией, для другого – помеха. Когда во время разговора по телефону из-за неисправности в цепях коммутации телефонной станции слышен разговор других людей, то каждая пара абонентов воспринимает разговор другой как помеху.

Полезность информации всегда **конкретна.** Нет полезной информации вообще. Информация полезна или вредна для конкретного ее пользователя. Под пользователями подразумевается как один человек или автомат, так и группа людей и даже все человечество. Чрезвычайно полезная информация для одних пользователей может не представлять ценности для других. Даже информация, ценная для всего человечества, например технология изготовления лекарств от опасной болезни, для конкретного здорового человека может не представлять интерес.

Поэтому при защите информации определяют, прежде всего, круг лиц (фирм, государств), заинтересованных в защищаемой информации, так как вероятно, что среди них окажутся злоумышленники.

В интересах защиты ценной (полезной) информации ее владелец (государство, организация, физическое лицо) наносит на носитель условный знак полезности содержащейся на нем информации, – **гриф секретности или конфиденциальности**. Гриф секретности информации, владельцами которой является государство (государственные органы), устанавливается на основании Закона «О государственной тайне» и ведомственных перечней сведений, составляющих государственную тайну. В соответствии с постановлением Правительства РФ № 870 от 4 сентября 1995 г. к информации **секретной, совершенно секретной и особой важности** относится информация, хищение или несанкционированное распространение которой может нанести ущерб соответственно государственной организации (предприятию, учреждению), отрасли (ведомству, министерству), субъекту Федерации и РФ в целом. Для несекретной информации, содержащей служебную тайну, вводят гриф «для служебного пользования».

Для обозначения степени конфиденциальности коммерческой информации применяют различные шкалы ранжирования. Наиболее распространена шкала: «**строго конфиденциально», конфиденциально» и «не подлежит разглашению**».

В качестве критерия для определения грифа конфиденциальности информации могут служить результаты прогноза последствий попадания информации к конкуренту или злоумышленнику.

Следствием разглашения или утери документа с грифом «строго конфиденциально» могут быть материальные и финансовые потери, которые могут привести организацию к банкротству или поглощению ее более мощной, а

также к физическому и морально-психологическому воздействию на персонал организации. При попадании к конкуренту информации документов с грифом «конфиденциально» организации могут быть нанесены значительные материальные и финансовые потери. «Разглашению не подлежит» информация, представляемая в органы контроля, переписка, договоры, сведения о сотрудниках организации, воспользовавшись которыми злоумышленник может нанести им или организации вред.

**3.** Хотя информация нематериальная, она покупается и продается. Поэтому **информацию можно рассматривать как товар.** Полезность информации как товара характеризуется его ценой. Цена информации зависит от ее ценности, но это разные понятия. Например, при проведении исследований могут быть затрачены большие материальные и финансовые ресурсы, которые завершились отрицательным результатом, т. е. не получена информация, на основе которой ее владелец может получить прибыль. Но отрицательные результаты представляют ценность для специалистов, занимающихся рассматриваемой проблемой, так как полученная информация укорачивает путь к истине. Детские фотографии имеют большую ценность для родителей изображенных на них детей, но рыночная цена у них близка к нулю до тех пор, пока изображенный на фотографии ребенок не становится знаменитым. Цена фотографии знаменитого человека пропорциональна его рейтингу. **Ценность информации — полезность ее для собственника (владельца, пользователя), цена — полезность информации для участников рынка.**

Цена информации, как любого товара, складывается из себестоимости и прибыли. Себестоимость определяется расходами владельца информации на ее получение путем:

- проведения исследований в научных лабораториях, аналитических центрах, группах, отдельными учеными и т. д.;
- покупки информации на рынке информации;
- добывания информации противоправными действиями.

Прибыль от информации ввиду ее особенностей может принимать различные формы, причем денежное ее выражение не является самой распространенной формой. В общем случае прибыль от информации может быть получена в результате следующих действий:

- продажи информации на рынке;
- материализации информации в продукции с новыми свойствами или технологией, приносящими дополнительную прибыль;
- использования информации для принятия более эффективных решений.

Последняя форма прибыли от информации не столь очевидна, но она самая распространенная. Это обусловлено тем, что любая деятельность человека есть по своей сути последовательность принятия им решений. Большинство решений принимается человеком бессознательно, он осознанно принимает в основном жизненно важные решения.

4. **Полезность (цена) информации изменяется во времени.** Распространение информации и ее использование приводят к изменению ее ценности и цены. Характер изменения ценности во времени зависит от вида инфор-

мации. Для научной информации эта зависимость часто имеет волнообразный вид. Информация об открытии даже новых законов или явлений природы вначале должным образом не оценивается. Например, в начале века результаты исследований по атомной физике носили чисто познавательный характер и интересовали узкий круг ученых. Информация в этой области приобрела чрезвычайно высокую цену, когда появились реальные возможности практического использования атомной энергии. По мере того как исчерпываются на определенном этапе научно-технического прогресса возможности практической реализации теоретических результатов, ценность информации убывает. Новые технологии или достижения в смежных областях могут увеличить ценность давно полученных знаний. Недаром говорят, что новое — это хорошо забытое старое.

Ценность (цена) большинства видов информации, циркулирующей в обществе, со временем уменьшается — информация стареет. Характер старения разведывательной информации приведен на рис. 1.3.

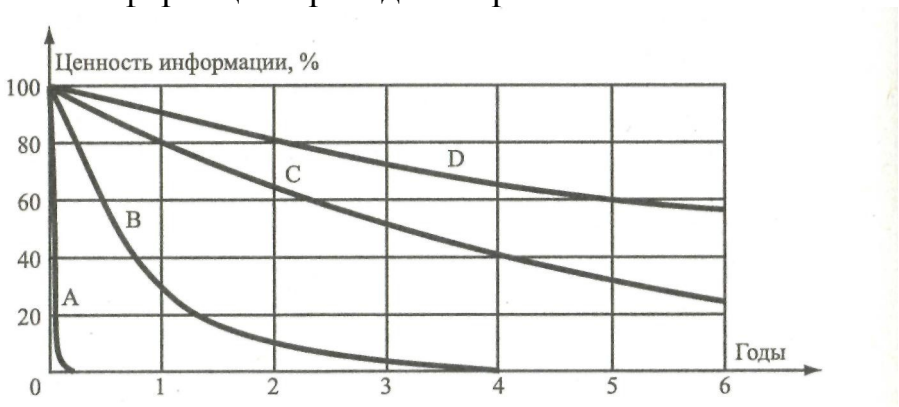



Рис. 1.3. Характер старения разведывательной информации

A — оперативно-тактическая информация (ценность теряется 10% в день);

B — стратегическая информация во время войны (ценность теряется 10% в месяц);

C — стратегическая информация в мирное время (ценность теряется 20% в год);

D — информация о сравнительно неизменных объектах (дорогах, мостах, природных ресурсах, ценность теряется 10% в год).

По степени старения коммерческая информация может характеризоваться следующим образом:

- оперативно-тактическая, теряющая ценность примерно по 10% в день (например, информация о выдаче 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.).

Ценность информация о законах природы убывает очень медленно. Ее старение проявляется в уточнении законов, например, в ограничениях законов Ньютона для микромира.

Характер старения информации можно аппроксимировать зависимостью, аналогичной правилу получения «сложного» процента. В соответствии с ней ценность информации через **m** интервалов времени, убывающая на **к** процентов за один интервал, оценивается по выражению:

$$С_и = С_{ио} (1 – к/ 100)^m,$$

где $С_{ио}$ — ценность информации в момент ее получения. Например, если ценность информации уменьшается в месяц на 10%, то через 6 месяцев она составит около 50% первоначальной ценности. Время, в течение которого ценность информации уменьшается до 10% первоначальной величины, можно назвать **временем жизни информации** $\tau_{жи}$. Время жизни рассматриваемой в примере информации составляет около 21 месяца.

5. **Невозможно объективно (без учета полезности ее для потребителя, владельца, собственника) оценить количество информации.** Для обеспечения эффективной защиты информации важно знать количество защищаемой информации. Однако объективно определить ее невозможно. Например, количество информации, содержащейся в книге, для разных читателей — разное. Даже один и тот же человек в разные периоды своей жизни находит в книге каждый раз что-то новое для себя. Количество информации в голове человека можно косвенно оценить по его действиям, так как для принятия обоснованного решения необходимо больше информации.

Иногда полезность информации связывают с ее качеством. Но понятие «качество» применительно к информации не имеет самостоятельного значения, так как оно поглощается понятием «количество». Действительно, количество информации, например, в фотографии зависит от ее качества. Чем более резкое изображение на фотографии, чем больше в нем полутонов и оттенков цвета, тем больше информации она содержит. Ухудшение качества изображения при копировании, например, видеокассет приводит к снижению количества информации и, как следствие, к уменьшению психологического воздействия фильма на зрителя. Под качеством информации обычно подразумевают качество отображения ее на носителе или ее достоверность (соответствие оригиналу). Качество информации в этом смысле можно достаточно объективно измерить.

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.

Знания отдельного человека, организации, государства образуют соответствующие тезаурусы. Тезаурусы различных организационных структур включают части тезаурусов входящих в их состав элементов, прежде всего людей. Например, тезаурус организации образуется из тезаурусов сотрудников по тематике их работы и других носителей информации (документов, продукции, материалов и т. д.).

Для передачи знаний тезаурусы должны пересекаться, т. е. они должны содержать общие элементы (понятия и отношения между ними). Если таковых нет, то владельцы разных тезаурусов просто не поймут друг друга. О таких людях говорят, что они разговаривают на «разных языках». Даже люди одной национальности часто говорят на «разных языках», вкладывая в одинаковые по форме понятия разное содержание. Подход к оценке количества информации по степени изменения тезауруса после ее получения, предложенный Ю. А. Шрейдером, можно назвать **тезаурусным.**

В общем случае количество информации, получаемое из сообщения ее получателем, зависит от соотношения тезауруса сообщения и получателя. Если тезаурус сообщения составляет часть тезауруса получателя или их тезаурусы настолько отличаются по составу, что не пересекаются, то количество получаемой информации минимальное. В первом варианте получатель не приобретает новые знания, и тезаурус получателя не пополняется, во втором — получатель не понимает смысл сообщения и не может установить отношения с другими элементами тезауруса.

Обобщая сказанное, циркуляцию информации в человеческом обществе можно представить исходя из следующей модели.

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 как за счет синтеза знаний владельцем путем проведения собственных исследований или разработок, так и за счет их законного и незаконного приобретения.

Законное приобретение знаний возможно путем организованного обучения в учебных заведениях, самостоятельного изучения литературы (самообучения), приглашения на работу более знающего специалиста, покупки патента или лицензии. Приобретение знаний путем хищения информации является незаконным способом увеличения тезауруса.

Приближенно относительное количество информации можно оценить путем определения доли тематических вопросов, на которые получены ответы, удовлетворяющие потребителя или получателя информации. С этой целью вся предметная область, которая интересует получателя информации, разделяется на **n** тематических вопросов, из которых на **m** получены ответы с достаточной полнотой и достоверностью, а отношение n/m характеризует в долях или процентах количество информации. Чем большее количество тематических вопросов, тем точнее оценки.

Применительно к видам информации количества информации приближенно можно оценить на основе следующих соображений.

В качестве единицы семантической информации по аналогии с признаковой информацией целесообразно выбрать то, что пытаются выделить в любом документе, — **мысль.** Она может быть выражена одним словом или большим количеством предложений. Но семантическая информация нужна человеку для передачи прежде всего мыслей. Цена информации также зависит от полезности и количества содержащихся в них мыслей. Формальным

путем выявить мысль пока нельзя. Однако человек может в любом сообщении определить, по крайней мере, основные из содержащихся в нем мыслей. Мысли реферата, доклада, курсовой работы, дипломного проекта и других документов концентрируют в заключении. Конечно, сами мысли могут существенно отличаться по ценности или полезности. За одни мысли ее автор получает Нобелевскую премию, другие мысли не интересны даже близкому человеку. Если ценность мысли оценить коэффициентом в интервале 0-1, то количество семантической информации в сообщении определяется как взвешенная (по ценности) сумма содержащихся в нем мыслей.

Такой подход хорошо согласуется с широко применяемой оценкой информации в выступлениях, статьях, отчетах и других информационных материалах. Например, в выступлении такого-то докладчика много полезных мыслей, в статье такого-то автора не содержится ни одной стоящей мысли. Полезность публикации соответственно содержащихся в ней мыслей определяется по количеству ссылок на нее в работах других авторов. Чем более кратко и четко излагает человек свои мысли, тем больше он ценится как специалист.

На практике используют более грубый и простой, так называемый **объемный способ измерения информации** путем подсчета количества (в битах или байтах) символов сообщения или измерения характеристик носителя (количества листов, времени передачи сообщения и др.). Часто покупатели книг оценивают их полезность по количеству листов. Интуитивно кажется, что большее число листов содержит большее количество информации. Но такая зависимость верна далеко не всегда. Сравнительно небольшой по объему рассказ Э. Хемингуэя «Старик и море» превосходит по эмоциональному воздействию многие толстые романы.

6. **Информация способна случайным образом «растекаться» в пространстве.** Так как человеку присуща любознательность, переходящая у многих в любопытство, а также иногда даже трудно сдерживаемое желание поделиться с другими новостями, то при общении (взаимодействии) людей происходит выравнивание их тезаурусов. Следовательно, в организации и обществе, если не предпринимаются дополнительные усилия по поддержанию неравномерности информационной энтропии, происходит ее выравнивание, т. е. выравнивание тезаурусов разных сотрудников или членов общества. Выравнивание тезаурусов происходит путем передачи информации от тезауруса большего объема тезаурусу меньшего объема. Кроме целенаправленной (законной или незаконной) деятельности по передаче информации имеют место случайные процессы выравнивания тезаурусов владельцев, аналогично выравниванию температуры в замкнутом пространстве. Этот процесс объективно проявляется в любой организации, государстве и человеческом обществе в целом путем случайных, трудно контролируемых процессов распространения информации от источника с большим объемом тезауруса к получателю, в том числе несанкционированному, с меньшим объемом тезауруса. Как показывает опыт, со временем круг лиц, которым становится известна секретная (конфиденциальная) информация, расширяется случайным образом. Кто-то под большим секретом рассказал новости приятелю или жене, те приоткрыли

тайну другим людям и т. д. Это процесс объективный в том смысле, что только за счет дополнительных усилий и часто больших затрат удается приостановить или замедлить процесс «растекания» информации. По своей сути он аналогичен, только в информационной сфере, процессу выравнивания энтропии в природе. Например, при уменьшении энтропии в какой-либо точке пространства, вызванном нагреванием или даже рождением человека, со временем температура выравнивается, а человек умирает и превращается в прах, энтропия которого неизмеримо выше, чем у живого человека.

При выравнивании тезаурусов коммерческая цена информации убывает, а ценность информации может как возрастать, так и снижаться. Действительно, закон Ома знают очень много людей, но от этого полезность его для практики не уменьшается. Но покупателя на эту информацию вряд ли удастся найти, так как изучение закона Ома входит в программу школьного образования.

7. **При копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а ее цена снижается.** После снятия копии с документа на ксероксе или другим способом количество информации в нем не меняется. В результате этого несанкционированное копирование (хищение) информации может остаться незамеченным для ее владельца, если отсутствуют иные признаки проникновения злоумышленника к ее источнику и факта хищения. Но если при копировании происходят воздействия на информационные параметры носителя, приводящие к изменению их значений, или незначительные изменения накапливаются, то количество информации уменьшается. Ухудшается качество звука и изображения соответственно на аудио- и видеопленке из-за механического разрушения магнитного слоя, книжка зачитывается до дыр, блекнут яркие цвета на картинках-репродукциях на стенах светлой комнаты.

Так как при каждом копировании увеличивается число ее законных и незаконных пользователей, то в соответствии с законами рынка цена снижается. Например, видеопиратство вызывает большое беспокойство у владельцев видеопродукции, так как широкое распространение пиратских копий значительно сбивает цены на рынке.

## 1.3. Источники и носители информации, защищаемой техническими средствами

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 [3]:

- 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 в объеме, превышающем, как правило, необходимый для выполнения его функциональных обязанностей. Распространение конфиденциальной информации между сотрудниками организации является одним из проявлений процессов выравнивания тезаурусов. Например, в результате неформальных межличностных отношений (дружественных, приятельских) конфиденциальная информация может поступать к посторонним лицам, которые к сохранению «чужих» тайн относятся менее ответственно, чем к своим. Тщеславные люди непреднамеренно разглашают конфиденциальные сведения в публичных выступлениях и беседах с целью продемонстрировать свою эрудицию или заинтересовать собеседника и т. д. 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.

Поэтому служба безопасности в интересах локализации ценной информации должна постоянно помнить о достаточно объективных процессах распространения информации внутри 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 относится 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, так как они содержат, как правило, достоверную информацию в отработанном и сжатом виде, в особенности, если документы подписаны или утверждены. Информативность различных публикаций имеет широкий диапазон оценок: от очень высокой, когда описывается открытие, до преднамеренной или непреднамеренной дезинформации. К последней, например, относятся публикации с недостаточно проверенными и достоверными результатами.

**Датчики.** 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. Критерием отнесения технического средства к источни-

кам информации может служить ответ на вопрос потребителя информации об ее источнике. Легко можно представить реакцию потребителя информации на ответ, что ее источник - телефонный аппарат в таком-то помещении или компьютер. Также некорректно рассматривать в качестве источников информации радио- или телевизионные приемники. Очевидно, что источники этой информации даже не дикторы, читающие текст, а редакции и конкретные люди, готовящие текст или высказывающие свое мнение.

**Продукция** (без документации) 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 лекарства). Для получения семантической информации о сущности ноу-хау с целью его использования производят изучение и исследование продукции путем разборки, расчленения, выделения отдельных составных частей и элементов, проведения физического и химического анализа и т. д.

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. Даже при печатании на пишущей машинке остаются следы документов на копировальной бумаге и ленте, которые после использования машинистка бросает в корзину для бумаг. Отходы производства в случае небрежного отношения с ними (сбрасывания на свалку без предварительной селекции, сжигания или резки бумаги и т. д.) могут привести к утечке ценной информации. Для такой возможности существуют, кроме того, психологические предпосылки сотрудников, серьезно не воспринимающих 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.

Таким образом, источниками конфиденциальной информации могут быть как физические лица, так и различные объекты. Как правило, для добывания информации между источником и получателем существует посредник - носитель информации, который позволяет органу разведки или злоумышленнику получать информацию дистанционно, в более безопасных условиях. Информация источника также содержится на носителе. **Следовательно, носителями являются материальные объекты, обеспечивающие запись, хранение и передачу информации в пространстве и времени.** Известны 4 вида носителей информации:

- люди;
- материальные тела (макрочастицы);
- поля

- 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, исказив 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 бумаги восстанавливают подчищенные надписи, по изменению структуры металла двигателя определяют его заводской номер, перебитый автомобильными ворами. Материальные тела (папирус, 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**. 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 гелия) радиоактивных излучений. Попытки использования для переноса информации других элементарных частиц с лучшей проникающей способностью (меньшим затуханием в среде распространения), например, нейтрино, не привели пока к положительным результатам.

## 1.4. Запись и съем информации с ее носителя

В редких случаях информация от источника непосредственно передается получателю, т. е. источник сам переносит ее в пространстве к месту расположения получателя или получатель вступает в непосредственный контакт с источником, например, проникает в помещение, вскрывает сейф и забирает документ. В большинстве случаев она переносится от источника к получателю промежуточным носителем.

Материализация (запись) любой информации производится путем изменения параметров носителя. **Механизм запоминания и воспроизведения** информации человеком в настоящее время еще недостаточно изучен и нет од-

нозначного и ясного представления о носителях информации в мозгу человека. Рассматривается химическая и электрическая природа механизмов запоминания.

Запись информации на материальные тела производится путем изменения их физической структуры и химического состава. На бумаге информация записывается путем окрашивания элементов ее поверхности типографской краской, чернилами, пастой и другими красителями.

Записанная на материальном теле информация считывается при просмотре поверхности тела зрительным анализатором человека или автомата, обнаружении и распознавании ими знаков, символов или конфигурации точек. Для людей, лишенных зрения, информация записывается по методу Брайля путем изменения физической структуры бумаги выдавливанием соответствующих знаков (букв и цифр). Информация считывается не зрительным анализатором, а тактильными рецепторами пальцев слепых людей.

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. Модулируемое колебание называется **несущим.** Если меняются значения амплитуды аналогового сигнала, то модуляция называется амплитудная (АМ), частоты — частотная (ЧМ), фазы — фазовая (ФМ). Максимальное изменение информационного параметра несущей относительно его номинального значения называется **глубиной модуляции,** а максимальное отклонение значения информационного параметра несущей относительно максимального изменения информационного параметра модулирующего сигнала — **индексом модуляции.**

При модуляции дискретных сигналов в качестве признаков применяются также длительность импульса, частота его повторения и др. С целью уплотнения информации на носителе и экономии тем самым энергии носителя применяют сложные (с одновременным использованием различных параметров сигнала) виды модуляции. Например, для радиовещания в УКВ-диапазоне (58-73, 87,5-108 МГц) используется частотная модуляция с максимальным изменением (девиацией) частоты 50 кГц. При максимальной частоте модулирующего сигнала 15 кГц индекс частотной модуляции составляет $m_{чм} = 3,3$, а глубина модуляции на частоте 100 МГц — 0,0005.

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

- для АМ: $\Delta F_{ам} = 2F_{мод}$;
- для ЧМ: $\Delta F_{чм} = 2F_{мод} (m_{чм}+1)$;

Ширина спектра широко применяемых модулированных сигналов составляет:

- АМ-узкополосных сигналов, используемых в радиовещании на длинных, средних и коротких волнах, — 5…15 кГц;
- используемых для радиосвязи ЧМ - узкополосных (NFM) — 5…15 кГц;
- ЧМ - широкополосных (WFM) в УКВ радиовещании и при передаче звука в телевидении — 150…250 кГц.

Ширина спектра ЧМ - сигнала составляет 50…250 кГц вместо 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. Так как действие помех проявляется, прежде всего, в изменении амплитуды сигнала, то ЧМ - сигналы обладают существенно большей помехоустойчивостью, чем АМ - сигналы. Это свойство ЧМ - сигналов обеспечивает высокое качество радиовещания в УКВ-диапазоне.

Выделение информации из модулированного электрического сигнала производится путем обратных преобразований — демодуляции его в детекторе (демодуляторе) приемника. При демодуляции выделенный и усиленный сигнал, наведенный электромагнитной волной в антенне, преобразуется таким образом, что сигнал на выходе детектора соответствует модулирующему сигналу передатчика. Демодуляция, как любая процедура распознавания, обеспечивается путем идентификации текущей признаковой структуры сигнала с эталонной структурой, заданной априори или полученной в процессе его приема. Эталонная признаковая структура при ЧМ - модуляции определяется частотой настройки контура детектора. При демодуляции АМ - сигналов в качестве эталонной амплитуды используется усредненная амплитуда несущего колебания на выходе детектора, относительно которой сравнивается текущее значение амплитуды принимаемого сигнала.

# 2. ДЕМАСКИРУЮЩИЕ ПРИЗНАКИ ОБЪЕКТОВ ЗАЩИТЫ

Задача защиты признаковой информации решается, прежде всего, путем предотвращения обнаружения и распознавания признаков объектов, по которым можно обнаружить и распознать объекты, т. е. найти эти объекты среди других объектов, определить их назначение, задачи, функции и характеристики. Признак объекта, позволяющий обнаруживать и распознавать объект, которому принадлежит признак, среди других объектов, называется **демаскирующим.**

## 2.1. Классификация демаскирующих признаков объектов защиты

Классификация демаскирующих признаков по различным основаниям дана на рис. 2.1 [2].

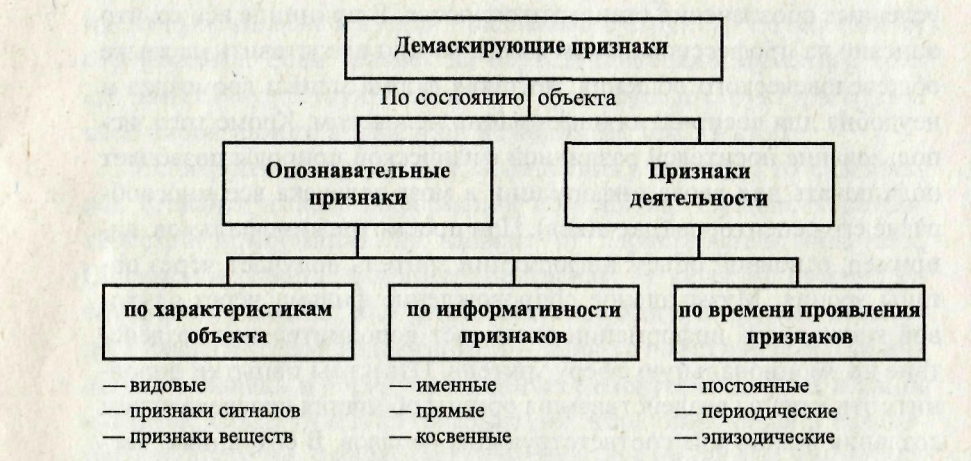



Рис. 2.1. Классификация демаскирующих признаков

В зависимости от состояния объекта его демаскирующие признаки разделяются на **опознавательные признаки** и **признаки деятельности.**

**Опознавательные признаки** описывают объекты в статическом состоянии: его внешний вид, излучения, физические и химические свойства и др. **Признаки деятельности** объектов характеризуют этапы и режимы функционирования объектов. Например, этапы создания новой продукции включают: научные исследования, подготовку к производству, изготовление новой продукции, ее испытания и т. д. Признаки деятельности представляют собой последовательность во времени событий или действий составных элементов рассматриваемого объекта и взаимодействующих с ним объектов, а также значения статистических характеристик событий и действий. Например, по активности посещения студентами библиотек и их количеству в читальном зале можно спрогнозировать время сдачи курсового проекта, зачета или экзамена. По активности работы средств радиосвязи войсковой части можно определить вид их деятельности: повседневная деятельность в местах постоянной дислокации, подготовка к передислокации, перемещение, развертывание в месте новой дислокации.

Демаскирующие признаки объекта можно разделить на три группы:

- видовые признаки;
- признаки сигналов;
- признаки веществ.

К **видовым признакам** относятся форма объекта, его размеры, детали объекта, тон, цвет и структура его поверхности и др.

**Признаки сигналов** описывают параметры полей и электрических сигналов, генерируемых объектом: их мощность, частоту, вид (аналоговый, импульсный), ширину спектра и т. д.

**Признаки веществ** определяют физический и химический состав, структуру и свойства веществ материального объекта.

Таким образом, совокупность демаскирующих признаков рассмотренных трех групп представляет собой модель объекта, описывающую его внешний вид, излучаемые им поля, внутреннюю структуру и химический состав содержащихся в нем веществ.

Важнейшим показателем признака является его **информативность.** Информативность признака оценивается мерой в интервале [0…1], характеризующей его индивидуальность. Чем признак более индивидуален, т. е. принадлежит меньшему числу объектов, тем он более информативен. Величину информативности можно определить как $I_k = (N-N_k)/N$, где $N_k$ — количество объектов, содержащих признак k, из N рассматриваемых. Если признак принадлежит одному объекту, то информативность максимальная и приближается к 1; если признак принадлежит всем объектам выборки, то информативность нулевая. Информативность конкретного k-го признака можно характеризовать вероятностью $P_к$ обнаружения конкретного объекта по этому признаку среди других рассматриваемых объектов.

Наиболее информативен **именной** признак, присущий одному конкретному объекту. Такими признаками являются фамилия, имя, отчество человека, папиллярный рисунок его пальцев, инвентарный номер прибора или образца мебели. Факты, например, о совпадении папиллярных узоров пальцев хотя бы двух разных людей не известны.

Информативность остальных демаскирующих признаков, принадлежащих рассматриваемому объекту и называемых **прямыми,** колеблется в пределах [0…1]. Признаки, непосредственно не принадлежащие объекту, но отражающие его свойства и состояние, называются **косвенными.** Эти признаки являются, как правило, результатом взаимодействия рассматриваемого объекта с окружающей средой. К ним относятся, например, следы ног или рук человека, автомобиля и других движущихся объектов. Следы краски или характер деформации поверхности автомобиля в результате автодорожного происшествия позволяют находить автомобиль, скрывшийся с места происшествия. Информативность косвенных признаков в общем случае ниже информативности прямых. Однако если в результате взаимодействия объектов на одном из них появляются именные признаки другого объекта, то информативность косвенного признака может приближаться к 1, например, четкие отпечатки пальцев на предметах, следы обуви, протектора шин машины и др.

По времени проявления признаки могут быть:

- постоянными, не изменяющимися или медленно меняющимися в течение жизненного цикла объекта;
- периодическими, например следы на снегу;
- эпизодическими, проявляющимися при определенных условиях, например, случайно появившееся на поверхности объекта пятно краски.

Структуры с наиболее достоверными априорными признаками объекта называются **эталонными,** а структуры с полученными в момент наблюдения и измерения признаками — **текущими.** Эталонные структуры периодически корректируются путем замены их недостаточно достоверных признаков более достоверными и информативными текущими признаками. Например, фотография, в паспорте как эталонная признаковая структура видовых признаков лица владельца, заменяется на новую при изменении информативных значений признаков в результате старения, отпускания бороды и усов, вживления волос на облысевшую часть головы, изменения черт лица после пластической операции.

## 2.2. Видовые демаскирующие признаки

Видовые демаскирующие признаки описывают внешний вид объекта. Они объективно ему присущи, но выявляются в результате анализа внешнего вида модели объекта – его изображения на экране оптического приемника (сетчатки глаза человека, фотоснимке, экрана 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 характеристики объектов (световые – освещенность, яркость и др.)
- геометрические характеристики объектов (форма, размеры объекта, цвет, освещенность, яркость, 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 периметру 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 объектов.

Тени объектов возникают в условиях прямого солнечного освещения и являются важными демаскирующими признаками объекта при наблюдении его сверху. Некоторые объекты (например, линии электропередачи, антенные мачты, ограждения и т. д.) часто распознают только по тени. Различают два вида тени: собственную, от элементов объектов, 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 и частот: в видимом, инфракрасном и радиодиапазоне.

Объекты по-разному отражают падающие на них лучи света. Например, коэффициент отражения листвы летом в ближнем инфракрасном диапазоне в 3-5 раз выше, чем в видимом, а у бетонных и асфальтовых покрытий отличаются незначительно.

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. Поверхность считается гладкой и отражение от нее зеркальное, если отношение среднеквадратичного значения высоты неровностей h к длине волны $\lambda$. 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, свежевыпавший снег. 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. Величина энергии, излучаемая любым телом с температурой Т, в соответствии с формулой Стефана — Больцмана пропорциональна величине $T^4$. В ближней (0,75-1,3 мкм) и средней (1,2-3,0 мкм) зонах ИК-излучения мощность теплового (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.

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, а к демаскирующим признакам добавляются признаки, характеризующие температуру поверхности объекта.

В общем случае к демаскирующим признакам объекта в ИК-диапазоне относятся:

- геометрические характеристики внешнего вида объекта (форма, размеры, детали поверхности);
- температура поверхности.

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 поверхностью (площадью) рассеяния (ЭПР).

**Эффективная площадь рассеяния –** способность объекта отражать электромагнитные волны. Физический смысл термина — площадь поверхности, расположенной перпендикулярно направлению сигнала облучающей РЛС, мощность отражённого сигнала от этой поверхности равна мощности сигнала отражённого от объекта. Величина имеет размерность площади и измеряется обычно в квадратных метрах.

Примеры для сравнения:

* Бомбардировщик B-52 имеет ЭПР равную 40 м².
* Обычный истребитель — 6 м².
* Бомбардировщик B-2B (построенный с использованием технологии стелс) — 0,75 м².
* Ударный самолёт F-117A (построенный с использованием технологии стелс) — 0,01÷0,025 м².
* Птица в полёте — 0,01 м².
* Человек — ~0,8 м².

К **основным видовым демаскирующим признакам объектов** радиолокационного наблюдения относятся:

- эффективная поверхность рассеяния;
- геометрические и яркостные характеристики (форма, размеры, яркость);
- 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.

Таким образом, 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.

Разрешение изображения цифрового фотоаппарата определяется разрешением его светоэлектрического преобразователя и в настоящее время составляет 20…30 млн. пикселей. Это гораздо меньше разрешающей способно-

сти лучших пленочных фотоаппаратов (200 млн. пикселей) или разрешающей способности до 500 лин./мм.

Следовательно, 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.

## 2.3. Демаскирующие признаки сигналов

По существу сигнал представляет распространяющийся в пространстве носитель с информацией, содержащейся в значениях его физических параметров. К сигналам относятся: **собственные** (обусловленные тепловым движением электронов, радиоактивные) излучения объектов, **отраженные** от объектов поля и волны, **и созданные** человеком электромагнитные поля и электрический ток от источников сигналов.

**Информационные параметры сигналов** представлены на рис. 2.2 [2].


Рис. 2.2. Классификация сигналов

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

Амплитуда простого и достаточно распространенного в природе гармонического сигнала изменяется по синусоидальному закону:

$U(t) = U_0 \sin(\omega t)$, $\omega = 2\pi f$ – круговая частота.

Частота f измеряется в Гц и называется линейной.

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

$$U(t) = U_0 + \sum_{k=1}^{N} U_k \cos(k\omega_1 t - \varphi_k)$$

где $U_0$ — постоянная составляющая сигнала; $U_к$ — амплитуда к-й гармоники сигнала (к = 1, 2, ..., N); $k\omega_1$, и $\varphi_k$ — частота и фаза к-й гармоники сигнала; $\omega_1 = 2\pi/T_п$ — частота 1-й гармоники.

Параметры ряда Фурье вычисляются по соответствующим формулам, например. Ряд Фурье представляет собой математическую модель периодического сигнала, так же как любой цвет может быть разложен на составляющие красного, зеленого и синего цветов. Совокупность гармонических (спектральных) составляющих сигнала образует 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. Разность между максимальной и минимальной частотами спектра сигнала, между которыми сосредоточена основная часть, например 95% энергии, называется **шириной спектра** $\Delta f$. Пример графического изображения спектра периодического сигнала представлен на рис. 2.3.

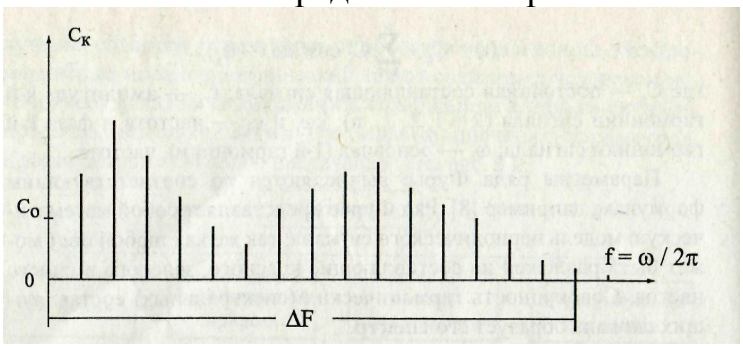



Рис. 2.3. Пример спектра периодического аналогового сигнала

Частоты составляющих спектра непериодического аналогового сигнала непрерывно меняются. При наблюдении спектра такого сигнала на экране анализатора спектра положение и уровень различных спектральных составляющих непрерывно изменяются и спектр выглядит как сплошной.

В соответствии с изменением амплитуды аналогового сигнала меняется его энергия или мощность, пропорциональная квадрату амплитуды. В зависимости от времени измерения энергии сигнала различают **среднюю** и **мгновенную мощность.** Десятичный логарифм отношения максимальной мгновенной мощности сигнала к минимальной называется **динамическим диапазоном сигнала.** Динамический диапазон речи диктора радио и телевидения составляет 25-30 дБ, вокального ансамбля — 45-65 дБ, а симфонического оркестра достигает 70-95 дБ.

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

- частота или диапазон частот;
- амплитуда или мощность сигнала;
- фаза сигнала;
- длительность сигнала;
- вид модуляции;
- ширина спектра сигнала;

- динамический диапазон сигнала.

У **дискретных сигналов** амплитуда имеет конечный, заранее определенный набор 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. 2.4.

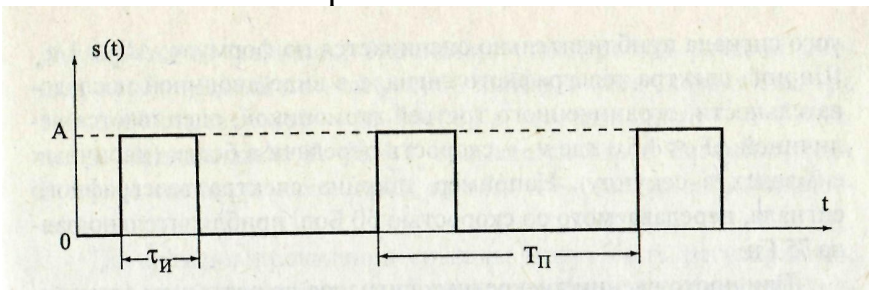



Рис. 2.4. Пример дискретного сигнала

Дискретный сигнал характеризуется следующими параметрами:

- амплитудой A или мощностью P,
- длительностью импульса $\tau_и$,
- периодом повторения $T_п$ или частотой $f_п = 1/T_п$ повторения импульсов (для периодических дискретных сигналов),
- шириной спектра сигнала $\Delta f$,
- скважностью импульсов $q = T_п/\tau_и$.

Спектр дискретного периодического сигнала содержит бесконечное количество убывающих по амплитуде гармоник. Вид спектра для бинарного периодического сигнала иллюстрируется рис. 2.5.

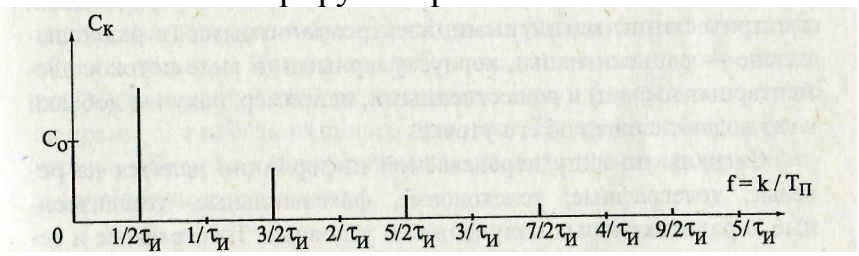



Рис. 2.5. Пример спектра дискретного периодического сигнала

Учитывая, что большая часть энергии сигнала сосредоточена в области частот 0-$1/\tau_и$, ширина спектра бинарного периодического сигнала приблизительно оценивается по формуле: $\Delta f = 1/\tau_и$.

**Различие сигналов по физической природе**. Сигналы могут быть

- акустическими,
- электрическими,
- магнитными,
- электромагнитными (в радиодиапазоне — радиосигналы),
- корпускулярными (в виде потоков элементарных частиц)
- вещественными, например, пахучие добавки в газ подают сигнал об его утечке.

**Различие сигналов по виду передаваемой информации.** Сигналы делятся на:

- речевые,
- телеграфные,
- телекодовые,
- факсимильные,
- телевизионные,
- о радиоактивных излучениях
- условные.

Телеграфные и телекодовые сигналы используются для передачи буквенно-цифровой информации с низкой и высокой скоростью соответственно. Факсимильные и телевизионные сигналы обеспечивают передачу неподвижных и подвижных изображений. Сигналы радиоактивных излучений являются демаскирующими признаками радиоактивных веществ. Условные сигналы несут информацию, содержание которой предварительно определено между ее источником и получателем, например горшок с цветком на подоконнике в литературных произведениях о разведчиках — о провале явки.

Вид информации, содержащейся в сигнале, изменяет его демаскирующие признаки: форму, ширину спектра, частотный и динамический диапазон. 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. Произведение спектра сигнала на его длительность: $B = \Delta f \cdot T_c$. называется **базой сигнала.** Если B < 1, то сигнал узкополосный, при B > 1 — сигнал широкополосный.

**Различие сигналов по времени проявления** сигналы могут быть:

- регулярными, время появления, которых получателю информации известно, например сигналы точного времени,
- 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 разговоров может с достаточно высокой вероятностью служить демаскирующим признаком закладного устройства с акустическим автоматом.

## 2.4. Демаскирующие признаки веществ

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.

**Веществом** называют материальные объекты в твердом, жидком или газообразном состоянии, состоящие из частиц одного или нескольких химических элементов, имеющие массу и объем. Классификация веществ приведена на рис. 2.6.


Рис. 2.6. Классификация веществ

Вещества делятся на простые и химические соединения (сложные). **Простые вещества** состоят из атомов одного химического элемента, **химические соединения** — из разных элементов. Химический элемент образуют атомы с одинаковым положительным зарядом ядра (с одинаковым порядковым номером в периодической системе Д. И. Менделеева). Атомы химических элементов могут существовать в свободном состоянии при очень высокой температуре или в составе простых веществ. Свойства химических соединений не совпадают со свойствами образующих его химических элементов.

**По свойствам химические элементы** условно делятся на **металлы и неметаллы.** К металлам относятся простые вещества, имеющие в обычных условиях кристаллическую структуру (кроме ртути), хорошую теплопроводность и электропроводность.

Простые вещества, не обладающие признаками металлов, относятся к **неметаллам**.

**Химические соединения**, в состав которых входит элемент углерод, относят к **органическим.** Но простейшие соединения углерода (оксиды — соединения из углерода и кислорода, угольная кислота и ее соли, некоторые другие),

**Химические соединения,** не содержащие углерод, относятся к **неорганическим соединениям**.

**Классификация основных признаков веществ** представлена на рис. 2.7.

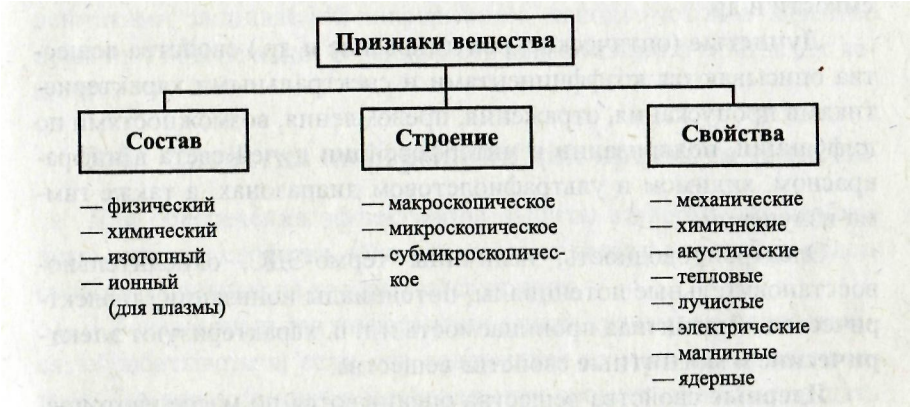



Рис. 2.7. Классификация признаков веществ

**Состав:**

**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.**

**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 газового разряда (для газообразных веществ).

**Строение:**

**Строение веществ** описывают на макроскопическом, микроскопическом и субмикроскопическом уровнях. Оно может представлять собой кристаллическую решетку, набор макромолекул, молекул, субатомных частиц и атомов.

**Свойства:**

**Механические** свойства веществ характеризуют их прочность на сжатие и растяжение, твердость, вязкость, плотность, пористость, пластичность, смачиваемость, непроницаемость 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-излучений.

**Электрические и магнитные** свойства вещества: электропроводность, величины термо-ЭДС, окислительно-восстановительные потенциалы, потенциалы ионизации, диэлектрическая и магнитная проницаемость и т. п.

**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 содержатся не только в конечном продукте, но и в исходных и промежуточных продуктах технологического процесса, применяемых для получения этого вещества. Вещество, содержащее демаскирующие вещественные признаки объекта защиты или технологию его изготовления, называют **демаскирующим веществом.** 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. В результате физико-химического анализа демаскирующих веществ добывается информация о составе, структуре, свойствах и технологии изготовления продукции, которая может содержать государственную и 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.

# 3. ХАРАКТЕРИСТИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

## 3.1. Виды угроз безопасности информации, защищаемой техническими средствами

Угрозы создают потенциальную опасность для объекта или предмета защиты. Сосулька на крыше дома весной создает угрозу жизни прохожих, но она не влияет на их здоровье, пока не упадет на голову. Также изменения в информации или ее хищение возникают при реализации угроз. Следовательно, **угрозы представляют собой состояния или действия взаимодействующих с носителями информации субъектов и объектов материального мира, которые могут привести к изменению, уничтожению, хищению и блокированию информации.** Под блокированием информации понимаются изменения условий хранения информации, которые делают ее недоступной для пользователя.

Угрозы, при реализации которых происходит воздействие различных сил (механических, электрических, магнитных) на источник информации, называются **угрозами воздействия на источник информации,** а угрозы, приводящие к несанкционированному распространению носителя к злоумышленнику, — **угрозами утечки информации.** Классификация угроз рассмотрена на рис. 3.1.

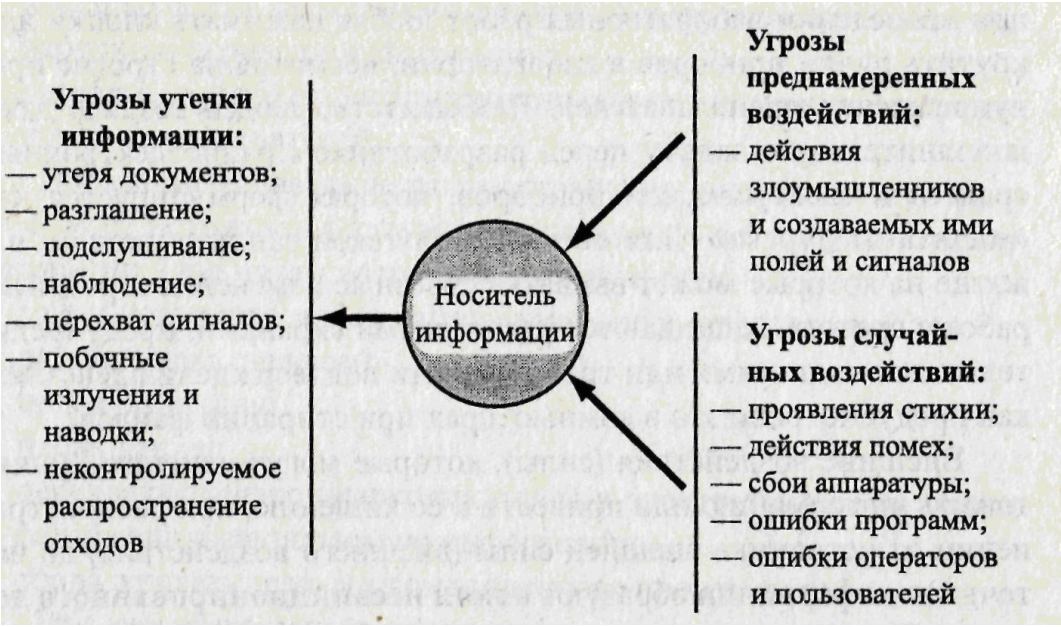



Рис. 3.1. Виды угроз

Воздействия, которые создаются злоумышленниками, являются **преднамеренными.** К ним относятся как непосредственные воздействия людей (злоумышленников) на источник информации, так и воздействия полей и электрических сигналов технических средств, создаваемых людьми с целью уничтожения, изменения или хищения информации. Например, электромагнитный импульс, возникающий во время атомного взрыва или излучения элек-

тромагнитной пушки, способен уничтожить (стереть) информацию на машинных носителях.

На источники информации постоянно действуют случайные силы, вызванные стихией природы, случайными физическими процессами в средствах хранения, обработки и передачи информации, ошибками операторов и технического персонала. Такие угрозы воздействия называются **случайными.** С целью уменьшения влияния неблагоприятных факторов окружающей среды в хранилищах архивов и музеев поддерживают определенную температуру, влажность, химический состав воздуха.

Внешние воздействия (силы), которые могут изменить, уничтожить информацию или привести к ее хищению, при распространении от источника внешней силы (внешнего воздействия) до источника информации образуют **канал несанкционированного доступа.** Если эти силы целенаправленно организуются, то канал несанкционированного доступа называется **преднамеренный,** если силы случайные, то канал несанкционированного доступа — **случайный.**

Причин возникновения каналов несанкционированного доступа очень много. Типовыми из них являются:

- выполнение операции по добыванию информации органом разведки зарубежного государства, конкурента, криминальной структуры;
- попытки несанкционированного получения информации сотрудником организации или иным физическим лицом с целью ее продажи, шантажа, мести и другим мотивам;
- проявление стихийных сил (пожара, наводнения, урагана, землетрясения);
- неисправности программно-аппаратных средств хранения, обработки и передачи информации;
- ошибки в работе с программно-аппаратными средствами операторов и пользователей.

Несанкционированное распространение носителя с информацией от ее источника к злоумышленнику называется **утечкой информации.** Она может возникнуть в результате:

- утери источника информации (документа, продукции и др.);
- разглашения сведений;
- подслушивания;
- наблюдения;
- перехвата электромагнитных полей и электрических сигналов, содержащих защищаемую информацию;
- сбора отходов дело- и промышленного производства.

Эти действия пользователя информации и злоумышленника создают угрозы утечки информации, которые в случае попадания ее к злоумышленнику приводят к утечке.

При **случайной утере** источника закрытой информации они попадут к злоумышленнику при совпадении многих условий, в том числе, если источник будет найден злоумышленником или человеком, который ему его пере-

даст. Вероятность этого невысока. Чаще найденный на территории организации источник возвращается человеку, который его потерял, или передается соответствующим должностным лицам.

Утечка информации в результате ее **непреднамеренного разглашения** происходит чаще, чем утеря источника. Даже прошедшие инструктаж люди не могут постоянно контролировать свою речь, особенно в случае повышенного эмоционального состояния. Например, в перерыве закрытого совещания его участники часто продолжают обсуждение вопросов совещания в коридоре и в местах для курения, в которых могут находиться посторонние люди. Разглашение возможно в городском транспорте, на улице, дома, на различных научных и иных конференциях. Ученые для получения признания у зарубежных коллег разглашают полученные научные сведения, содержащие государственную тайну. Они для оправдания своих действий навязывают обществу мнение, что научные результаты принадлежат всему человечеству, забывая при этом, что человечество состоит из отдельных государств и людей, которые беззастенчиво используют их для достижения собственных целей, противоречащих интересам большинства людей. Слова об общечеловеческих ценностях или интересах народа часто используются как красивые бумажки, в которые заворачивают корысть. История знает много примеров того, к каким бедам и трагедиям людей приводила «борьба за народные интересы и общечеловеческие ценности».

Несанкционированный прием злоумышленником (его техническим средством) сигнала с защищаемой информацией и его демодуляция позволяют ему добывать эту информацию. При этом на носитель никакого воздействия не оказывается, что обеспечивает скрытность добывания. Прием оптических и иных сигналов от объектов и получение с их помощью изображений этих объектов называются **наблюдением,** прием и анализ акустических сигналов — **подслушиванием,** а прием и анализ радио - и электрических сигналов — **перехватом.** Исторически сложившиеся названия могут вызывать неоднозначность толкования. Например, подслушивание может быть непосредственным (с помощью ушей) и с помощью технических средств. Причем в последнем варианте оно может осуществляться в принципе на любом расстоянии, например, путем перехвата междугородних или международных телефонных разговоров.

**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.

**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, чертеж т. д. Например, текст или схема конструкции прибора на столе руководителя или специалиста могут быть подсмотрены в ходе их посещения. Также возможно наблюдение через окно помещения 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;
- с помощью приборов 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, в принципе, 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

**Перехват** предполагает несанкционированный прием радио - и электрических сигналов и извлечение из них семантической информации, демаскиру-

ющих признаков сигналов и формирование изображений объектов при перехвате телевизионных или факсимильных сигналов.

Многообразие технических средств и их комплексное применение для добывания информации порой размывают 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.

Следовательно, **угрозы утечки информации представляют собой условия и действия, при которых носитель с защищаемой информацией может попасть к злоумышленнику.** Путь несанкционированного распространения носителя информации от источника к злоумышленнику называется **каналом утечки информации.** Если распространение информации производится с помощью технических средств, то канал утечки информации называется **техническим каналом утечки информации.**

Угрозы утечки, так же как угрозы воздействия, могут быть случайными и преднамеренно создаваемыми злоумышленником. Если характеристики источников опасных сигналов злоумышленнику априори не известны, то технические каналы утечки информации являются **случайными.** Когда технический канал утечки информации организуется злоумышленником, например, с помощью закладного устройства, то такой канал утечки информации является **организованным.**

Угроза оценивается по величине ущерба, который возникает при ее реализации. Различается **потенциальный и реальный ущерб.** Потенциальный ущерб существует при появлении угрозы, реальный — при реализации угрозы. Вероятность или риск возникновения угрозы зависит от многих факторов, основными из которых являются:

- цена защищаемой информации;
- уровень защищенности информации;
- квалификация злоумышленника, его ресурс и затраты на добывание им информации;
- криминогенная обстановка в месте нахождения организации.

Чем выше цена информации, тем сильнее побудительный мотив для злоумышленника. Любой здравомыслящий преступник, задумывая преступление, рассчитывает получить больше, чем он потратит на его подготовку и выполнение. Поэтому вероятность угрозы $P_{ву}$ выше нуля тогда, когда цена информации превышает затраты на ее добывание. Она резко возрастает при существенном увеличении отношения цены информации $C_и$ к затратам на ее добывание $C_д$ — $C_и$ / $C_д$. Качественно эта зависимость иллюстрируется кривой на рис. 3.2.

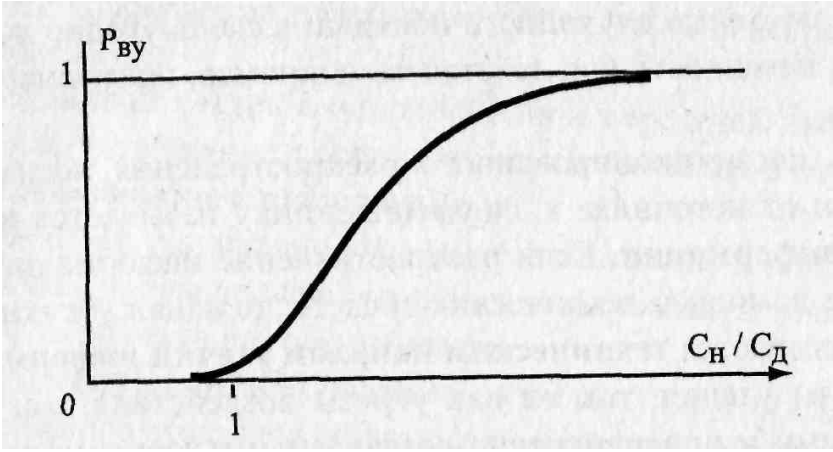



Рис. 3.2. Зависимость вероятности возникновения угрозы утечки от соотношения цены информации и затрат злоумышленника на ее добывание

Уровень защищенности информации определяет затраты на добывание информации. Его рост уменьшает отношение $C_и / C_д$, следовательно, вероятность угрозы.

Вероятность реализации возникшей угрозы определяется уровнем ее защиты и квалификацией злоумышленника. Чем выше уровень защиты, тем сложнее довести процесс добывания информации до конца.

## 3.2. Источники угроз безопасности информации, защищаемой техническими средствами

Любая угроза, в том числе безопасности информации, имеет свой источник. Эффективно предотвращать угрозы можно, если известны ее источники, так же как нельзя вылечить человека, не устранив причину болезни, — можно лишь временно устранить ее симптомы. Когда у человека болит голова, он принимает таблетку анальгина или другого болеутоляющего лекарства. Но через некоторое время боль возобновляется. Это будет повторяться до тех пор, пока не будет устранена причина головной боли. Поэтому в современной медицине возрастающее внимание уделяется диагностике болезней, создаются оснащенные современной техникой диагностические центры.

Раскрытие любого преступления начинается также с ответа на вопрос «кому это выгодно?». По этой же причине служба безопасности любой структуры постоянно занимается выявлением источников возможных угроз в деятельности организации или фирмы. Однако сделать это не так просто. Многие источники угроз тщательно маскируются. Между угрозой и ее источником может существовать длинная цепочка посредников. Часто эту цепочку для скрытия источника разрывают, убивая, например, киллера после реализации им угрозы.

**В общем случае источниками преднамеренных угроз являются:**

- органы зарубежной разведки;
- органы разведки коммерческих структур государства;
- криминальные структуры;

- завербованные, психически больные или недовольные своим положением сотрудники организации.

Наибольшие угрозы информации создают профессионалы. 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 различаются.

**Самую мощную разведку имеют США**. В настоящее время, согласно открытой зарубежной печати, структуру разведывательного сообщества США образуют следующие организации:

- Центральное разведывательное управление (ЦРУ);
- Министерство национальной безопасности;
- Разведывательные подразделения Министерства обороны США;
- Разведывательные подразделения гражданских ведомств США;
- Штаб разведки разведывательного сообщества или Центральная разведка.

**ЦРУ** является наиболее крупной разведывательной организацией и состоит из пяти основных директоратов (оперативного, научно-технического, информационно-аналитического, административного и планирования) и ряда самостоятельных подразделений (финансово-планового отдела, отдела шифрования, секретариата, управления по связи с общественностью и др.).

**Оперативный директорат** решает задачи по добыванию информации силами агентурной разведки, организации и проведения тайных операций, по осуществлению контрразведывательного обеспечения агентурной деятельности, по борьбе с терроризмом и наркобизнесом.

**Научно-технический директорат** проводит исследования и разработки в области технических средств разведки, эксплуатирует стационарные технические комплексы сбора, обработки и передачи информации, обеспечивает сотрудничество с научными центрами США.

**Информационно-аналитический директорат** проводит обработку и анализ разведывательной информации и готовит выходные документы для президента, Совета национальной безопасности, конгресса и других потребителей.

**Административный директорат** занимается вопросами подбора кадров на работу в ЦРУ, их подготовкой и переподготовкой, обеспечивает безопасность персонала и объектов ЦРУ и др.

**Директорат планирования** занимается планированием и координацией деятельности разведки.

**В число разведывательных подразделений Министерства обороны входят:**

- разведывательные подразделения собственно Министерства обороны;
- разведывательные подразделения Министерства армии США;
- разведывательные подразделения Министерства ВВС США;
- разведывательные подразделения ВМС США.

В свою очередь, основными разведывательными подразделениями собственно Министерства обороны являются:

- Разведывательное управление Министерства обороны (РУМО), занимающегося военно-стратегической разведкой;
- Агентство национальной безопасности (АНБ), которое ведет радиоэлектронную разведку, а также разрабатывает коды и шифры. Оно располагает одним из самых крупных центров по обработке данных, самыми мощными ЭВМ, имеет около 2 тыс. станций радиоэлектронного перехвата, численность персонала составляет более 120 тыс. человек. Силы и средства АНБ составляют основу системы радиоэлектронной разведки «Эшелон», обеспечивающей перехват информации по всему миру;
- Национальное управление военно-космической разведки.

**К разведывательным организациям гражданских ведомств США относятся:**

- управление разведки и исследований Госдепартамента;
- разведывательные подразделения Министерства энергетики;
- разведывательные подразделения Министерства торговли;
- разведывательные подразделения Министерства финансов;
- управление Федерального бюро расследований (ФБР).

Разведка Госдепартамента обеспечивает сбор информации, необходимой для проведения внешней политики США, участвует в разработке разведывательных операций и национальных разведывательных программ США.

Разведывательные подразделения других ведомств собирают информацию об экспортных операциях, о финансовом и валютном положении иностранных государств, об энергетике других государств, особенно об атомной энергетике, разработке и производстве ядерного оружия и по другим вопросам.

Управление контрразведки ФБР не только само ведет сбор разведывательной информации об иностранных гражданах, но и оказывает помощь другим организациям разведывательного сообщества.

Даже из краткого перечня разведывательных служб США следует, что разведкой занимаются все основные государственные структуры: от президента, который возглавляет СНБ, до различных ведомств.

Мощную разведку имеют другие развитые страны, прежде всего Россия, Великобритания, Германия, Франция, Израиль.

Состав органов разведки коммерческих структур существенно различается в зависимости от ее возможностей, прежде всего, капитала и вида деятельности. Разведка промышленных гигантов может составить конкуренцию государственной разведке. Разведкой мелкой фирмы могут заниматься всего несколько человек службы безопасности.

Организованная преступность располагает также большими финансовыми и техническими возможностями для ведения разведки и добывания информации.

Преднамеренные угрозы воздействия реализуются путем **непосредственного и дистанционного воздействия** на источник информации. Для

непосредственного воздействия на источник информации злоумышленник должен проникнуть к источнику информации, преодолев рубежи защиты и контролируемые зоны. Очевидно, что риск обнаружения и задержания злоумышленника силами и средствами системы защиты информации велик. Существенно меньший риск для злоумышленника возникает при использовании им средств дистанционного воздействия на информационные параметры источника информации.

Современные средства силового разрушающего воздействия представляют собой по существу электромагнитное оружие, способное дистанционно вывести из строя любую информационную систему, в том числе уничтожить хранящуюся или обрабатываемую в ней информацию. Электромагнитное оружие генерирует поток кратковременных (длительностью в единицы и менее наносекунд) и чрезвычайно мощных электрических (напряжением единицы и десятки кВ) импульсов или радиоимпульсов (мощностью в сотни и тысячи кВт), которые, распространяясь по проводам или в пространстве в виде узконаправленного луча, разрушают элементы радиоэлектронных средств обработки и хранения информации и (или) изменяют значения информационных параметров носителей информации.

Органы разведки различных структур являются источниками угроз воздействий и утечки информации. Они могут оказывать как воздействия на источник информации, так и на носители ее в виде сигналов и отходов производства. Источники случайных угроз отличаются от преднамеренных угроз отсутствием у них целей по изменению, уничтожению, хищению и блокированию информации.

Среди стихийных сил, которые могут в случае возникновения оказать воздействие на носитель информации, наибольшую угрозу создает пожар. Он наиболее часто происходит, может полностью уничтожить носители информации, его тушение может сопровождаться залитием мест пожара водой и пеной с не менее разрушительными для носителя информации последствиями.

В соответствии со статьей 1 Закона РФ «О пожарной безопасности» **пожар — неконтролируемое горение, причиняющее материальный ущерб, вред жизни и здоровью граждан, интересам общества и государства**». Под горением понимается сложная физико-химическая реакция окисления, сопровождающаяся выделением тепла и дыма, появлением пламени или тления. Для возникновения горения необходимо наличие «треугольника горения»: **горючей среды, источника зажигания и окислителя.**

Источниками угроз пожара, наводнения, механических разрушений могут быть не только природные явления, но и плоды недобросовестной деятельности человека, который своевременно не ремонтирует здания, помещения и их инфраструктуру. Наиболее частой причиной пожара в зданиях называют короткое замыкание между проводами электропроводки, которое возникает, прежде всего, из-за разрушения вследствие старения изоляции проводов.

Проржавевшие трубы водо- и теплоснабжения в случае их прорыва могут вызвать наводнение, особенно разрушительное в случае горячей воды.

Так как утечка информации по акустическому, оптическому и радиоэлектронному техническим каналам происходит с помощью сигналов, в информационные параметры которых записывается защищаемая информация, то источниками угроз утечки являются, прежде всего, источники сигналов в этих каналах.

### 3.3. Опасные сигналы и их источники

Носители информации в виде полей и электрического тока называются **сигналами.** Если информация, содержащаяся в сигналах, секретная или конфиденциальная, а сигналы могут быть приняты (перехвачены, подслушаны) злоумышленником и с них, в принципе, может быть «снята» эта информация, то такие сигналы представляют опасность для информации и называются **опасными. Опасные сигналы** – сигналы, содержащие секретную или конфиденциальную информацию, которые могут быть приняты злоумышленником способным сныть с них информацию.

Опасные сигналы могут быть **функциональными** и **случайными.**

**Функциональные сигналы** создаются для выполнения радиосредством заданных функций по обработке, передаче и хранению информации. При передаче закрытой информации функциональными сигналами ее отправитель осознает потенциальные угрозы безопасности содержащейся в сигналах информации. Принимает он необходимые меры или нет, это его выбор. По небрежности или злому умыслу, он иногда пренебрегает этими мерами. Например, на раннем этапе становления рыночных отношений бизнесмены часто по радиотелефонной сотовой связи разглашали сведения, составляющие коммерческую тайну. Более опытные люди при разговоре по открытой телефонной линии для скрытия от посторонних ушей некоторых аспектов разговора применяют так называемый «эзоповский» язык, т. е. слова со скрытым смыслом, не всегда понятным посторонним лицам.

**К основным источникам функциональных сигналов относятся:**

- передатчики (источники сигналов) систем связи;
- передатчики радиотехнических систем;
- излучатели акустических сигналов гидролокаторов и акустической связи;
- люди как источники условных сигналов.

**Средства систем связи** образуют наиболее многочисленную и разнообразную группу источников сигналов с семантической информацией. К системам и средствам связи относятся системы и средства радиосвязи, проводной, радиорелейной, космической и оптической связи, ионосферной, тропосферной и метеорной радиосвязи. Они занимают ведущее место в обеспечении информационного обмена во всех сферах общественно-производственной деятельности и личной жизни людей.

Источниками радиосигналов, излучаемых в окружающее пространство, являются стационарные и мобильные радиопередающие устройства систем радиосвязи, а электрических сигналов, передаваемых по проводам, — теле-

фонные, телеграфные, факсимильные аппараты, ПЭВМ, объединенные в сети, модемы аппаратуры передачи данных, телевизионные камеры кабельного телевидения и др.

В последнее время для передачи информации в качестве источников сигналов применяются также лазеры оптических средств связи. Уступая радиосигналам по дальности распространения, в особенности при неблагоприятных климатических условиях, оптические системы связи имеют значительно лучшие параметры по полосе пропускания и помехоустойчивости. Кабели волоконно-оптических линий связи с широкими возможностями по уменьшению величины затухания света и снижения себестоимости изготовления постепенно вытеснят металлические кабели проводных систем электросвязи.

Радио, электрические и световые сигналы циркулируют как внутри организации, так и распространяются на большие, а при их ретрансляции — на любые расстояния. По телефону можно переговорить с абонентом в любом месте Земли, радиосигналы соответствующей частоты и мощности способны донести информацию также до любой ее точки.

Учитывая широкое применение средств связи и большие дальности распространения сигналов, перехват сигналов средств связи представляет один из эффективных и широко распространенных методов добывания информации. Сигналы средств связи содержат не только семантическую информацию, но и информацию о признаках сигналов и местоположении их источников. Такая информация характеризует технические решения новых средств и их возможности, что представляет интерес, как для внутреннего, так и для внешнего (зарубежного) конкурента.

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

Среди радиотехнических систем и средств значительную долю занимают радиолокационные станции, предназначенные для наблюдения воздушного пространства и земной поверхности в радиодиапазоне. Возможности радиолокаторов по добыванию информации определяются в основном характеристиками радиотехнических сигналов и распределением их энергии в пространстве (диаграммой направленности). 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.

Так как радио- и гидролокационные станции создают техническую основу для противоракетной, противовоздушной и противолодочной обороны, то параметры сигналов новейших локаторов вызывают большой интерес у разведки других государств. Очевидно, что 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. Радио-

телеметрические средства и системы обеспечивают измерение и передачу различных физических величин удаленных объектов, а средства и системы радиотелеуправления — управление ими.

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 фразами часто пользуются люди во время конфиденциального разговора по открытому телефону, условными сигналами (паролями) обмениваются незнакомые люди при конфиденциальной встрече.

Однако работа радиоэлектронных средств, используемых для приема, обработки, хранения и передачи сигналов, а также различных электрических приборов сопровождается явлениями и физическими процессами, которые могут создавать побочные радио - и электрические сигналы. Если эти сигналы по тем или иным причинам могут содержать секретную или конфиденциальную информацию и к ним возможен доступ технических средств злоумышленника, то опасность для этой информации существенно выше, чем для аналогичной информации, но содержащейся в функциональных сигналах. Такие случайно возникающие сигналы называются **случайными опасными сигналами.** Эти сигналы возникают в силу объективных физических процессов, часто независимо от пользователя технического средства. Без проведения специальных исследований его пользователь может и не знать о наличии случайных сигналов и тех угроз, которым подвергается секретная или конфиденциальная информация. В этом состоит существенное отличие функциональных опасных сигналов от случайных опасных сигналов.

К техническим средствам обработки, передачи и хранения, создающим опасные сигналы, относятся:

- средства телефонной проводной связи;
- средства мобильной телефонной и радиосвязи;
- средства электронной почты;
- средства электронной вычислительной техники;
- аудиоаппаратура и средства звукоусиления;
- радиоприемные устройства;
- видеоаппаратура;
- телевизионные средства;
- средства линейной радиотрансляции и оповещения.

Кроме того, случайные опасные сигналы создают электрические приборы, в том числе:

- средства охранной сигнализации;
- средства пожарной сигнализации;
- средства размножения документов;
- средства системы кондиционирования и вентиляции воздуха;
- бытовые приборы, оргтехника и иное производственное оборудование, имеющее в своем составе элементы преобразования акустической ин-

формации в электрические сигналы (акустоэлектрические преобразователи);

- электропроводящие коммуникации здания, проходящие через контролируемую зону.

Характеристики опасных случайных сигналов радиоэлектронных средств и электрических приборов априори неизвестны ни злоумышленнику, ни их пользователю. Для их обнаружения и определения характеристик проводят специальные проверки и исследования этих средств и приборов.

В зависимости от принадлежности циркулирующей (обрабатываемой, хранящейся, передаваемой) в технических средствах и системах информации к секретной (конфиденциальной) или несекретной эти средства и системы делятся на **основные технические средства и системы (ОТСС)** и **вспомогательные технические средства и системы (ВТСС).**

К основным техническим средствам и системам относятся средства (системы) и их коммуникации (линии связи), обеспечивающие обработку, хранение и передачу защищаемой информации. Из этого не следует, что ОТСС должны обрабатывать только защищаемую информацию. В условиях рынка это экономически нецелесообразно. В общем случае ОТСС могут использоваться для решения задач, не связанных с сохранением тайны, но в них априори приняты меры по защите информации. Если в технических средствах (системах) приема, обработки, хранения и передачи информации такие меры отсутствуют, то они относятся к вспомогательным. Вспомогательные технические средства и системы (ВТСС) не предназначены для обработки защищаемой информации, но могут размещаться совместно с ОТСС в контролируемой зоне. Последнее замечание имеет принципиальное значение, так как именно близость размещения ВТСС к ОТСС вынуждает рассматривать вспомогательные средства и системы как потенциальные источники опасных сигналов. Из сравнения назначения ОТСС и ВТСС следует, что множества ОТСС и ВТСС пересекаются. Действительно, в одном помещении могут размещаться средства, например, однотипные компьютеры, часть из которых являются основными, другие — вспомогательные. Вспомогательный компьютер может быть подключен к интегральной сети общего пользования, например к Internet, что нельзя делать для компьютера, относящегося к основному средству обработки информации. К ВТСС отнесены:

- различного рода телефонные средства и системы;
- средства и системы передачи данных в системе радиосвязи;
- средства и системы охранной и пожарной сигнализации;
- средства и системы оповещения и сигнализации;
- средства и системы кондиционирования;
- средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания и радиоприемники и т. д.);
- средства электронной оргтехники;

# 4. МЕТОДЫ ДОБЫВАНИЯ ИНФОРМАЦИИ

## 4.1. Основные принципы разведки

Жизненная необходимость в информации для любых государственных или коммерческих организаций 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.

Добывание информации органами разведки основывается на следующих принципах:

- целеустремленность;
- активность;
- непрерывность;
- скрытность;
- комплексное использование сил и средств добывания информации.

**Целеустремленность** предусматривает определение задач и объектов разведки, ведение ее по единому плану и сосредоточение усилий органов разведки на выполнении основных задач.

**Активность** предполагает активные действия всех элементов системы разведки по добыванию информации, прежде всего по поиску оригинальных способов и путей решения задач применительно к конкретным условиям.

**Непрерывность** разведки подчеркивает постоянный характер добывания информации, и независимость этих действий от времени года, суток, погоды, любых условий обстановки. При изменении обстановки в соответствии с принципом активности меняются способы и средства добывания.

**Скрытность** ведения разведки обеспечивается путем проведения мероприятий по подготовке и добыванию информации в тайне, в интересах, как безопасности органов добывания, так и скрытия фактов утечки или изменения информации. Реализация этого принципа позволяет разведке повысить безопасность органа добывания и выиграть время для более эффективного применения добытой информации.

О том, что конфиденциальная информация стала достоянием конкурента, руководство фирмы узнает обычно по косвенным признакам:

- снижению доходов или усилению позиций конкурента в связи с «выбросом» им на рынок аналогичных товаров, но с лучшими потребительскими свойствами или по более низким ценам;
- появлению публикаций в периодической печати и патентов по результатам исследований, ведущихся в лабораториях фирмы;
- перераспределению традиционной клиентуры в пользу конкурента.

Скрытность достигается применением пассивных технических средств, маскировкой и камуфлированием аппаратуры, легендированием и засекречиванием мероприятий по добыванию информации.

Учитывая многообразие способов и форм отображения информации, ориентация на способы и средства ее добывания, эффективные в определенных условиях, далеко не всегда приводит к положительным результатам в других условиях. Поэтому эффективное добывание информации проводится путем **комплексного использования различных способов и средств добывания информации.** Кроме того, при комплексировании обеспечивается дублирование данных, что является основным направлением повышения достоверности получаемой информации.

Добывание информации на основе указанных принципов осуществляется постоянно легальными способами и при недостаточности полученной этими способами информации — путем проведения тайных операций.

Легальное добывание информации проводится путем изучения и обработки по интересующим разведку вопросам публикаций в средствах массовой информации, периодических научных и популярных журналах, трудах высших учебных заведений и научно-производственных организаций, правительственных изданиях, учебных пособиях и др. Ценную информацию можно получить из открытых правительственных источников и отчетов. Нужную информацию можно найти в материалах, имеющих непосредственное отношение к деятельности фирмы: в соглашении о лицензиях, статьях и докладах, годовых отчетах фирм, отчетах коммивояжеров, обзорах рынков и докладов инженеров-консультантов, внутренних печатных изданиях, телефонных справочниках, рекламной литературе и проспектах. Этот перечень можно многократно продолжить. По оценке заместителя начальника разведки ВМС США Захариаса во время Второй мировой войны разведка ВМС США получала 95% информации из открытых источников.

Органы обработки информации зарубежной разведки ведущих стран выписывают практически всю открытую центральную и местную печатную продукцию других государств. Результаты анализа возможностей добывания информации из легальных источников свидетельствуют, во-первых, о росте таких источников и, во-вторых, о том, что по мере роста объема мало управляемых информационных потоков все большая часть информации, содержащая тайну, попадает в открытые источники.

Однако наиболее ценная информация добывается нелегальным путем, в результате проведения тайных мероприятий спецслужбами и органами коммерческой разведки. Нельзя сбором и анализом сколь угодно большого объема открытых данных определить формулу и технологию нового вещества, если они изложены в документе, хранящемся за семью печатями.

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 орга-

нов чувств или используемых им технических средств, копирования информации и передачи ее потребителю.

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.

## 4.2. Классификация технической разведки

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 (рис. 4.1) [2]:

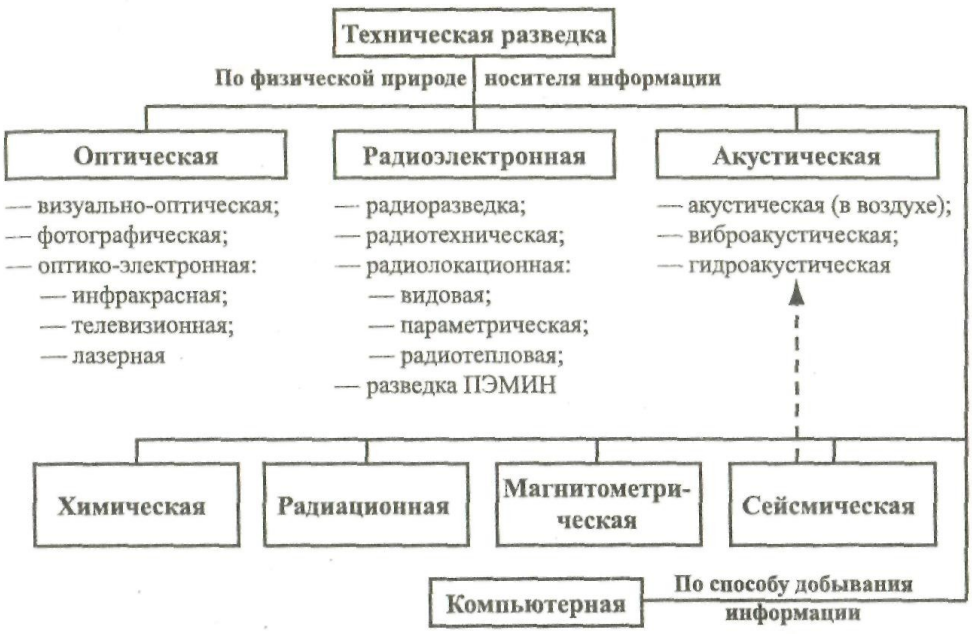



Рис. 4.1. Классификация технической разведки

- оптическая разведка (носитель — электромагнитное поле в видимом и инфракрасном диапазонах);
- радиоэлектронная разведка (носитель — электромагнитное поле в радиодиапазоне или электрический ток);
- акустическая разведка (носитель — акустическая волна в газообразной, жидкой и твердых средах);
- химическая разведка (носитель — частицы вещества);

- радиационная разведка (носитель — излучения радиоактивных веществ);
- сейсмическая разведка (носитель — акустическая волна в земной поверхности);
- магнитометрическая разведка (носитель — магнитное поле).

В связи с бурным развитием вычислительной техники самостоятельное значение приобретают силы и средства, добывающие информацию из компьютеров и вычислительных сетей. Классификационный признак для этого сравнительно нового вида технической разведки — **компьютерной разведки,** иной, чем для указанных видов рассматриваемой классификационной схемы, а именно — способы добывания информации. Основным способом добывания информации этим видом является перехват сигналов в компьютерах и их сетях. Учитывая, что компьютеры становятся основным средством обработки и хранения информации, возможности ее непрерывно растут.

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.

В **визуально-оптической** разведке человек добывает информацию с помощью визуальных приборов.

**Фотографическая разведка** позволяет регистрировать изображение объекта наблюдения на фотопленке, на магнитную ленту; – на DVD-диск; – на жесткий диск; – на флэш-карту.

Средства **инфракрасной разведки** преобразуют изображение в инфракрасном диапазоне в видимое, но одноцветное изображение, цвет которого соответствует свечению люминофора экрана.

**Телевизионная** разведка обеспечивает не только добывание информации о движущихся объектах, но и передачу этой информации на большое расстояние.

**Лазерная разведка** решает две группы задач: получение информации по результатам облучения объекта лазерным лучом (для подсветки, измерения дальности, дистанционного физического и химического анализа) и определения источников и характеристик лазерного излучения. Последние три вида, использующие электронную технику, образуют **оптикоэлектронную разведку.** Технический прогресс размазывает границу между фотографической и оптикоэлектронной разведкой. Наряду с традиционными пленочными фотоаппаратами интенсивно развивается цифровая фотография. Основу ее составляют светоэлектрические преобразователи, на выходе, которого эквивалент-

ные изображению сигналы оцифровываются и в цифровой форме запоминаются в устройствах полупроводниковой или магнитной памяти.

**Радиоэлектронная разведка** в зависимости от характера добываемой информации подразделяется на:

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

**Радиоразведка** добывает, в основном, семантическую информацию путем перехвата радиосигналов с конфиденциальной информацией,

**Радиотехническая** добывает информацию о параметрах (признаках) радиотехнических сигналов,

**Радиолокационная** добывает информацию о видовых признаках радиолокационного изображения объекта на экране радиолокатора,

**Радиотепловая** добывает информацию о признаках, проявляющихся через собственные электромагнитные излучения объектов в радиодиапазоне.

Силы и средства, используемые для добывания информации из побочных электромагнитных излучений и наводок, образуют разведку **ПЭМИН**, которая отличается от радиоразведки более чувствительной аппаратурой.

**Акустическая разведка** в зависимости от среды распространения акустической волны делится

- акустическую (в воздухе),
- гидроакустическую (в воде) и
- виброакустическую (в твердой среде, в основном в строительных конструкциях и различных трубах).

**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 объекты, например подводные лодки в погруженном состоянии.

**Сейсмическая разведка** обеспечивает добывание информации из акустических (сейсмических) волн, распространяющихся в земной коре. Корректно включить в этот вид как подвид в акустическую разведку, как показано на рис. 6.1 пунктирной стрелкой. Однако в документах и структурно сейсмическая разведка выделена в отдельный вид.

### 4.3. Технология добывания информации

Независимо от принадлежности органа разведки и решаемых им задач технология добывания информации в общем случае представляет процесс, который начинается с момента постановки задачи ее пользователями (военно-

политическим руководством страны или отдельных ведомств, руководством фирмы) до момента предоставления пользователям информации, соответствующей поставленным задачам и требованиям.

Технология добывания информации предусматривает следующие этапы:

- организация добывания;
- добывание данных и сведений;
- информационная работа.

Любая деятельность без организации представляет собой хаотичный процесс.

**Организация добывания информации включает**:

- декомпозицию (структурирование) задач, поставленных пользователями информации;
- разработку замысла операции по добыванию информации;
- планирование;
- постановку задач исполнителям;
- нормативное и оперативное управление действиями исполнителей и режимами работы технических средств.

Постановка соответствующих плану задач исполнителям перед проведением разведывательной операции рассматривается как **нормативное управление.** Но неучтенные факторы и изменившиеся условия требуют внесения корректив в процесс управления. Такое управление называется **оперативным.** Организацией добывания информации занимаются органы планирования и управления.

**Добывание данных и сведений.** Сведения и данные добываются соответствующими органами путем поиска источников информации и ее носителей, их обнаружения, установления разведывательного контакта с ними, получения данных и сведений. Сведения и данные представляют фрагменты информации и отличаются друг от друга тем, что данные снимаются непосредственно с носителя, а сведения— проанализированные данные.

**Поиск объектов разведки** (источников и носителей информации, источников сигналов) производится в пространстве и во времени, а для носителей в виде полей и электрического тока — также по частоте сигнала. Поиск завершается обнаружением объектов разведки и получением от них данных.

**Обнаружение** интересующих разведку объектов в процессе поиска производится по их демаскирующим признакам и заключается в процедуре выделения объекта на фоне других объектов. Основу процесса обнаружения составляет процедура **идентификации** — отождествление путем сравнения текущих признаковых структур, формируемых в процессе поиска, с эталонной признаковой структурой объекта разведки.

Эталонные признаковые структуры содержат достоверные (по оценке органов разведки) признаки объекта или сигнала, полученные от первоисточников, например из документа или по данным, добытым из разных источников. Например, фотография в паспорте является эталонным описанием лица конкретного человека. Его признаковая структура состоит из набора признаков лица, которые криминалисты используют для составления фотороботов.

Эталоны по мере изменения признаков корректируются. Например, несколько раз в течение жизни человека заменяются фотографии в паспорте, которые представляют собой эталонные изображения владельца паспорта для идентификации его личности. Эталонные признаковые структуры об объектах окружающего мира человек хранит в своей памяти. Он постоянно их формирует в процессе развития, обучения и работы. Когда человек рождается, у него отсутствуют эталонные признаковые структуры объектов окружающего мира. В процессе собственных наблюдений и опыта, полученных знаний у него постепенно и постоянно формируются эталонные признаковые структуры, которые со временем корректируются. Например, когда человек встречает через 20 лет одноклассника, внешний вид которого существенно изменился, то вначале он может и не узнать своего бывшего приятеля, так как наблюдаемые (текущие) признаки отличаются от эталонных двадцатилетней давности. После получения подтверждения о том, что текущие признаки действительно принадлежат его школьному приятелю, в памяти производится корректировка эталона и при следующей встрече сомнения не возникают.

Путем идентификации текущей признаковой структуры с эталонной человек или автомат обнаруживают объект, которому соответствует эталонная признаковая структура. Чем больше признаков совпадает, тем выше вероятность обнаружения объекта.

Добытые данные, как правило, разрозненные. Они преобразуются в сведения, отвечающие на поставленные задачи, в ходе **информационной работы,** выполняемой органами сбора и обработки информации.

**Информационная или аналитическая работа** включает следующие последовательно выполняемые процессы:

- сбор и накопление данных и сведений от органов добывания;
- видовую обработку;
- комплексную обработку.

Данные и сведения (в случае предварительной обработки данных в органе добывания) передаются в орган видовой обработки.

Если в добывании информации участвуют органы различных видов, например, оптической и радиоэлектронной разведки, то осуществляется комплексная обработка сведений, поступивших от органов видовой обработки. Необходимость видовой обработки обусловлена различиями языков признаков, добываемых органами различных видов. Данные от органов добывания поступают, как правило, на языке признаков — параметры сигналов, изображения объектов разведки, координаты источников излучений и т. д. В результате видовой обработки синтезируется информация на профессиональном языке. В результате этого сведения, используемые для комплексной обработки, представляются на одном профессиональном языке. После комплексной обработки итоговая информация представляется на языке ее потребителей.

Видовая и комплексная обработка, в свою очередь, состоит из трех последовательно выполняемых процессов:

- осмысливание данных и сведений,

- построение гипотез и умозаключений
- формулирование выводов,
- проверка выводов.

Последняя операция выполняется с целью исключения грубых ошибок и пропуска дезинформации. При формировании сведений применяются следующие **методы синтеза информации:**

- логические;
- структурные;
- статистические.

**Логические** методы используют для синтеза информации законы логики, учитывающие причинно-следственные связи в реальном мире. Они лежат в основе так называемого «здравого смысла» человека и являются основным методом синтеза информации человеком. Чем большими знаниями и опытом владеет человек, тем больше информативных связей он учитывает при принятии решения. Причинно-следственные временные связи обеспечивают также выявление и прогнозирование действий объектов по признакам их деятельности в различные моменты времени.

**Структурные** методы учитывают объективно существующие связи между элементами объекта. Например, любой прибор имеет многоуровневую иерархическую структуру. Она включает блоки, узлы и детали, которые во время работы взаимодействуют друг с другом. Эти связи определяют конструкцию прибора и зафиксированы в конструкторской документации. При ее отсутствии специалисты восстанавливают конструкцию, назначение и функции по отдельным элементам и связям.

**Статистические** методы обеспечивают идентификацию и интерпретацию объектов и характера их деятельности по часто проявляющимся признакам, получаемым в результате статистической обработки добываемых данных. В качестве таких признаков выступают статистически устойчивые параметры случайных событий: средние значения, дисперсии, функции распределения. Например, частое появление возле территории фирмы одних и тех же людей или автомобилей, обнаружение в помещениях фирмы закладных устройств служат признаками повышенного интереса конкурента или других субъектов к фирме или отдельным ее сотрудникам.

Таким образом, информационная работа включает аналитическую обработку больших массивов данных и сведений. Органы обработки широко привлекают к информационной работе в качестве аналитиков высококвалифицированных специалистов, которые интерпретируют данные и сведения. Кроме того, проводятся интенсивные работы по автоматизации процессов информационной работы.

## 4.4 Способы доступа органов добывания к источникам информации

Возможности разведки по добыванию информации зависят, прежде всего, от способов доступа ее органов добывания (агентов, технических средств) к источникам информации и обеспечения разведывательного кон-

такта с ними [4]. Эти факторы связаны между собой. Чем ближе удается приблизиться органу добывания к источнику информации, тем выше вероятность установления разведывательного контакта с ним.

Доступ к информации обеспечивается, когда 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
- временное.

**Пространственное условие** предполагает, что злоумышленник знает о месте нахождения источника информации или видит объект наблюдения. Если оно не известно, то источник приходится искать. Если область поиска велика, то процесс обнаружения источника информации может существенно затрудниться и затянуться во времени.

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.

Так как добывание информации является динамичным процессом, то необходима синхронизация работы всех элементов, обеспечивающих этот процесс. Необходимость функционирования времени органа добывания, синхронизированного со временем возможности доступа к 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.

Способы несанкционированного доступа к информации можно разделить на три группы:

- физическое проникновение злоумышленника к источнику информации;
- сотрудничество злоумышленника с работником (гражданином другого государства или фирмы), имеющим легальный или нелегальный доступ к интересующей разведку информации;

- дистанционное добывание информации без нарушения границ контролируемой зоны.

Физическое проникновение к источнику информации возможно путем скрытого или с применением силы проникновения злоумышленника к месту хранения источника , 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 априорной информации о месте нахождения источника, системе безопасности, возможных маршрутах движения и других сведений. Кроме того, скрытое проникновение не может носить регулярный характер, так как оно связано с большим риском для злоумышленника и приемлемо для добывания чрезвычайно ценной информации.

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.** К таким источникам относятся, например, документы, которыми можно шантажировать конкурента или вытеснить его с рынка после публикации.

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.** Подкупленный человек может стать постоянным и инициативным источником информации.

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. Зарубежными спецслужбами иногда создаются для приезжающих в их страну специалистов различного рода провокационные ситуации с целью получения компрометирующих материалов для последующего шантажа.

**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 и или любом другом месте вроде бы невинных вопросов, ответы на которые для специалиста содержат конфиденциальную информацию.

Выпытывание под пыткой характерно для криминальных элементов, которые не утруждают себя применением скрытых, требующих длительной подготовки, способов добывания информации.

Добывание информации технической разведкой осуществляется в результате разведывательного контакта технических средств добывания с носителем информации, который распространяется в пространстве от ее источника. Если носитель информации распространяется за пределы контролируемой зоны, то возможно добывание информации без нарушения границ контролируемой зоны. Границей контролируемой зоны государства является государственная граница, границей контролируемой зоны организации — граница ее территории, которая отображается в общем случае забором. При распространении в пространстве носитель информации теряет энергию и все в большей степени изменяются под действием помех его информационные параметры, содержащие защищаемую информацию. Поэтому добывание информации возможно на таком удалении от источника, при котором обеспечивается допустимое для злоумышленника качество получаемой информации, т. е. выполняется энергетическое условие разведывательного контакта. Чем дальше находится злоумышленник или его техническое средство от контролируемой зоны, тем меньше риск злоумышленника. Поэтому в общем случае контакт их с носителем осуществляется в зоне добывания, в которой качество добываемой информации не ниже допустимой, а риск минимален.

Способы доступа средств технической разведки к носителям без нарушения контролируемой зоны, т. е. с минимальным риском для злоумышленника, предусматривают размещение технических средств в местах вне контролируемых зон с выполнением энергетического условия разведывательного контакта.

В общем случае за пределы контролируемой организации защищаемая информация переносится всеми носителями. Поэтому добывание информа-

ции без нарушения контролируемой зоны непосредственно или с помощью технических средств возможно путем подслушивания, скрытного наблюдения, перехвата сигналов с информацией, взятия проб воздуха, воды, твердых частиц возле территории организации. Если защищаемый источник находится на достаточно большом удалении от забора, то с целью обеспечения энергетического условия разведывательного контакта на территории организации или на ее границе скрытно устанавливают ретрансляторы — закладные устройства.

Добывание информации зарубежной технической разведкой без нарушения государственной границы возможно, учитывая большие расстояния от источников сигналов до границы, для носителей с достаточно высокой энергией или малым затуханием в среде распространения. Такими носителями являются электромагнитные волны в оптическом и радиодиапазонах. Так как в каналах связи используются в основном высокочастотные сигналы, распространяющиеся в пределах прямой видимости, то дальность добывания информации зависит не только от мощности носителя информации и чувствительности приемника, но и высоты размещения средства разведки над земной поверхностью. Комплексы радио- и радиотехнической разведки размещаются на естественных высотах (холмах и горах) вблизи государственной границы. С развитием космической связи, каналы которой используются для обеспечения служебной связи и по которым передается закрытая информация, обеспечивается перехват радиосигналов средствами наземной разведки.

Наряду с наземными и надводными комплексами радио- и радиотехнической разведки широко применяют средства оптической и радиоэлектронной разведки, размещаемые на воздушных и космических аппаратах. В качестве воздушных аппаратов используются пилотируемые и беспилотные самолеты, а также привязные аэростаты. Самолеты барражируют на определенном участке вдоль государственной границы, а аэростаты крепятся в заданных местах с внутренней стороны границы с помощью троса. На платформе аэростата устанавливается малогабаритная приемная аппаратура, сигналы и электрический ток питания средств на платформе передаются по проводам троса.

Существенно большие потенциальные возможности доступа к объектам разведки имеет космическая разведка. Она позволяет приблизить техническое средство добывания информации к любому объекту разведки на территории государства на расстояние 130-150 км и передать добытую информацию (изображения объектов, перехваченные сообщения) через спутники-ретрансляторы в реальном масштабе времени.

Однако космическая разведка по сравнению с другими имеет ряд особенностей, существенно **ограничивающих ее возможности**:

1. Космические аппараты (КА) на низких круговых орбитах имеют высокую скорость движения относительно поверхности Земли (период вращения составляет около 90 минут), в результате чего время видимости объекта с КА составляет до 10 минут. За это короткое время можно получить фотографии объектов разведки, но оно недостаточно для ведения непрерывной радио- и

радиотехнической разведки. С повышением высоты полета КА период его вращения увеличивается вплоть до 24 часов для геостационарных орбит. Но одновременно снижается энергия сигнала, достигающего средства КА.

2. Параметры орбит определяются с высокой точностью, что позволяет рассчитывать время пролета КА над любым защищаемым объектом и обеспечить его временное скрытие.

### 4.5. Показатели эффективности добывания информации

Наиболее общим показателем эффективности разведки, включающей органы управления, добывания и обработки, является степень выполнения поставленных перед нею задач. Для более объективного определения **эффективности** используется группа **общесистемных показателей** количества и качества информации, таких как:

- полнота добываемой информации;
- своевременность добывания информации;
- достоверность информации;
- вероятность обнаружения и распознавания объекта;
- точность измерения демаскирующих признаков;
- затраты на добывание информации.

**Полноту полученной информации** можно оценить отношением числа положительных ответов на тематические вопросы к их общему количеству. Тематический вопрос определяет границы информации, необходимой для ответа на этот вопрос. Очевидно, что тематические вопросы можно детализировать до ответов на них в виде «да-нет»». Чем выше степень детализации тематических вопросов, тем точнее оценка полноты полученной информации. Тематические вопросы имеют иерархическую структуру и определяются в результате структурирования конфиденциальной информации при планировании мероприятий по ее добыванию. Поскольку тематические вопросы имеют различную значимость («вес»), то количественно полноту информации $П_и$ с учетом «веса» тематического вопроса можно приближенно оценить по формуле:

$$П_и = \sum_{i=1}^{n} a_i \beta_i, \quad \sum_{i=1}^{n} a_i = 1,$$

где $a$ — «вес» i-го тематического вопроса; $\beta_i = 1$, когда количество и качество информации соответствуют i-му тематическому вопросу, и равно 0, когда не соответствует.

**Своевременность информации** является важным показателем ее качества, так как она влияет на цену информации. Если добытая информация устарела, то затраты на ее добывание оказались напрасными — она не может быть эффективно использована злоумышленником. Поэтому своевременность следует оценивать относительно продолжительности ее жизненного цикла. Если время устаревания информации существенно больше времени ее использования после добывания, то она своевременная. В противном случае она устаревшая.

**Достоверность информации** — важнейший показатель качества информации. Она искажается в результате дезинформирования и под действием помех. Так как использование ложной (искаженной) информации может нанести в общем случае больший ущерб, чем ее отсутствие, то выявлению достоверности добытой информации ее пользователь уделяет большое внимание.

Для оценки достоверности используют следующие частные показатели:

- достоверность сообщения в смысле отсутствия ложных сведения и данных;
- разборчивость речи;
- вероятность ошибочного или неискаженного приема дискретной единицы (бита, символа, цифры, буквы, слова).

Достоверность информации в смысле отсутствия в ней элементов дезинформации зависит от надежности источника, которая может оцениваться по качественной шкале с уровнями:

- совершенно надежный;
- обычно надежный;
- довольно надежный;
- не всегда надежный;
- ненадежный;
- надежность не может быть определена.

Качество подслушиваемой речи наиболее объективно оценивается показателем, называемым **разборчивостью речи.** В соответствии с лингвистическим делением речи на фразы, слова, слоги и звуки разборчивость делят на **смысловую, слоговую и звуковую (формантную) разборчивость речи.** С точки зрения защиты речевой семантической информации наиболее наглядным является показатель смысловой разборчивости (разборчивости фраз). Однако получение объективных оценок смысловой разборчивости затруднено из-за избыточности речи. Более надежные результаты получаются при определении слоговой или звуковой разборчивости. Поэтому они получили наибольшее распространение.

**Разборчивость речи соответствует выраженной в процентах доли принятых без искажения единиц (фраз, слов, букв, звуков) по отношению к общему количеству переданных.** Избыточность письменной или устной речи снижает требования к значениям разборчивости и обусловлена различными значениями частоты использования в речи букв, а также существенно меньшим количеством разрешенных грамматикой слогов, слов и фраз по отношению к возможным комбинациям слогов, слов и фраз, которые теоретически можно составить из букв алфавита. Достаточно сказать, что в течение 80% времени телефонного разговора абоненты обмениваются лишь 155 разными словами.

Соотношения между качеством речи и количественными значениями слоговой и словесной разборчивости приведены в таблице 4.1.

Таблица.1

| *Понятность речи* | *Разборчивость,%* | |
|---|---|---|
| | *слоговая* | *словесная* |
| Предельно допустимая | 25–40 | 75–87 |
| Удовлетворительная | 40–56 | 87–93 |
| Хорошая | 56–80 | 93–98 |
| Отличная | 80–100 | 98–100 |

Цифровые данные также обладают избыточностью, но в контексте конкретного сообщения. Например, если в газете в июле месяце появляется прогноз погоды в Москве о температуре 0 или 50 градусов, то читатель этому сообщению не поверит и предположит об ошибке при верстке газеты. Однако исправить, т. е. указать точные значения цифр, он не сможет. Поэтому к достоверности передачи цифровых данных предъявляются высокие требования по достоверности передачи: **одна ошибка и менее на миллион цифр**. В ответственных случаях для повышения достоверности цифры пишутся прописью, как, например, принято при оформлении финансовых документов. В этом случае существенно понижается вероятность искажения цифр как под воздействием помех при передаче по каналам связи, так и в результате преступных действий злоумышленников.

**Вероятность обнаружения и распознавания объекта** определяется как мера идентификации текущей признаковой структуры, полученной при наблюдении объекта, с эталонной. Чем больше признаков текущей структуры совпадает с эталонными признаками объекта, и чем больше их информативность, тем выше вероятность обнаружения объекта. При распознавании объектов используется тот же механизм. Для достаточно достоверной оценки величины угроз безопасности информации необходимо определение возможностей и путей попадания информации к злоумышленнику.

# 5. МЕТОДЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

## 5.1. Классификация методов ИТЗИ

Классификация направлений и методов инженерно-технической защиты информации приведена на рис. 5.1 [2].

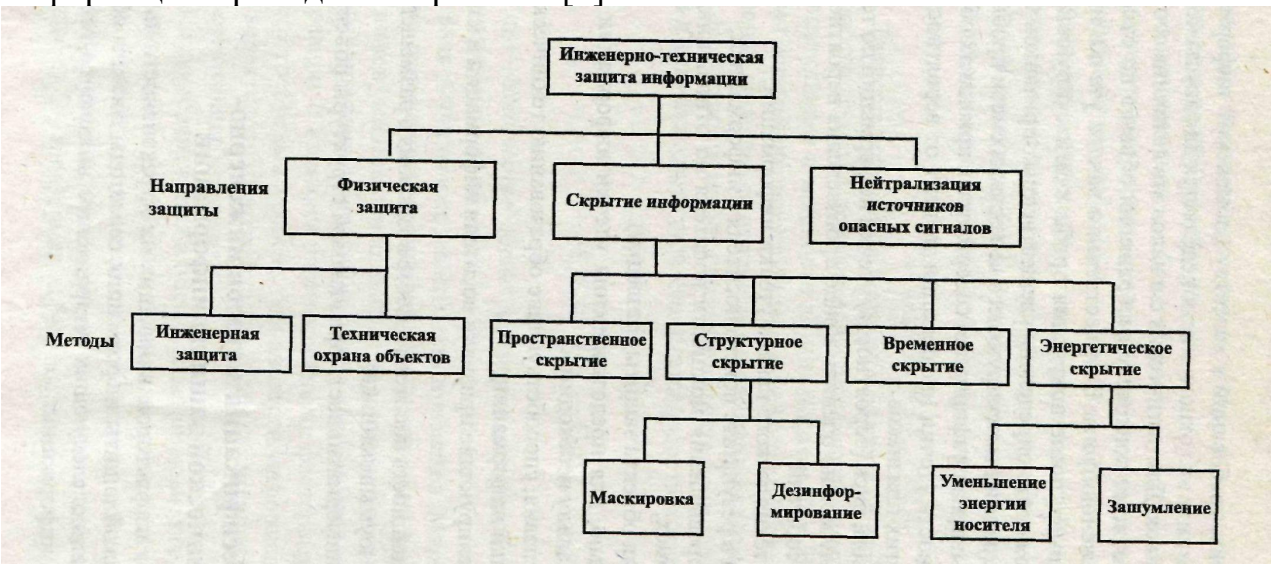



Рис. 5.1. Классификация направлений и методов ИТЗИ

**Физическая защита.** Затруднение движения источников угроз воздействия к источникам информации обеспечивается в рамках направления, называемого физической защитой. **Физическая защита - затруднение движения источников угроз воздействия к источникам информации**. Физическая защита обеспечивается методами **инженерной защиты и технической охраны**. **Инженерная защита** это использование **естественных** и **искусственных преград** на маршрутах возможного распространения источников угроз воздействия. Искусственные преграды создаются с помощью различных инженерных конструкций, основными из которых являются заборы, ворота, двери, стены, межэтажные перекрытия, окна, шкафы, ящики столов, сейфы, хранилища. Так как любые естественные и искусственные преграды могут быть преодолены, то для обеспечения надежной защиты информации, как и иных материальных ценностей, необходимы методы обнаружения вторжений в контролируемые зоны и их нейтрализации. Эти методы называются технической охраной объектов защиты**. Техническая охрана – это методы обнаружения и нейтрализации вторжений в контролируемую зону.**

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 кино пленка, 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 – электромагнитное поле с ин-

формацией нельзя хранить, например, в сейфе. Для защиты информации на таких носителях применяют методы скрытия информации.

**Скрытие информации** (прятанье, утаивание) объединяет группу методов защиты информации, основу которых составляют условия и **действия, затрудняющие поиск и обнаружение объектов защиты**, распознавание и измерение их признаков, снятие с носителей информации с качеством, достаточным для ее использования. Оно предусматривает такие изменения местоположения, времени передачи сообщения или проявления демаскирующих признаков, структуры информации, 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. Скрывать от злоумышленника можно как информацию, так и ее носитель. Различают **пространственное, временное, структурное и энергетическое скрытие.**

**Пространственное скрытие** затрудняет поиск и обнаружение злоумышленником источника информации в пространстве. Оно достигается размещением источника информации в местах, местоположение которых априори злоумышленнику не известно. Такие места хранения называются **тайниками.** Перед злоумышленником возникает дополнительная задача — поиск источника. Чем больше область поиска, тем труднее найти объект. Подводные лодки представляют большую угрозу, прежде всего, потому, что обеспечивается их высокая пространственная скрытность.

Наиболее древним стеганографическим способом скрытия информации является написание сообщения симпатическими (бесцветными без специальной тепловой или химической обработки) чернилами между строк письма или иного документа. Известно много способов записи данных, реализующих пространственное скрытие информации: запись наколом букв на оборотной стороне этикеток флаконов, банок или бутылок, на внутренней стороне спичечной коробки, внутри яйца и др. В годы расцвета фототехники для скрытной передачи сообщений использовалась так называемая «микроточка», изобретенная немецким ученым Э. Голдбергом. «Микроточка» представляла собой микроизображение разведывательного сообщения размером 0,01-1 мм$^2$, которое наклеивалось в качестве точки текста письма, открытки, под марку и иные места безобидной корреспонденции или предметов. Величина уменьшенных символов в «микроточке» достигала 1 микрона. Большие возможности по реализации стеганографических способов скрытия информации предоставляют компьютерные технологии записи информации. Компьютерная стеганография основывается на том, что файлы, содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери качества изображения или звука. Такая возможность обусловлена неспособностью органов чувств человека различать незначительные изменения в цвете изображения или в частотах звука. Поэтому в качестве контейнеров используются графические и звуковые файлы, содержащие оцифрованное изображение и звук. Младшие (1-4) разряды используемых многоразрядных кодов могут быть изменены без ухудшения качества изображения или

звука, в них можно записать секретную и конфиденциальную информацию и обеспечить ее эффективное скрытие. Например, качество эталонного изображения в формате bmp объемом 243 Кбайт незаметно отличается от того же изображения, в файле которого помещена иная информация объемом 119 Кбайт.

Отсутствие у злоумышленника данных о времени передачи сообщения с интересующей информацией или времени проявления демаскирующих признаков объекта защиты вынуждает злоумышленника тратить большие ресурсы на обеспечение непрерывности разведки. Этим достигается **временное скрытие.** Десятки тысяч операторов и технических средств Агентства национальной безопасности США постоянно и непрерывно «слушают» эфир в разных точках пространства в разных частотных диапазонах, чтобы не пропустить и перехватить информативное сообщение в каналах связи своего вероятного противника. Чем короче по времени передаваемое сообщение, тем сложнее его обнаружить. Поэтому одним из методов временного скрытия является передача с большой скоростью сообщения, накопленного за время, значительно превышающее время его передачи.

**Структурное 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.

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.

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.

Структурное скрытие, в результате которого информационный портрет изменяется под информационный портрет фона, называется **маскировкой.** Методы маскировки отличаются для разных видов сообщения. Маскировка семантической информации, представляемой в виде набора определенным образом связанных символов, обеспечивается криптографическими методами и называется **шифрованием.** Фоном для маскируемого сообщения является случайный набор символов. Поэтому чем меньше зашифрованное сообщение отличается от случайного, тем выше уровень скрытия информации.

Маскировка признаковой информации достигается изменением информативных признаков объекта защиты под признаки объектов фона. В зависимости от вида признаковой информации маскируются признаки объектов наблюдения, сигналов или демаскирующих веществ. Фон при наблюдении образуют другие объекты, в том числе предметы местности. Фоном для сигналов являются другие сигналы — помехи.

**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 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.

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.

**Маскировка признаков веществ** обеспечивается преобразованием признаков веществ под признаки других веществ, не интересующих злоумышленника. Например, для контрабанды наркотиков иногда их преобразуют в другое химическое вещество, пропускаемое таможенной службой и восстанавливаемое после провоза до первоначального состава.

Другой метод структурного скрытия заключается в трансформации исходного информационного портрета в новый, соответствующий ложной семантической информации или ложной признаковой структуре, и «навязывании» нового портрета органу разведки (злоумышленнику). Такой метод защи-

ты называется **дезинформированием.** Дезинформирование наиболее эффективно при скрытии семантической информации, когда в добытом сообщении содержится ложная информация. При скрытии признаковой информации граница между маскировкой и дезинформированием размытая. Принципиальное различие между ними состоит в том, что маскировка направлена на затруднение обнаружения объекта защиты среди других объектов фона, а дезинформирование — на создание ложного объекта прикрытия. При поиске орган разведки (злоумышленник) не находит замаскированный объект, при дезинформировании он обнаруживает другой объект вместо истинного, признаки которого невозможно изменить под признаки фона. Например, если в глухом месте без строений размещается шахта стратегической ракеты, то невозможно скрыть подъездные пути автотранспорта к ней. В этом случае структурное скрытие информации о месте нахождения ракетной установки обеспечивается не только маскировкой ее конструкции, но и имитацией функционирования этого объекта.

Дезинформирование осуществляется путем подгонки признаков информационного портрета защищаемого объекта под признаки информационного портрета ложного объекта, соответствующего заранее разработанной версии, — **объекта прикрытия.** 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.

**Основу третьего направления инженерно-технической защиты** информации составляют методы поиска, обнаружения и **нейтрализации источников** опасных сигналов. Так как эти источники обнаруживаются по их демаскирующим признакам, то эти методы содержат процедуры идентификации источников случайных опасных сигналов по их демаскирующим признакам.

## 5.2. Классификация объектов физической защиты

Классификация объектов физической защиты приведена в руководящих документах [5].

Уровень безопасности объекта определяется вероятностью его сохранения от хищения или уничтожения. Степень безопасности объекта зависит от своевременного реагирования технических средств охранной и тревожной сигнализации на возникающую угрозу и от времени преодоления физических барьеров: решеток, замков, задвижек на окнах и дверях, специальным образом укрепленных дверей, стен, полов, потолков и других строительных конструкций, то есть средств инженерно-технической укрепленности на пути возможного движения нарушителя. Чем раньше можно обнаружить возникшую угрозу объекту, тем быстрее ее можно пресечь. Это достигается правильным выбором и применением технических

средств охранной и тревожной сигнализации, их правильным размещением в охраняемых зонах. Средства инженерно-технической укрепленности увеличивают время, необходимое для их преодоления, что создает возможность задержания нарушителя. Особенно это проявляется при сочетании средств инженерно-технической укрепленности и технических средств охранной и тревожной сигнализации. Средства инженерно-технической укрепленности, помимо физического препятствия, выполняют функции психологического барьера, предупреждающего возможность проникновения нарушителя на охраняемый объект.

В зависимости от значимости и концентрации материальных, художественных, исторических, культурных и культовых ценностей, размещенных на объекте, последствий от возможных преступных посягательств на них, все **объекты**, их помещения и территории **подразделяются на две группы** (категории): А и Б. Ввиду большого разнообразия различных по составу объектов в каждой группе они дополнительно подразделяются на две подгруппы каждая: АI и АII, БI и БII.

**Объекты подгрупп АI и АII -** это **объекты особо важные, повышенной опасности и жизнеобеспечения,** противоправные действия (кража, грабеж, разбой, терроризм и т.п.) на которых, в соответствии с законодательством Российской Федерации, могут привести к крупному, особо крупному экономическому или социальному ущербу государству, обществу, предприятию, экологии и т.п.

**Особо важный объект:** объект, значимость которого определяется органами государственной власти Российской Федерации или местного самоуправления в целях определения мер по защите интересов государства, юридических и физических лиц от преступных посягательств и предотвращения ущерба, который может быть нанесен природе и обществу, а также от возникновения чрезвычайной ситуации.

**Объект жизнеобеспечения:** объект, на котором сконцентрирована совокупность жизненно важных материальных и финансовых средств, сгруппированных по функциональному предназначению и используемых для удовлетворения жизненно необходимых потребностей населения (например, в виде продуктов питания, жилья, предметов первой необходимости, а также в медицинском, санитарно-эпидемиологическом, информационном, транспортном, коммунально-бытовом обеспечении и др.).

**Объект повышенной опасности:** объект, на котором используют, производят, перерабатывают, хранят или транспортируют радиоактивные, взрыво- и пожароопасные, опасные химические и биологические вещества, создающие реальную угрозу возникновения чрезвычайной ситуации.

**Объекты подгрупп БI и БII** - это объекты, хищения на которых, в соответствии с законодательством Российской Федерации, могут привести к ущербу в размере до 500 МРОТ и свыше 500 МРОТ соответственно.

**Объекты подгруппы АI:**

объекты особо важные, повышенной опасности и жизнеобеспечения, включенные в перечень объектов, подлежащих государственной охране,

согласно Постановлению Правительства Российской Федерации от 14.08.1992 N 587;

объекты, включенные органами власти субъектов Российской Федерации или местного самоуправления в перечни объектов особо важных, повышенной опасности и жизнеобеспечения;

объекты по производству, хранению и реализации радиоактивных, наркотических веществ, сильнодействующих ядов и химикатов, биологических, токсических и психотропных веществ и препаратов;

ювелирные магазины, базы, склады и объекты, производящие и использующие ювелирные изделия, драгоценные металлы и камни;

объекты кредитно-финансовой системы (банки, операционные кассы вне кассового узла, пункты обмена валюты, банкоматы);

кассы предприятий, организаций, учреждений, головные кассы торговых предприятий;

**Объекты подгруппы АII** (специальные помещения объектов особо важных и повышенной опасности):

хранилища и кладовые денег и валюты, ценных бумаг;

хранилища ювелирных изделий, драгоценных металлов и камней;

хранилища секретной документации;

специальные хранилища взрывчатых, радиоактивных, наркотических, химических, бактериологических, токсичных и психотропных веществ и препаратов;

специальные фондохранилища музеев и библиотек.

**Объекты подгруппы БI:**

объекты хранения или размещения изделий технологического, санитарно-гигиенического и хозяйственного назначения, нормативно-технической документации, инвентаря и т.п.;

объекты мелкооптовой и розничной торговли (павильоны, палатки, ларьки, киоски).

**Объекты подгруппы БII:**

объекты хранения или размещения товаров, предметов повседневного спроса, продуктов питания, компьютерного оборудования, оргтехники, видео- и аудиотехники, кино- и фотоаппаратуры, натуральных и искусственных мехов, кожи, автомобилей и запасных частей к ним, алкогольной продукции с содержанием этилового спирта свыше 13 процентов объема готовой продукции.

Каждой подгруппе объектов соответствует определенный класс (степень) защиты конструктивных элементов (ограждающих конструкций и средств инженерно-технической укрепленности).

Требуемый класс защиты конструктивных элементов для различных подгрупп объектов приведен в таблице 5.1.

Таблица 5.1. Класс защиты конструктивных элементов

| Конструктивный элемент | AII | AI | БII | БI |
|---|---|---|---|---|
| | класс защиты | | | |
| 1. Строительные конструкции | | | | |
| Оболочка кладовой, хранилища | 4 | - | - | - |
| Наружные стены здания первого этажа, а также стены, перекрытия охраняемых помещений, расположенных внутри здания, примыкающие к помещениям других собственников | - | 3 | 2 | 1 |
| Наружные стены охраняемых помещений, расположенных на втором и выше этажах здания, а также стены, перекрытия этих помещений, расположенных внутри здания, не примыкающие к помещениям других собственников | - | 2 | 1 | 1 |
| Внутренние стены, перегородки в пределах каждой подгруппы | 1 | 1 | 1 | 1 |
| 2. Дверные конструкции | | | | |
| Входные двери в здание, выходящие на оживленные улицы и магистрали | - | 3 | 2 | 2 |
| Двери запасных выходов, двери, выходящие на крышу (чердак), здания во дворы, малолюдные переулки | - | 3 | 3 | 2 |
| Входные двери охраняемых помещений | 4 | 3 | 2 | 1 |
| Внутренние двери в помещениях в пределах каждой подгруппы | 1 | 1 | 1 | 1 |
| 3. Оконные конструкции | | | | |
| Оконные проемы первого этажа и подвала здания, выходящие на оживленные улицы и магистрали | - | 3 | 2 | 1 |
| Оконные проемы второго и выше этажа, не примыкающие к пожарным лестницам, балконам, карнизам и т.п. | - | 1 (2 <*>) | 1 | 1 |
| Оконные проемы первого этажа и подвала здания, выходящие во дворы, малолюдные переулки | - | 3 | 3 | 2 |
| Оконные проемы, примыкающие к пожарным лестницам, балконам, карнизам и т.п. | - | 3 | 3 | 2 |
| Оконные проемы помещений охраны | - | 3 (4 <**>) | - | - |
| 4. Запирающие устройства | | | | |
| Запирающие устройства входных и запасных дверей в здание, входных дверей охраняемых помещений, дверей, выходящих на крышу (чердак) здания | 4 | 3 | 2 (3 <**>) | 2 |
| Запирающие устройства внутренних дверей | 1 | 1 | 1 | 1 |
| 5. Периметр | | | | |
| Ограждения | 4 | 3 (4 <**>) | 2 | 1 |
| Ворота | 4 | 3 (4 <**>) | 2 | 1 |

## ХАРАКТЕРИСТИКИ СТРОИТЕЛЬНЫХ КОНСТРУКЦИЙ

**1. Строительная конструкция 1 класса защиты** (минимально необходимая степень защиты объекта от проникновения):

гипсолитовая, гипсобетонная толщиной не менее 75 мм;

щитовая деревянная конструкция толщиной не менее 45 мм;

конструкция из бревен или бруса толщиной 100 мм;

каркасная перегородка толщиной не менее 20 мм с обшивкой металлическими (в том числе профилированными) листами толщиной не менее 0,55 мм;

кирпичная перегородка толщиной 138 мм по СНиП 3.03.01-87;

перегородка из легкого теплоизоляционного бетона толщиной менее 300 мм;

внутренняя стеновая панель толщиной 100 мм по ГОСТ 12504-80;

пустотная железобетонная конструкция толщиной 160 мм по ГОСТ 9561-91;

**2. Строительная конструкция 2 класса защиты (**средняя степень защиты объекта от проникновения):

конструкция из бревен или бруса толщиной не менее 200 мм;

кирпичная стена толщиной 250 мм по СНиП 3.03.01-87;

пустотная железобетонная плита толщиной 220, 260 и 300 мм по ГОСТ 9561-91 из легкого бетона и толщиной 160 мм из тяжелого бетона;

сплошное железобетонное перекрытие толщиной 120, 160 мм по ГОСТ 12767-94 из легкого бетона;

стеновая панель наружная по ГОСТ 11024-84, внутренняя по ГОСТ 12504-80 и блок стеновой по ГОСТ 19010-82 из легкого бетона толщиной от 100 до 300 мм;

стена из монолитного железобетона по СНиП 3.03.01-87, изготовленная из тяжелого бетона, толщиной до 100 мм;

строительная конструкция 1 класса защиты, усиленная стальной сеткой по ГОСТ 23279-85 с толщиной прутка 8 мм и с ячейкой размерами 100 х 100 мм.

**3. Строительная конструкция 3 класса защиты** (высокая степень защиты объекта от проникновения):

кирпичная стена толщиной более 380 мм по СНиП 3.03.01-87;

пустотное железобетонное перекрытие толщиной 220, 260 и 300 мм по ГОСТ 9561-91 из тяжелого бетона;

сплошное железобетонное перекрытие толщиной 120 и 160 мм по ГОСТ 12767-94 из тяжелого бетона;

стеновая панель наружная по ГОСТ 11024-78 и блок стеновой по ГОСТ 19010-82 из легкого бетона толщиной более 300 мм;

стеновая панель наружная по ГОСТ 11024-84, внутренняя по ГОСТ 12504-80, блок стеновой по ГОСТ 19010-82 и стена из монолитного

железобетона по СНиП 3.03.01-87 толщиной от 100 до 300 мм из тяжелого бетона;

строительная конструкция 1 класса защиты, усиленная стальной (сваренной в соединениях) решеткой из прутка толщиной не менее 10 мм с ячейкой не более 150 х 150 мм;

строительная конструкция 2 класса защиты, усиленная стальной сеткой по ГОСТ 23279-85 с толщиной прутка 8 мм и с ячейкой размерами 100 х 100 мм.

**4. Строительная конструкция 4 класса защиты** (специальная степень защиты объекта от проникновения) - конструкция, соответствующая 5-му и выше классу устойчивости к взлому по ГОСТ Р 50862-96.

## ХАРАКТЕРИСТИКИ ДВЕРНОЙ КОНСТРУКЦИИ

**1. Дверная конструкция 1 класса защиты:**

дверь с полотнами из стекла в металлических рамах или без них: стекло обычное марок М4 - М8 по ГОСТ 111-2001, закаленное по ГОСТ 5727-88, армированное по ГОСТ 7481-78, узорчатое по ГОСТ 5533-86, трехслойное ("триплекс") по ГОСТ 5727-88 или защитное класса А1 по ГОСТ Р 51136-98;

дверь деревянная внутренняя со сплошным или мелкопустотным заполнением полотен по ГОСТ 6629-88, ГОСТ 14624-84, ГОСТ 24698-81. Толщина полотна менее 40 мм;

дверь деревянная со стеклянными фрагментами из листового обычного стекла марок М4 - М8 по ГОСТ 111-2001, армированного по ГОСТ 7481-78, узорчатого по ГОСТ 5533-86, тонированного по ОСТ 3-1901-85, безопасного по ГОСТ Р 51136-98. Толщина стекла фрагмента не нормируется;

решетчатая металлическая дверь произвольной конструкции, изготовленная из стальных прутьев сечением не менее 78 кв. мм, образующих ячейку площадью не более 230 кв. см и свариваемых в каждом пересечении.

**2. Дверная конструкция 2 класса защиты:**

дверь, соответствующая категории и классу устойчивости О-II и выше по ГОСТ Р 51242-98;

дверь, соответствующая классу устойчивости IA по ГОСТ Р 51224-98;

дверь деревянная наружная (типа НС по ГОСТ 24698-81) со сплошным заполнением полотен при их толщине не менее 40 мм;

дверь с полотнами из стекла в металлических рамах или без них с использованием защитного остекления класса А2 и выше по ГОСТ Р 51136-98 или обычного стекла, оклеенного защитной пленкой, обеспечивающей класс устойчивости остекления А2 и выше по ГОСТ Р 51136-98;

решетчатая металлическая дверь, изготовленная из стальных прутьев диаметром не менее 16 мм, образующих ячейку не более 150 х 150 мм и свариваемых в каждом пересечении. По периметру решетчатая дверь обрамляется стальным уголком размерами не менее 35 х 35 х 4 мм;

решетчатая раздвижная металлическая дверь, изготовленная из полосы сечением не менее 30 х 4 мм, с ячейкой не более 150 х 150 мм.

**3. Дверная конструкция 3 класса защиты:**

дверь, соответствующая категории и классу устойчивости У-I и выше по ГОСТ Р 51242-98;

дверь, соответствующая классу устойчивости IБ по ГОСТ Р 51224-98;

дверь деревянная со сплошным заполнением полотен толщиной не менее 40 мм, усиленная обивкой с двух сторон листовой сталью толщиной не менее 0,6 мм с загибом листа на внутреннюю поверхность двери или на торец полотна внахлест с креплением по периметру и диагоналям полотна гвоздями диаметром 3 мм и шагом не более 50 мм;

дверь деревянная со сплошным заполнением полотен толщиной не менее 40 мм с дополнительным усилением полотен металлическими накладками;

дверь с полотнами из стекла в металлических рамах или без них с использованием защитного остекления класса БI и выше по ГОСТ Р 51136-98;

дверь металлическая с толщиной наружного и стального внутреннего листа обшивки не менее 2 мм.

**4. Дверная конструкция 4 класса защиты:**

дверь, соответствующая категории и классу устойчивости С-II и выше по ГОСТ Р 51242-98;

дверь кабины защитная по ГОСТ Р 50941-96;

дверь защитная по ГОСТ Р 51072-97;

дверь для хранилища, сейфовой комнаты по ГОСТ Р 50862-96.

## ХАРАКТЕРИСТИКИ ОКОННОЙ КОНСТРУКЦИИ

**1. Оконная конструкция 1 класса защиты** (минимально необходимая степень защиты объекта от проникновения) - окна с обычным стеклом (стекло марки М4 - М8 по ГОСТ 111-2001 толщиной от 2,5 до 8,0 мм).

**2. Оконная конструкция 2 класса** (средняя степень защиты объекта от проникновения):

окно специальной конструкции с защитным остеклением класса А2 и выше по ГОСТ Р 51136-98 или с обычным стеклом, оклеенным защитной пленкой, обеспечивающей класс устойчивости остекления А2 и выше по ГОСТ Р 51136-98;

окно с обычным стеклом, дополнительно защищенное:

- защитными конструкциями, соответствующими категории и классу устойчивости О-II и выше по ГОСТ Р 51242-98;

- деревянными ставнями со сплошным заполнением полотен из досок толщиной не менее 40 мм;

- металлическими решетками произвольной конструкции, изготовленными из стальных прутьев сечением не менее 78 кв. мм, образующих ячейку площадью не более 230 кв. см и свариваемых в каждом пересечении.

**3. Оконная конструкция 3 класса защиты** (высокая степень защиты объекта от проникновения):

окно специальной конструкции с защитным остеклением класса А3 и выше по ГОСТ Р 51136-98;

окно с обычным стеклом, дополнительно защищенное:

- защитными конструкциями, соответствующими категории и классу устойчивости У-I и выше по ГОСТ Р 51242-98;

- защитными конструкциями, соответствующими классу устойчивости IБ по ГОСТ Р 51222-98;

- щитами или деревянными ставнями со сплошным заполнением полотен из досок толщиной не менее 40 мм, обитыми с двух сторон стальными листами толщиной не менее 0,6 мм;

- металлическими решетками, изготовленными из стальных прутьев диаметром не менее 16 мм, образующих ячейки не более 150 х 150 мм, или другими конструкциями соответствующей прочности.

**4. Оконная конструкция 4 класса защиты** (специальная степень защиты объекта от проникновения):

окно с обычным стеклом, дополнительно защищенное защитными конструкциями, соответствующими категории и классу устойчивости С-II и выше по ГОСТ Р 51242-98;

окно специальной конструкции с защитным остеклением класса Б1 и выше по ГОСТ Р 51136-98;

окно с пулестойким стеклом (бронестекло) по ГОСТ Р 51136-98 класса 1 и выше;

остекление кабины защитной - по ГОСТ Р 50941-96.

## ХАРАКТЕРИСТИКИ ОСНОВНОГО ОГРАЖДЕНИЯ

1. **Ограждение 1 класса защиты** (минимально необходимая степень защиты объекта от проникновения) - ограждение из различных некапитальных конструкций высотой не менее 2 м.

2. **Ограждение 2 класса защиты** (средняя степень защиты объекта от проникновения) - ограждение деревянное сплошное толщиной доски не менее 40 мм, металлическое сетчатое или решетчатое высотой не менее 2 м.

3. **Ограждение 3 класса защиты** (высокая степень защиты объекта от проникновения) - ограждение железобетонное толщиной не менее 100 мм, каменное и кирпичное толщиной не менее 250 мм, сплошное металлическое толщиной не менее 2 мм. Высота ограждения не менее 2,5 м.

4. **Ограждение 4 класса защиты** (специальная степень защиты объекта от проникновения) - ограждение монолитное железобетонное толщиной не менее 120 мм, каменное, кирпичное толщиной не менее 380 мм. Высота ограждения не менее 2,5 м с оборудованным дополнительным ограждением.

## ХАРАКТЕРИСТИКИ ВОРОТ

1. **Ворота 1 класса защиты** (минимально необходимая степень защиты объекта от проникновения) - ворота из некапитальных конструкций высотой не менее 2 м.

2. **Ворота 2 класса защиты** (средняя степень защиты объекта от проникновения):

комбинированные, решетчатые или реечные ворота из металлоконструкций, соответствующие категории и классу не ниже О-II по ГОСТ Р 51242-98;

деревянные ворота со сплошным заполнением полотен при их толщине не менее 40 мм;

решетчатые металлические ворота, изготовленные из стальных прутьев диаметром не менее 16 мм, образующих ячейку не более 150 х 150 мм и свариваемых в каждом пересечении.

Высота ворот не менее 2 м.

3. **Ворота 3 класса защиты** (высокая степень защиты объекта от проникновения):

комбинированные или сплошные ворота из металлоконструкций, соответствующие категории и классу не ниже У-1 по ГОСТ Р 51242-98;

ворота деревянные со сплошным заполнением полотен при их толщине не менее 40 мм, обшитые с двух сторон стальным металлическим листом толщиной не менее 0,6 мм;

комбинированные или сплошные ворота из стального листа толщиной не менее 2 мм, усиленные дополнительными ребрами жесткости и обивкой изнутри доской толщиной не менее 40 мм.

Высота ворот не менее 2,5 м.

4**. Ворота 4 класса защиты** (специальная степень защиты объекта от проникновения):

сплошные ворота, соответствующие категории и классу не ниже С-I по ГОСТ Р 51242-98;

сплошные ворота из стального листа толщиной не менее 4 мм, усиленные дополнительными ребрами жесткости.

Высота ворот не менее 2,5 м.

## 5.3. Средства технической охраны объектов

Средства обнаружения злоумышленника составляют основу комплекса охраны источников информации и других ценных объектов, так как от вероятности обнаружения вторжения и оповещения о нем сил нейтрализации зависит эффективность нейтрализации угроз. Основными средствами обнаружения являются [2]:

- извещатели;
- приемно-контрольные приборы;
- пульты централизованной охраны;
- средства телевизионной охраны;
- средства освещения.

**Извещатели.** Разнообразие видов охраняемых зон и их характеристик привело к многообразию видов и типов извещателей. Классификация их дана на рис. 5.2.

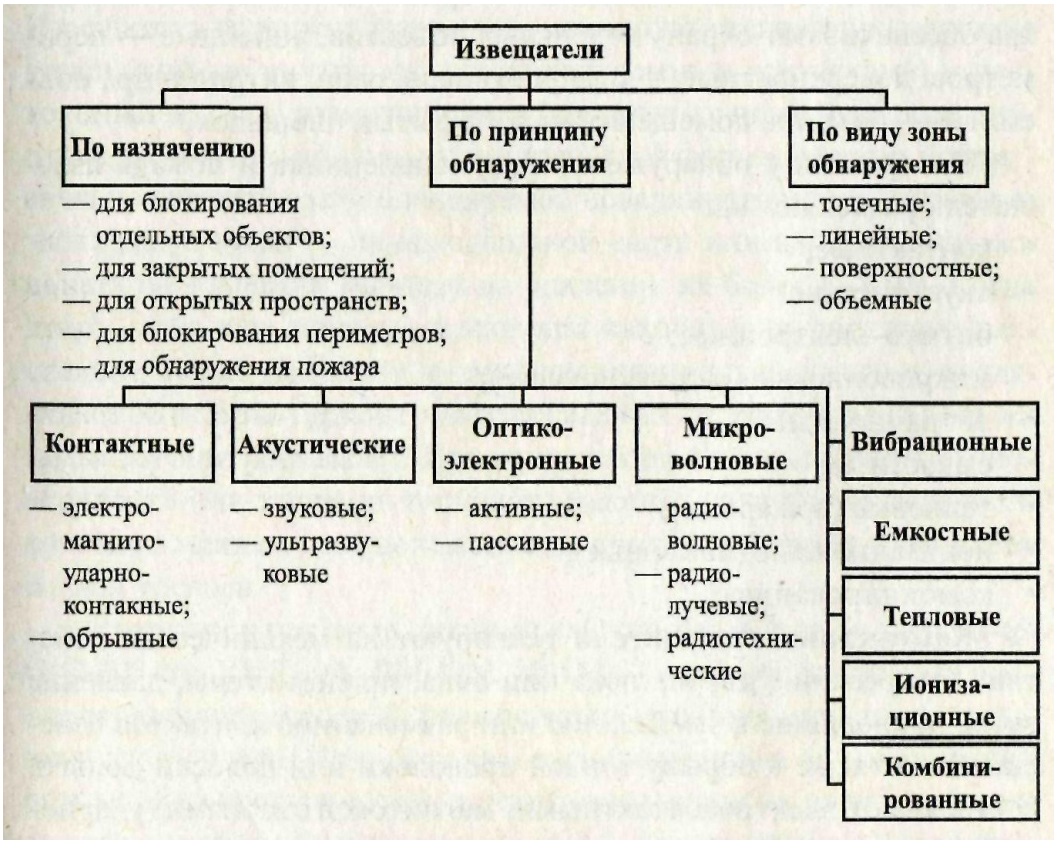



Рис. 5.2. Классификация типов извещателей

**По назначению** извещатели делятся на средства для блокирования отдельных объектов, обнаружения злоумышленника и пожара в закрытых помещениях, обнаружения нарушителя на открытых площадках и блокирования периметров территории, здания, коридора. Такое деление обусловлено особенностями указанных зон и требованиями к средствам обнаружения в этих зонах. Средства охраны помещений и открытых площадок должны обнаруживать злоумышленника в любой точке этих зон, периметровые — при пересечении им периметра зоны. К средствам для охраны закрытых помещений предъявляются менее жесткие требования по устойчивости средств к климатическим воздействиям, но ограждения помещения вызывают многочисленные переотражения излучаемых извещателями полей, и эти особенности необходимо учитывать при создании и грамотной эксплуатации соответствующих средств.

**По виду охраняемой зоны** средства обнаружения делятся на точечные, линейные, объемные и поверхностные. Точечные средства обеспечивают охрану отдельных объектов, линейные — периметров, поверхностные — стен, потолков, окон, витрин и др., объемные — объемов помещений или открытых площадок.

**По принципу обнаружения** злоумышленника и пожара извещатели разделяют на:

- контактные;
- акустические;
- оптикоэлектронные;
- микроволновые (радиоволновые);
- вибрационные;
- емкостные;
- тепловые (пожарные);
- ионизационные (пожарные);
- комбинированные.

**Контактные извещатели** реагируют на механические действия (открывание двери, люка или окна, пролом стены, давление веса), приводящие к замыканию или размыканию контактов извещателя, а также к обрыву тонкой проволоки или полоски фольги. Они бывают электроконтактными, магнитоконтактными, ударноконтактными и обрывными.

**Электроконтактные извещатели** представляют собой выключатели, которые под действием механической силы (при открытии злоумышленником двери, оконной рамы, форточки, шкафа и др.) размыкают или замыкают электрические цепи, соединяющие извещатели с приемно-контрольным прибором. Электроконтактые извещатели могут быть закамуфлированы под коврик перед дверью. Под тяжестью злоумышленника листы замыкаются через отверстия в диэлектрике, что приводит к возникновению сигналов тревоги.

**Магнитоконтактные извещатели** предназначены для блокирования открывающихся поверхностей (дверей, окон, люков и др.), а также переносимых предметов (экспонатов музеев и выставок). Извещатель содержит геркон (герметичную стеклянную трубку с укрепленными внутри магнитоуправляемыми контактами) и постоянный магнит, размещенных в одинаковых пластмассовых корпусах прямоугольной или цилиндрической формы. Магнит крепится на подвижной части блокируемой поверхности или на музейном экспонате, геркон — на неподвижной части или на подставке экспоната параллельно магниту на удалении не более 6-8 мм. Когда дверь, окно, люк закрыты, а экспонат находится на подставке, расстояние между магнитом и герконом минимальное, магнит притягивает контакты геркона и в зависимости от типа извещателя их замыкает или размыкает. Возникает сигнал тревоги.

**Ударноконтактные датчики** обеспечивают блокирование поверхностей, прежде всего, оконных стекол, разрушающихся от удара. Принципы работы основаны на замыкании или размыкании электрических контактов во время их колебаний после удара по стеклу, к которому приклеен корпус датчика. Один контакт извещателя прикреплен к его корпусу, на конце другого, упругого контакта укреплен массивный груз. В силу инерционности этого груза гибкий контакт при колебаниях корпуса практически не изменяет своего положения, в результате чего он замыкается или размыкается с движущимся вместе с корпусом другим контактом.

Основу **обрывных извещателей** составляют тонкий провод, алюминиевая фольга и токопроводящий слой стекла или пленки. Провода диаметром 0,1-0,25 мм применяются для блокировки деревянных и прочих некапиталь-

ных конструкций помещения, решеток окон, небольших временных стоянок. Провод прокладывается по всей внутренней блокируемой поверхности параллельными рядами с расстоянием между рядами проволоки не более 200 мм, заделывается внутрь или вокруг стержней решеток окон, навешивается на кусты и деревья на высоте около 1 м вокруг охраняемой стоянки. Провод, уложенный на поверхности, маскируют шпаклевкой с последующим окрашиванием или покрывают листовым материалом (оргалитом, фанерой и др.).

Обрывные извещатели имеют высокую помехоустойчивость и широко применяются для блокирования поверхностей (на пролом и стекла на разбивание) и периметров.

**Акустические извещатели** для обнаружения злоумышленника используют акустические волны в звуковом и ультразвуковом диапазонах, которые возникают при разрушении им механических преград или отражаются от нарушителя при проникновении его в охраняемое помещение. Акустические извещатели, реагирующие на акустические сигналы при разрушении злоумышленником блокируемой поверхности, являются пассивными, ультразвуковые извещатели излучают акустические волны и являются активными.

Ультразвуковые датчики (ДУЗ-4, ДУЗ-4М, ДУЗ-5, ДУЗ-12, «Фикус-МП-2», «Эхо-2», «Эхо-3» и др.) генерируют сигнал тревоги при появлении злоумышленника в контролируемой зоне охраняемого помещения. Извещатель содержит излучатель акустической волны в ультразвуковом диапазоне, приемник (акустоэлектрический преобразователь) и электронный блок обработки. Излучатель посылает в охраняемое помещение акустическую волну с частотой выше 23 кГц. В результате интерференции прямых и отраженных волн в помещении возникают «стоячие» волны. При появлении в помещении человека, а также пламени пожара изменяется конфигурация отражающих поверхностей и характер «стоячих волн», а следовательно, изменяется уровень акустического сигнала на входе приемника, что приводит к появлению сигналов тревоги на выходе электронного блока.

В **оптикоэлектронных извещателях** для обнаружения злоумышленника и пожара используются инфракрасные лучи. По принципу действия такие извещатели делятся на активные и пассивные. Активные инфракрасные излучатели состоят из одной или нескольких пар излучателя ИК-лучей и фотоприемника. Сигнал тревоги формируется при пересечении ИК-луча злоумышленником.

Излучатель активного оптикоэлектронного извещателя создает узкий луч света в ИК-диапазоне, который в дежурном режиме освещает его фотоприемник. При пересечении луча злоумышленником или появлении на пути его распространения дыма уровень сигнала на выходе фотоприемника резко уменьшается, что приводит к формированию сигнала тревоги.

Так как излучатели создают узкие лучи в ИК-диапазоне, то активные оптикоэлектронные излучатели используются в основном для блокирования длинных поверхностей – коридоров, стен, заборов, периметров территории и зданий, т. е. выполняют функции линейных извещателей. С целью повышения надежности блокирования создают несколько параллельных лучей с по-

мощью средств, в комплект которых входит соответствующее количество пар излучатель-фотоприемник.

Оптикоэлектронные извещатели используются также для обнаружения пожара, сопровождаемого обильным образованием дыма. Дым может ослабить луч извещателей, применяемых для блокирования поверхностей до уровня, при котором происходит формирование сигнала тревоги. Специальные пожарные извещатели постоянно контролируют оптическую плотность воздуха возле потолка помещения. Пожарный извещатель имеет полость, в которой установлены излучающий светодиод и фотодиод приемника. При попадании внутрь оптической камеры частиц дыма рассеянный ими ИК-свет освещает фотодиод. Срабатывание извещателей с выдачей сигнала «Пожар» происходит при задымлении среды, снижающей ее прозрачность на 0,05-0,2 дБ/м.

Пассивные оптикоэлектронные извещатели формируют сигнал тревоги при попадании на вход термочувствительного элемента ИК-излучения от злоумышленника или от очага пожара. Эффективность работы пассивного извещателя тем выше, чем больше разность между температурой источника тепла и температурой фона. При разнице менее (2-3)° С извещатель «слепнет», т. е. электрический сигнал в блоке обработки, соответствующий тепловому излучению злоумышленника или пожара, не отличается от помех.

Так как пассивные оптикоэлектронные извещатели чувствительны к любым ИК-излучениям, в том числе батарей отопления, кондиционеров, к солнечным лучам, то с целью снижения вероятности ложной тревоги в извещателях сигнал тревоги формируется при последовательном пересечении источником ИК-излучений чувствительных зон. С учетом этого извещатель нужно устанавливать в помещении таким образом, чтобы исключалось движение злоумышленника к объекту защиты в створе луча.

**Микроволновые (радиоволновые) извещатели** используют для обнаружения злоумышленников электромагнитные волны в СВЧ диапазоне (9-30 ГГц). Они содержат СВЧ генератор, приемник и передающие и приемные антенны. Так как на электромагнитное поле в СВЧ диапазоне не влияют акустические помехи, свет и в существенно меньшей степени атмосферные осадки, то эти извещатели все более широко применяются для охраны помещений, открытых пространств и периметров.

В зависимости от вида электромагнитного поля микроволновые излучатели делятся на **радиолучевые, радиоволновые** и **радиотехнические.**

В **радиолучевых** извещателях для блокирования периметров («Радий-1», «Пион-Т (ТМ)», «Риф-РЛ», «Гарус», «Лена-2», «Протва», «Витим») антенна излучателя формирует узкую диаграмму направленности в виде вытянутого эллипсоида с высотой и шириной в середине зоны обнаружения 2…10 м. Длина одного участка обнаружения достигает 300 м. При пересечении человеком электромагнитного луча, излучаемого передающим устройством в сторону приемника, уменьшается, из-за экранирующих свойств человека, напряженность поля в точке приема, в результате чего возникает сигнал тревоги.

**Радиоволновые** объемные извещатели формируют объемную зону обнаружения, заполняющую электромагнитным полем весь объем помещения. Для снижения мощности излучения, что важно для безопасности обслуживающего персонала и повышения помехоустойчивости, в современных извещателях предусматривается импульсный режим работы. Кроме того, для уменьшения ложных тревог в схеме объемных извещателей реализуется принцип селекции на основе эффекта Доплера.

**Радиотехнические** извещатели обнаруживают злоумышленника по изменениям им характеристик СВЧ поля. Электромагнитное поле создается одним или несколькими СВЧ передатчиками. В качестве передающий антенны применяется специальный радиочастотный кабель, прокладываемый вдоль периметра охраняемой территории. Антенна приемника размещается в центре территории или в виде кабеля, параллельного передающему. При вторжении злоумышленника в чувствительную зону извещателя характеристики сигнала на входе приемника изменяются, что вызывает сигнал тревоги.

В извещателе «Бином» (Россия) и «S-Trax» электромагнитное поле создается между двумя параллельно проложенными коаксиальными кабелями с отверстиями. Кабели укладываются по периметру блокируемой территории в землю на глубине 10…15 см и на расстоянии 2…3 метров друг от друга. Из отверстий кабеля, подключенного к генератору, «вытекает» электромагнитное поле и «втекает» в отверстия кабеля, подключенного к приемнику. Кабели этих извещателей создают зону обнаружения шириной до 10 м и высотой и глубиной около 70 см. Закапывание кабелей в землю позволяет применять этот извещатель для обнаружения подкопа, обеспечивает его хорошую маскировку, высокую помехоустойчивость от транспорта, однако на чувствительность этого извещателя влияет электропроводность грунта.

К **вибрационным** относятся извещатели, обнаруживающие злоумышленника по создаваемой им вибрации в грунте при движении, в легком заборе (типа сетки «рабица») при попытке преодоления его нарушителем, при открывании дверей, окон, люков и др. конструкций. Вибрационные извещатели отличаются от акустических инфразвуковым диапазоном воспринимаемых ими частот колебаний блокируемой поверхности. В зависимости от физической природы преобразования механического давления в электрический сигнал вибрационные извещатели бывают электретные, магнитные, волоконно-оптические, трибоэлектрические. Если датчики извещателя размещаются в грунте, то вибрационные извещатели называют также сейсмическими.

**Емкостные** извещатели («Ромб-К4», «Пик», «Барьер-М», «Риф», «Градиент» и др.) создают сигналы тревоги при приближении злоумышленника к объекту охраны. С точки зрения радиотехники движение злоумышленника можно представить как приближение токопроводящей поверхности достаточно большой площади, являющейся моделью злоумышленника, к токопроводящей поверхности антенны емкостного извещателя, размещенной на объекте охраны. В качестве антенны может быть использована токопроводящая поверхность охраняемого объекта (например, сейфа) или электрический провод, укрепляемый в оконных или дверных

проемах, шкафах, на стенах складов и т. д. Между человеком и антенной существует распределенная емкость, величина которой обратно пропорциональна расстоянию между ними. Принцип работы емкостных извещателей состоит в изменении эквивалентной (собственно контура и распределенной) емкости контура генератора сигналов извещателя, вызванной увеличением распределенной емкости между приближающимся нарушителем и антенной извещателя. Изменение емкости приводит к изменению частоты генератора и уменьшению амплитуды связанного с ним контура, настроенного на частоту генератора при отсутствии вблизи антенны человека. Несовпадение частот в контурах приводит к снижению амплитуды колебаний во втором контуре, уменьшение которой менее порога вызывает сигнал тревоги. Чувствительность емкостных датчиков оценивается максимальным расстоянием приближения к антенне, которое составляет 10… 30 см.

Для **обнаружения пожара** применяются извещатели, реагирующие на демаскирующие признаки пожара – повышенную концентрацию дыма в воздухе, высокую температуру и излучения открытого пламени. В различных условиях эти демаскирующие признаки имеют разную информативность.

На повышение температуры в помещении реагируют **тепловые извещатели.** Тепловые извещатели применяют в помещениях, в которых при возгорании быстро повышается температура воздуха. Тепловые извещатели делят на максимальные и дифференциальные.

**Максимальные** подают сигнал тревоги при превышении значения температуры воздуха температуры срабатывания извещателя.

В качестве чувствительных к температуре элементов в них применяются:

- терморезисторы, уменьшающие свое сопротивление при повышении температуры;
- термобиметаллические пластины с разными коэффициентами теплового расширения, изгибаемые и размыкающие электрические контакты при повышении температуры;
- легкоплавкие сплавы (Вуда с температурой плавления 60,5°С, д'Арсе — 79°С), замыкающие при нормальной температуре контакты извещателя;
- термоферриты с уменьшающейся с повышением температуры магнитной проницаемостью и используемые в качестве сердечников электромагнитных реле, которые размыкают контакты при снижении магнитного поля менее уровня срабатывания реле.

В извещателях с терморезисторами уменьшение сопротивления приводит к увеличению силы протекающего через них тока. При превышении его значения заданного (эталонного) возникает сигнал тревоги. Изменяя эталонное значение силы тока, можно настроить извещатель на требуемую максимально допустимую температуру.

Максимальные тепловые извещатели имеют достаточно большую инерционность (30-90 с), обусловленную временем нагревания чувствительного элемента до температуры срабатывания.

Меньшую инерционность и большую устойчивость к изменениям внешней среды имеют **дифференциальные тепловые извещатели**. Дифференциальный извещатель содержит два чувствительных элемента, один из которых (внешний) контактирует с воздухом среды, а другой — внутренний, размещен внутри корпуса извещателя и непосредственного контакта с окружающей средой не имеет. Сигналы с каждого из чувствительных элементов подаются на входы дифференциального усилителя. Сигнал на выходе этого усилителя пропорционален разности входных сигналов. Когда температура обоих чувствительных элементов одинакова, то сигнал на выходе усилителя близок к нулю. Медленное повышение температуры воздуха в помещении из-за, например, жаркой погоды не изменяет уровень сигнала на выходе дифференциального усилителя. При быстром изменении температуры воздуха нагревание чувствительных элементов происходит с разной скоростью. В результате этого входные сигналы отличаются по величине, уровень сигнала на выходе усилителя увеличивается, что приводит к формированию сигнала тревоги.

Так как дым является наиболее информативным признаком пожара и, что особенно важно, на начальном этапе возгорания, когда нет еще открытого пламени, то наиболее широко применяются пожарные извещатели, реагирующие на дым. По принципам работы различают оптические и ионизационные извещатели.

В **оптическом извещателе** измерительная камера с отверстиями для поступления воздуха содержит ИК-излучатель (светодиод) и фотоприемник (фотодиод), расположенные друг против друга. При отсутствии в воздухе дыма свет от излучателя попадает на фотоприемник почти без затухания. При задымленности воздуха световой поток на элементе фотоприемника уменьшается, сигнал на его выходе снижается до порогового значения.

В **ионизационных извещателях** вместо света используется поток радиоактивного слабого излучения частиц плутония-239 со сверхнизкой излучающей активностью 10 мкКю и америций-241 с активностью 0,8-0,9 мкКю. Поток радиоактивных излучений направляется в 2 камеры. В измерительную камеру проходит окружающий воздух, а контрольная камера изолирована от воздуха. При отсутствии дыма в измерительной камере разность сигналов на выходах детекторов мала. В случае появления дыма в ней интенсивность потока снижается, разность уровней сигналов детекторов возрастает, возникает сигнал тревоги. Ионизационные извещатели относятся к наиболее надежным пожарным датчикам, их конструкция обеспечивает полную радиационную безопасность. Но их не рекомендуется устанавливать в детских учреждения, школах, жилых помещениях и других местах, где они могут быть изъяты и разобраны детьми или чрезмерно любопытными взрослыми.

Указанные извещатели являются точечными и используются в основном для помещений типовой конфигурации. Для обнаружения возгораний в длинных и узких помещениях или конструкциях (кабельных каналах, транспортных депо, химических реакторах и др.) применяют линейные тепловые извещатели и традиционные периметровые инфракрасные извещатели.

Линейный тепловой извещатель представляет собой кабель, содержащий 4 медных проводника, каждый из которых покрыт оболочкой из материала с отрицательным температурным коэффициентом. Оболочки проводников в кабеле плотно прижаты друг к другу. Концы проводников попарно соединены друг с другом, образуя две петли. Сопротивление между петлями зависит от сопротивления оболочек, значение которой изменяется при изменении их температуры. Блок обработки линейного теплового извещателя формирует сигнал тревоги при снижении этого сопротивления менее заданного значения.

Периметровые инфракрасные извещатели реагируют на повышение величины затухания среды за счет ее задымленности так же, как реагируют они на пересечение луча злоумышленником.

**Приемно-контрольные приборы (ПКП)** обеспечивают:

- одновременный прием сигналов тревоги от извещателей с подачей световой и звуковой сигнализации;
- передачу сигналов тревоги на пульт централизованного наблюдения;
- возможность увеличения емкости за счет добавления к базовому составу линейных блоков;
- автоматический переход на резервное автономное питание в случае выключения основного;
- формирование сигналов оповещения операторов в случае обрыва или короткого замыкания шлейфов.

ПКП классифицируются по информационной емкости (количеству подключаемых шлейфов) и информативности (количеству видов извещателей). По информационной емкости они бывают малой емкости (до 5 шлейфов), средней (6-50 шлейфов) и большой емкости (свыше 50 шлейфов). ПКП малой информативности обеспечивают работу до 2 видов извещателей, средней — от 3 до 5 видов извещателей. Преимущественно они используются для охраны одного объекта.

При создании ПКП проявляется тенденция расширения на базе микропроцессоров их функциональных возможностей в части автоматизации контроля за состоянием извещателей, адаптации к их различным характеристикам, совершенствования алгоритмов обработки.

Например, в ПКП «Буг» предусмотрена возможность программирования параметров прибора с учетом особенностей подключаемых шлейфов, мажоритарная обработка сигналов, защита от попыток несанкционированного доступа к его элементам и повреждения линий связи.

В современных ПКП средней и большой емкости предусматривается возможность передачи извещений на пульты централизованного наблюдения по отдельному каналу связи.

**Пульты централизованной охраны** предназначены для централизованного приема, обработки и индикации информации с объектов охраны. Они обеспечивают:

- контроль состояния охраняемого объекта;

- взятия объекта под охрану и снятие с охраны;
- автоматическое переключение аппаратуры АТС на средства охраны;
- регистрацию нарушения шлейфов охраняемых объектов с указанием номера объекта и характера нарушения;
- световую индикацию номеров объекта, где произошло нарушение.

Состояние объекта охраны определяется по типу передаваемого от него извещения и по признакам состояния («норма», «замыкание», «обрыв») абонентской линии между объектом и пунктом централизованной охраны. Короткое замыкание или обрыв вызывают изменения тока в линии, в результате чего выдается сигнал тревоги со звуковой сигнализацией и световой индикацией номера объекта.

Для **передачи извещений и команд управления** на пульт централизованного наблюдения используются линии телефонной связи, специальные проводные линии, радиоканалы, комбинированные линии связи.

Передача извещений по телефонным линиям связи производится в комплексах «Центр-КМ», «Нева-10»», «Нева-10М», «Прогресс-ТС», «Атлас-2М», «Фобос» и др., обеспечивающих обслуживание от 30 до 400 и более охраняемых объектов.

Для централизованной охраны не телефонизированных объектов применяются радиосистемы передачи извещений «Струна-2» и «Струна-3». Они состоят из пульта централизованного наблюдения с приемником и объектовых блоков с передатчиками в диапазоне частот 166,7…166,95 МГц. По радиоканалу передается 8 видов извещений: «снят», «взят», «проникновение-вход», «проникновение-периметр», «пожар», «вызов», «авария». Радиосистема «Струна-2» предназначена для охраны до 7 пространственно разнесенных объектов, удаленных от пункта охраны до 3 км, а «Струна-3» — до 160 объектов на удалении до 3 и 6 км (при использовании направленных передающих и приемных антенн).

В автоматической системе тревожной сигнализации по линиям городской телефонной сети «Циклон» автоматизируются процессы взятия под охрану и снятия с охраны. Вся тревожная и служебная информация (время, номер объекта, вид извещения) автоматически фиксируется. В системе предусмотрена работа с 4 АТС и обслуживание до 1000 номеров.

**Средства телевизионной охраны**

Основными средствами телевизионной охраны являются **телевизионные камеры** и **мониторы.**

Обычное разрешение аналоговых **телевизионных камер** для видеоконтроля составляет для черно-белых 380-450 ТВЛ и цветных меньше — 300-320 ТВЛ, в системах высокого разрешения применяют камеры с повышенной четкостью, равной 500-600 и 375— 450 линиям соответственно. Для обычного формата кадра (размеров по вертикали и горизонтали) 3/4 изображение при разрешении 400 ТВЛ состоит из 1200000 пикселей.

Спектральная характеристика ПЗС матриц по сравнению с характеристикой глаза сдвинута в сторону более длинных лучей и захватывает инфракрас-

ную область. Поэтому при инфракрасной подсветке возможно видеонаблюдение, незаметное для злоумышленника. Эта особенность телевизионных камер на ПЗС камерах используется для создания ловушек злоумышленнику, который, выбирая для движения темные места, попадает в зону видеонаблюдения.

Камеры обычной чувствительности позволяют наблюдать в сумерках, при освещенности 0,1-0,5 лк для черно-белых камер и 1-3 лк для цветных камер, а камеры высокой чувствительности — в условиях лунной ночи (порядка 0,01 лк).

Для обеспечения приемлемого качества изображения в широком диапазоне освещенности объекта, в том числе мерцающем свете газоразрядных ламп, телевизионные камеры системы видеонаблюдения оснащаются дополнительными устройствами: электронным затвором, автоматической диафрагмой (автоирисом), автоматической регулировкой усиления сигналов ПЗС-матрицы, гамма-коррекции, компенсации засветки и внешней синхронизации.

По конструктивному признаку телевизионные камеры делятся на **корпусные и бескорпусные.** Бескорпусные телевизионные камеры имеют малые габариты и устанавливаются в различных бытовых предметах для скрытого наблюдения. Камеры для открытого наблюдения размещаются в защитных кожухах. Кожухи камер, устанавливаемых в отапливаемых помещениях, имеют разнообразную конструкцию, обеспечивающую установку на стене, в углу помещения или на потолке. Защитные свойства кожухов классифицируются в соответствий с международным стандартом двухразрядным номером. Первая цифра в интервале 0-6 указывает на степень защиты кожуха от проникновения посторонних предметов (твердых тел диаметром от 1 мм до 50 мм, песка, пыли), вторая (в интервале 0-8) — от проникновения воды. Кожухи камер, применяемые на открытом воздухе, имеют прочный («вандалоустойчивый») корпус и устойчивое к удару стекло окошка перед объективом. Шлицы винтов на кожухе имеют нестандартную форму или спиливаются. Для работы в широком диапазоне климатических условий они герметизируются, на них укрепляется солнцезащитный козырек, в них оборудуется подогрев. Некоторые кожухи имеют дополнительное оборудование — вентиляторы, дворники, омыватели стекла. Кожухи наружного наблюдения для исключения возможности изменения злоумышленником ориентации камеры жестко закрепляются на стенах, столбах и других конструкциях по возможности на большой высоте (4-5 м).

Для осмотра пространства территории или помещения с помощью средне- и длиннофокусных объективов телевизионные камеры устанавливаются на дистанционно управляемых поворотных платформах с углом поворота в горизонтальной плоскости до 350 градусов и до 180 градусов в вертикальной плоскости. Если в процессе наблюдения наряду с получением панорамных изображений требуется рассматривать детали объектов наблюдения, то используются объективы с переменным фокусным расстоянием, управляемые с пульта оператором.

**Мониторы,** так же как и телекамеры, делятся на черно-белые и цветные. Они имеют размер экрана 7, 9, 12, 14, 15, 17, 21 дюйм и разрешающую

способность выше разрешающей способности телевизионных камер. При использовании в системе видеоконтроля обычных черно-белых камер используют мониторы с разрешением 500-800 ТВЛ, для цветных — 300-400 ТВЛ. В системах высокого разрешения применяют черно-белые мониторы с разрешением 900-1000 ТВЛ, цветные — 450-500 ТВЛ.

Основным элементом монитора, определяющим его размеры, разрешающую способность, цветовую гамму, яркость и контраст изображения, является электронно-лучевая трубка (кинескоп), жидкокристаллическая или плазменная панели.

По мере увеличения количества установленных телевизионных камер возникает необходимость в повышении числа мониторов. Однако при установке на рабочем месте охранника более 4-6 мониторов у него во время наблюдения быстро наступает психологическая усталость, особенно при использовании мониторов **с** электронно-лучевыми трубками. Так как дрожание изображения на них становится особенно заметным в периферической области зрения, то при увеличении количества мониторов возрастает вредное влияние дрожания изображения на зрение. Поэтому для охранного телевидения предпочтительными являются более дорогие мониторы с частотой кадровой развертки в 100 Гц.

С целью снижения нагрузки на оператора и повышения эффективности видеоконтроля применяют **видеокоммутаторы, видеоквадраторы, мультиплексоры, детекторы движения, специальные видеомагнитофоны** и так называемые видеоменеджеры на базе компьютеров.

Современные **видеокоммутаторы** делятся на коммутаторы последовательного действия и матричные видеокоммутаторы.

Видеокоммутаторы последовательного действия подключают несколько (4-20) телекамер к одному монитору с последовательным автоматическим «листающим» и ручным режимами работы, позволяющие просматривать изображения всех камер или выборочно от некоторых из них. В современных коммутаторах предусматриваются: регулировка времени просмотра изображения каждой камеры; входы для сигналов тревоги от извещателей для быстрого подключения к монитору сигналов от ближайшей к извещателю камеры; «залповый» режим, который позволяет наблюдать участки охраняемой зоны, на каждом из которых устанавливаются нескольких камер.

Матричные видеокоммутаторы имеют встроенный процессор и обеспечивают дополнительно к функциям последовательных видеокоммутаторов вывод на экран монитора: изображений от камер в любом порядке с управлением их поворотными устройствами и вариообъективами, номеров камер и названий помещений, в которых они установлены, сообщений о сигналах тревоги, текущего времени, даты, инструкции оператору и др. Указанные функции позволяют создавать гибкие и наращиваемые системы охраны объектов защиты.

**Видеоквадраторы (разделители экранов)** уменьшают количество используемых мониторов путем одновременного показа на одном экране монитора нескольких изображений (4 и более). При этом экран делится на части

по количеству телекамер. Различают видеоквадраторы «реального времени», обеспечивающие смену изображений одновременно на всех квадратах экрана монитора, и видеоквадраторы последовательного типа с последовательным переключением изображений в квадратах. Квадраторы имеют также дополнительные (по количеству камер) тревожные входы для подключения средств сигнализации, обеспечивают вывод на полный экран изображения от соответствующей камеры, остановку кадра, передачу сигналов тревоги на другие средства и запись на видеомагнитофон.

**Видеомультиплексоры** — устройства, выполняющие временное мультиплексирование, первоначально создавались для обеспечения записи видеосигналов от нескольких (до 16) камер на одну видеокассету и непрерывное воспроизведение видеосигналов одной камеры. Современные дуплексные и триплексные мультиплексоры обладают широкими функциональными возможностями, в том числе позволяют просматривать на экране мониторов изображения от одних камер и записывать на видеомагнитофон сигналы от других камер. Записанные изображения могут просматриваться в полноэкранном формате, режимах квадрированного экрана, «картинки в картинке» и мультиэкрана. Многие мультиплексоры имеют дополнительные функции, в том числе: двукратного увеличения воспроизводимого изображения и просмотра, ранее сделанных записей одновременно с текущей записью изображений с работающих камер, встроенные детекторы движения, генераторы титров, даты и времени. Широкий набор встроенных функций и возможность программирования микропроцессора с помощью функциональных клавиш или клавиатуры персонального компьютера позволяют использовать мультиплексор как устройство управления до 256 камер системы видеоконтроля.

**Видеодетектор движения** представляет собой автономный или встроенный в мультиплексор электронный блок, который запоминает текущий кадр изображения, сравнивает его с последующим и выдает сигнал тревоги при несовпадении сравниваемых изображений. Различают аналоговые и цифровые детекторы движения. В аналоговых детекторах сравниваются уровни сигналов одинаковых элементов изображения. При попадании в зону наблюдения объекта, отсутствующего на предыдущем изображении, изменяются соответствующие яркости элементов его изображения и уровни сигналов. Если эти изменения превышают установленный порог, детектор движения выдает сигнал тревоги. Введение порога снижает вероятность ложных тревог из-за электрических помех или природных явлений в зоне наблюдения (дождя, снега и др.). Сигнал тревоги подается при превышении этой разности более порогового значения.

В цифровых извещателях создаются предпосылки для существенного повышения помехоустойчивости путем введения в память микропроцессора участков изображения, изменения в которых вызывают сигнал тревоги. Для этого поле изображения разделяется на большое количество ячеек, из которых составляют участки сравнения произвольной конфигурации. В эти участки не включаются, например, качающиеся ветви деревьев, пол, помеще-

ния, по которому могут пробегать грызуны и другие объекты, не связанные со злоумышленником или его действиями. В ряде видеодетекторов можно задавать программным путем также характеристики прогнозируемого движения злоумышленника: начало, направление и скорость движения человека, время суток и др. Например, все входящие в помещение люди вызывают сигнал тревог, а выходящие — нет. Видеодетектор в виде автономного блока может быть сопряжен с любым средством системы видеоконтроля.

Для регистрации и документирования изображений видеокамер применяются **специализированные видеомагнитофоны,** которые в отличие от бытовых обеспечивают существенно большую длительность записи: от 24 часов до 40 суток. Увеличение продолжительности записи достигается за счет записи с пропуском кадров (Time-laps recording), с уплотненной записью и записью по тревоге.

Наиболее распространенный вариант — записывается не каждый кадр, а выборочно. В видеомагнитофоне с длительностью до 24 часов записывается каждый 8-й кадр, а в варианте наиболее длительной записи — каждый 320-й кадр. Но при этом способе речь не записывается. На каждом кадре регистрируется дата и время, что позволяет с точностью до минут восстановить события в случае возникновения нештатных ситуаций. По тревоге может осуществляться также переход из медленных «time-lapse» режимов в один из более быстрых, вплоть до номинальной скорости.

В магнитофонах с записью по тревоге для обеспечению малого времени от подачи сигнала «Запись» до начала записи предусмотрен режим ожидания. В этом режиме лента видеокассеты заправлена, а видеоголовка постоянно вращается. Для исключения протирания ленты вращающейся головкой лента медленно продвигается со скоростью 6 полукадров за 3 мин.

Современные методы M-JPEG сжатия цифрового видеосигнала в 15-25 раз без ухудшения качества обеспечили существенные преимущества цифровой видеозаписи:

- запись практически не подвержена старению и может храниться сколь угодно долго;
- при копировании не происходит ухудшения качества изображения копий;
- простота выбора любого кадра изображения, его вставки в документ и распечатывания изображения на обычном принтере.

Для регистрации отдельных кадров видеоизображения на бумаге применяются **видеопринтеры,** которые позволяют зафиксировать изображение контролируемой зоны на бумаге.

Провода кабелей электропитания, передачи видеосигналов, управления для исключения возможности их перерезывания или вытягивания помещаются в металлические рукава или трубы.

**Средства освещения**

Средства освещения включают:

- осветительные приборы;

- устройства управления освещением;
- кабели электропитания.

Время продвижения злоумышленника к источникам информации, вероятность его обнаружения и время его задержания зависят также от освещенности рубежей защиты и контролируемых зон в темное время суток и при плохих погодных условиях. В интересах защиты применяют три вида освещения: **дежурное, охранное** и **аварийное.**

**Дежурное освещение** повышает освещенность объектов, рубежей защиты и контролируемых зон в темное время суток и при плохой погоде до уровня, необходимого для визуального наблюдения и наблюдения с помощью телевизионных средств. Чрезмерная освещенность требует значительного ресурса. Кроме того, нерационально выполненное дежурное освещение способствует изучению злоумышленником системы защиты и упрощает его проникновение к источнику информации.

**Охранное извещение** предназначено для увеличения освещенности участков рубежей и зон, из которых поступили сигналы тревоги. В обычном режиме (при отсутствии нарушений) охранное освещение выключено. Оно должно обеспечить:

- равномерную освещенность охраняемой зоны шириной 3-4 м;
- возможность автоматического включения освещенности на отдельном участке при срабатывании сигнала тревоги от извещателя, установленного на этом участке;
- управления работой средств освещения из помещения контрольно-пропускного пункта (КПП);
- совместимость с техническими средствами охранной сигнализации и охранного телевидения;
- непрерывность работы на КПП и постах охраны.

**Аварийное освещение** предназначено для обеспечения минимального освещения на опасных участках рубежей и зон при нарушении в результате действий злоумышленника, стихии и технической неисправности нормального энергоснабжения системы защиты от сети 220/380 В. Аварийное освещение включается автоматически или вручную и должно обеспечить не менее 5% освещенности при охранном освещении.

В качестве осветительных приборов применяются **светильники подвесные** и **консольного типа,** а также **прожекторы.** Светильники наружного освещения закрываются небьющимися колпаками (плафонами) или металлической сеткой. Прожектор представляет собой осветительный прибор дальнего действия, в котором свет концентрируется посредством светооптической системы — металлического зеркала или линзы, в фокусе которых размещается источник света. В зависимости от мощности прожектора диаметр отражателя составляет 25-50 см.

В качестве источников света используются различные **лампы накаливания, газоразрядные лампы** и **ИК-прожекторы.**

**Вакуумные, криптоновые** и **галогенные** лампы накаливания напряжением 220 В выпускаются мощностью до 1000 Вт. Криптоновые лампы содер-

жат нейтральный газ криптон, уменьшающий испарение вольфрама из раскаленной нити лампы. В галогенной лампе температура нити повышена на 400-500 градусов относительно температуры вакуумных, что увеличивает светоотдачу приблизительно в 1,5 раза. Сохранение более раскаленной вольфрамовой нити от перегорания в течение длительного (в 3-5 раз большего, чем вакуумных) времени эксплуатации достигается в результате так называемого галогенного цикла. С этой целью в колбу лампы вводят йод. Пары йода, взаимодействуя с парами вольфрама, образуют йодистый вольфрам — галоген, который вблизи нити при температуре 2700-2900°С разлагается на йод и вольфрам. Вольфрам оседает на нити и снова испаряется — галогенный цикл повторяется. Так как колба лампы разогревается до температуры 600-700°С, то ее изготавливают из кварцевого стекла. Она имеет меньшие размеры и не боится влаги.

Основной недостаток ламп накаливания — низкая световая отдача (10-26 лм/Вт) и сравнительно малый срок службы (1000— 2000 ч).

**Разрядные** лампы имеют световую отдачу в 5-10 раз, а срок службы в 10-20 раз больше. В зависимости оттого, что является основным источником излучения, разрядные лампы делятся на следующие группы:

- газо - и паросветные, в которых излучение вызвано возбуждением атомов, молекул или рекомбинацией ионов газов, паров металлов (ртути, натрия) и их соединений;
- люминесцентные, источником света которых являются люминофоры, возбуждаемые излучением разряда;
- электродосветные, свет в которых излучают электроды, раскаленные в разряде до высокой температуры.

Для скрытого телевизионного наблюдения за действием злоумышленника применяются также **ИК-осветители.** В качестве источников ИК-света применяют лампы накаливания, закрытые непрозрачными для видимого света фильтрами, и полупроводниковые приборы (светодиоды). Светодиоды по сравнению с лампами имеют меньшие габариты, большую надежность и срок службы (5000 ч), но мощность их излучения мала. Поэтому в ИК прожекторах размещается большое количество светодиодов в виде матриц. Мощность оптического излучения ИК прожекторов составляет 50 Вт при угле рассеянии (10-20)°.

Кабели электропитания осветительных приборов прокладываются, как правило, под землей или в металлических трубах вдоль забора и стен зданий. Допускается использование воздушных сетей электропитания, расположенных на территории таким образом, чтобы исключалась возможность их повреждения, прежде всего, из-за ограждения.

# 6. ПОБОЧНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ И НАВОДКИ

Физическую основу случайных опасных сигналов, возникающих во время работы в выделенном помещении радиосредств и электрических приборов, составляют побочные электромагнитные излучения и наводки (ПЭМИН). Процессы и явления, образующие ПЭМИН, по способам возникновения можно разделить на 4 вида [2, 6]:

- не предусмотренные функциями радиосредств и электрических приборов преобразования внешних акустических сигналов в электрические сигналы;
- паразитные связи и наводки;
- побочные низкочастотные излучения;
- побочные высокочастотные излучения.

За рубежом побочные электромагнитные излучения называют «компрометирующими» излучениями (compromising emanations). Факты побочных излучений отмечены еще в XIX веке. Например, в 1884 г. в телефонных аппаратах на улице Грей-Стоун-Род в Лондоне прослушивались телеграфные сигналы, излучаемые неглубоко и параллельно проложенными под землей телеграфными проводами. Первые работы по изучению этих излучений появились еще в 20-е годы, но полномасштабные исследования их начались с 40-50-х годов XX века. Этому способствовало то, что развитие радиоприемной техники к этому времени создало возможности по практическому добыванию информации из побочных излучений. Например, после Второй мировой войны американскими спецслужбами были обнаружены побочные излучения и восстановлен в результате их перехвата информационный сигнал телетайпа советского представительства в Берлине. С середины 80-х годов постоянно растет количество по этой проблеме не только закрытых, но и открытых публикаций.

## 6.1. Побочные преобразования акустических сигналов в электрические сигналы

Преобразователи внешних акустических сигналов в электрические сигналы называются **акустоэлектрическими преобразователями.** К акустоэлектрическим преобразователям относятся физические устройства, элементы, детали и материалы, способные под действием переменного давления акустической волны создавать эквивалентные электрические сигналы или изменять свои параметры. Классификация акустоэлектрических преобразователей по физическим процессам, создающим опасные сигналы, приведена на рис. 7.1.

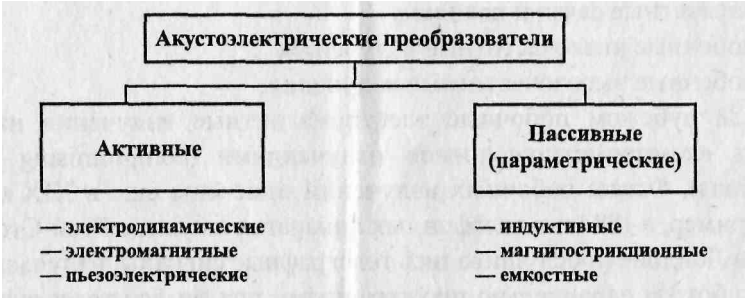



Рис. 6.1. Классификация акустоэлектрических преобразователей

На выходе активных акустоэлектрических преобразователей под действием акустической волны возникают электрические сигналы. У пассивных акустоэлектрических преобразователей те же действия акустической волны вызывают лишь изменения параметров преобразователей.

По способам формирования электрического сигнала активные акустоэлектрические преобразователи могут быть **электродинамическими, электромагнитными и пьезоэлектрическими.**

Опасные сигналы в **электродинамических акустоэлектрических преобразователях** возникают в соответствии с законом электромагнитной индукции при перемещении провода в магнитном поле под действием акустической волны.

Наибольшей чувствительностью обладают электродинамические акустоэлектрические преобразователи в виде динамических головок громкоговорителей (см. рис. 6.2).

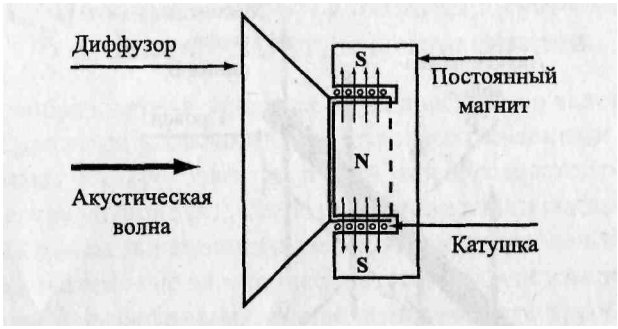



Рис. 6.2. Схема электродинамического громкоговорителя

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 проводах катушки возникает электродвижущая сила (ЭДС), величина которой пропорциональна громкости звука.

Аналогичный эффект возникает в **электромагнитных акустоэлектрических преобразователях.** Электрические сигналы индуцируются в катушках электромагнитов этих устройств в результате изменений напряженности создаваемых ими полей, вызванных изменениями под действием акустической волны воздушного зазора между сердечником и якорем электромагнита

или статора (неподвижной части) и ротора (подвижной) части электродвигателя. Для приведенной на рис. 6.3 схемы электромагнитного акустоэлектрического преобразователя напряжение E на концах проволоки, намотанной на катушке, пропорционально количеству витков W, площади s и относительной магнитной проницательности $\mu_o$ сердечника, обратно пропорционально расстоянию Δ между полюсом сердечника и подвижного якоря.

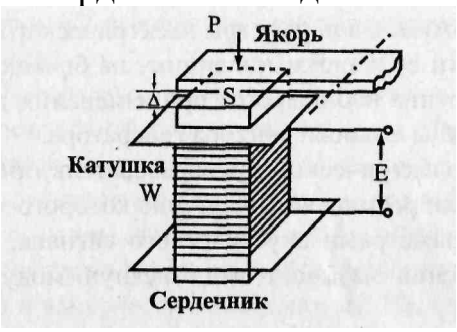



Рис. 6.3. Схема электромагнитного акустоэлектрического преобразователя

Перечень бытовых радио- и электроприборов, в которых возникают подобные процессы и которые устанавливаются в служебных и жилых помещениях, достаточно велик. 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 цепях 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.

**Активными пьезоэлектрическими акустоэлектрическими преобразователями** являются также некоторые кристаллические вещества (кварц, сегнетовая соль, титанат и ниобат бария и др.), которые широко применяются в радиоаппаратуре для стабилизации частоты и фильтрации сигналов, в качестве акустических излучателей сигналов вызова в современных телефонных аппаратах вместо электромеханических звонков. На поверхности этих веществ при механической деформации их кристаллической решетки (давлении на поверхность, изгибе, кручении) возникают электрические заряды.

В **пассивных акустоэлектрических преобразователях** акустическая волна изменяет параметры элементов схем средств, в результате чего изменяются параметры циркулирующих в этих схемах электрических сигналов. В большинстве случаев под действием акустической волны изменяются параметры индуктивностей и емкостей электрических цепей. В соответствии с этим акустоэлектрические преобразователи называются **индуктивными** и **емкостными.**

Если схема электрической цепи содержит катушку с витками проволоки, то под действием акустической волны изменяются расстояние между витками и геометрические размеры самой катушки. В результате этого, как следует из соответствующих формул, изменяется индуктивность катушки. Если, например, катушка является элементом частотно-задающего контура генератора, то

изменение индуктивности вызывает частотную модуляцию сигнала генератора. В итоге информация, записанная в параметры акустической волны, переписывается в параметры электрического сигнала, способного перенести ее к злоумышленнику на большое расстояние. Аналогичная картина наблюдается при изменении под действием акустической волны емкости контура генератора.

Если акустоэлектрический преобразователь представляет собой реактивное сопротивление, величина которого меняется в соответствии с параметрами акустического сигнала, то изменение этого сопротивления вызывает амплитудную модуляцию тока в цепи.

Разновидностью индуктивного является магнитострикционный акустоэлектрический преобразователь. **Магнитострикция** проявляется в изменении магнитных свойств ферромагнитных веществ (электротехнической стали и ее сплавов) при их деформировании (растяжении, сжатии, изгибании, кручении). Такое явление называется Виллари-эффектом или обратной магнитострикцией, открытым итальянским физиком Э. Виллари в 1865 г. Этот эффект обусловлен изменением под действием механических напряжений доменной структуры ферромагнетика. Прямая магнитострикция заключается в изменении геометрических размеров и объема ферромагнитного тела при помещении его в магнитное поле. В результате обратной магнитострикции под действием акустической волны изменяется магнитная проницаемость сердечников контуров, дросселей, трансформаторов радио- и электротехнических устройств, что приводит к эквивалентному изменению значений индуктивностей цепи и модуляции протекающих через них высокочастотных сигналов.

К наиболее распространенным случайным акустоэлектрическим преобразователям относятся:

- вызывные устройства телефонных аппаратов;
- динамические головки громкоговорителей, электромагнитные капсюли телефонных трубок, электрические двигатели вторичных часов системы единого времени и бытовых электроприборов;
- катушки контуров, дросселей, трансформаторов, провода монтажных жгутов, пластины (электроды) конденсаторов;
- пьезоэлектрические вещества (кварцы генераторов, виброакустические излучатели акустических генераторов помех);
- ферромагнитные материалы в виде сердечников трансформаторов и дросселей.

Угроза информации от акустоэлектрического преобразователя зависит, прежде всего, от его чувствительности. **Чувствительность** акустоэлектрического преобразователя характеризуется отношением величины электрического сигнала на его выходе или изменения падающего на нем напряжения к силе звукового давления на поверхность чувствительного элемента преобразователя на частоте f = 1000 кГц и измеряется в В/Па или мВ/Па. Очевидно, что чем выше чувствительность случайного акустоэлектрического преобразователя, тем больше потенциальная угроза от него для безопасности акустической информации.

Чувствительность в мВ/Па некоторых акустоэлектрических преобразователей приведена в таблице 6.1.

Таблица 6.1

| *№ п/п* | *Акустоэлектрический преобразователь* | *Чувствительность, мВ/Па* |
|---|---|---|
| 1 | Электродинамический микрофон | 4–6 |
| 2 | Электродинамический громкоговоритель | 2–3 |
| 3 | Абонентский громкоговоритель | 30–45 |
| 4 | Вторичные электрические часы | 0,1–0,5 |
| 5 | Электромеханический звонок телефонного аппарата | 0,05–0,6 |
| 6 | Пьезоэлектрическое вызывное устройство телефонного аппарата | 8–11 |
| 7 | Телефонный капсюль | 3–5 |
| 8 | Электромагнитное реле | 0,04–0,5 |
| 9 | Трансформаторы, дроссели | 0,001–0,2 |

Опасные сигналы, образованные акустоэлектрическими преобразователями, могут:

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

Техническую основу для реализации первой угрозы создают, например, неработающий громкоговоритель 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 значительные расстояния, достаточные для снятия 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, может 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 сети составляют единицы и доли мВ, их нетрудно отделить 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 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 наводить в цепях рядом расположенных радиоэлектронных средств электрические сигналы с аналогичным эффектом.

## 6.2. Паразитные связи и наводки

В любом радиоэлектронном средстве или электрическом приборе наряду с токопроводами (проводами, проводниками печатных плат), предусмотренными их схемами, возникают многочисленные побочные пути, по которым распространяются электрические сигналы, в том числе опасные сигналы акустоэлектрических преобразователей. Эти пути создаются в результате паразитных связей и наводок. Первопричиной их являются поля, создаваемые электрическими зарядами и токами в цепях радиоэлектронных средств и приборов.

Постоянные электрические заряды и электрический ток в элементах и цепях радиосредств и электрических приборов создают соответствующие электрические и магнитные поля, а заряды и ток переменной частоты — электромагнитные поля. Поля распространяются в пространстве и воздействуют на элементы и цепи других технических средств и систем. Кроме того, для функционирования средств и систем необходимо обеспечить гальваническое соединение их элементов. Из-за гальванических соединений возникают дополнительные пути для распространения сигналов одних узлов и блоков по цепям других. В результате воздействия побочных полей и влияния через проводники и резисторы сигналов одних узлов и блоков на сигналы других блоков и узлов возникают паразитные связи и наводки как внутри радиоэлектронных средств, так и между рядом расположенными средствами. Эти связи и наводки ухудшают работу узлов, блоков и средств в целом. Поэтому при

проектировании радиоэлектронных средств уровни этих паразитных связей и наводок снижают до допустимых значений. Чем выше требования к характеристикам средств, тем требуются большие усилия, а следовательно, и затраты для нейтрализации паразитных связей и наводок.

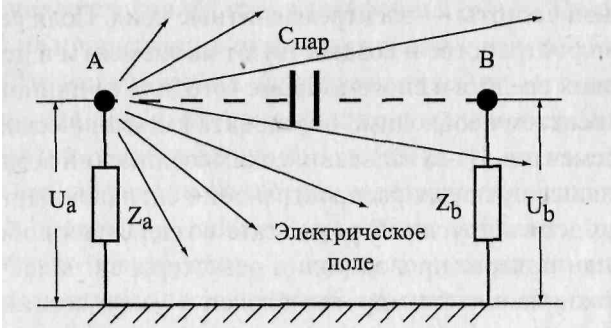
Однако, несмотря на принимаемые меры по снижению уровня паразитных связей и наводок для обеспечения требуемых характеристик радиоэлектронного средства, остаточный их уровень создает угрозы для информации, содержащейся в информационных параметрах сигналов, циркулирующих в радиоэлектронном средстве. **Поэтому любое радиоэлектронное средство или электрический прибор следует с точки зрения информационной безопасности рассматривать как потенциальный источник угрозы безопасности информации.**

Известны три вида паразитных связей:

- емкостная;
- индуктивная;
- гальваническая.

**Емкостная связь** образуется в результате воздействия электрического поля, индуктивная — воздействия магнитного поля, гальваническая связь — через общее активное сопротивление.

Модель емкостной паразитной связи представлена на рис. 6.4.




Рис, 6.4. Паразитная емкостная связь

На этом рисунке $U_a$ — переменное напряжение точки **А** относительно корпуса, создающий электрическое поле. В результате воздействия этого поля в точке **В** также возникает переменное напряжение.

Так как между рядом расположенными основными и вспомогательными средствами связи существует паразитная емкостная связь, способствующая передаче сигналов с защищаемой информацией от основных технических средств и систем (**ОТСС)** к вспомогательным техническим средствам и системам (**ВТСС**), то для определения величины наводки надо знать их паразитные емкости. Эти емкости называются **собственными емкостями** радиоэлектронного средства и электрического прибора.

**Паразитная индуктивная связь** иллюстрируется рис. 6.5.

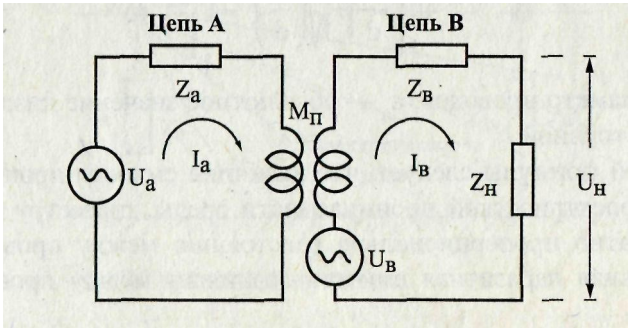



Рис. 6.5. Паразитная индуктивная связь

Переменный ток, протекающий по цепи **А**, создает магнитное поле, силовые линии которого достигают проводников другой цепи **В** и наводят в ней ЭДС

Взаимная индуктивность замкнутых цепей зависит от взаимного расположения и конфигурации проводников. Она тем больше, чем большая часть магнитного поля тока в одной цепи пронизывает проводники другой цепи.

**Гальваническую паразитную связь** еще называют связью через общее сопротивление, входящее в состав нескольких цепей. Такими общими сопротивлениями могут быть сопротивление соединительных проводов и устройств питания и управления. Например, узлы и блоки компьютера, осуществляющего обработку информации, соединены с напряжением +5 В блока питания. Для установки «0» триггеров дискретных устройств на соответствующие их входы подается одновременно соответствующий сигнал управления. На рис. 6.6 приведена упрощенная схема, иллюстрирующая возникновение гальванической связи.

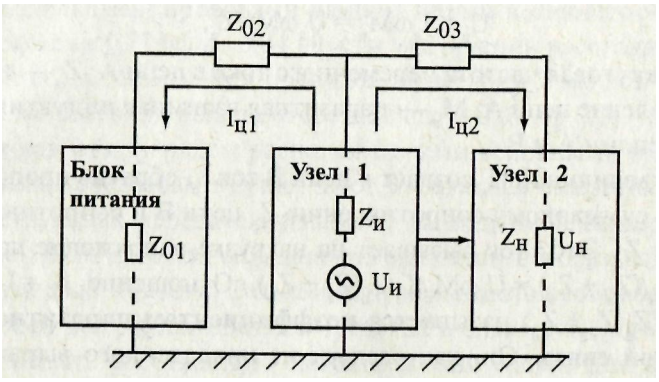



Рис. 6.6. Паразитная гальваническая связь

В соответствии с ним к блоку питания через общие сопротивления $Z_{01}$, $Z_{02}$ и $Z_{03}$ подключены узел 1 и узел 2 радиоэлектронного средства. Сигнал напряжением $U_и$ 1-го узла создает токи $I_{ц1}$ и $I_{ц2}$ в результате которых на эквивалентном сопротивлении $Z_н$ 2-го узла возникает напряжение наводки $U_н$. Отношение $\beta = U_н / U_и$ называется **коэффициентом паразитной гальванической связи.**

Если побочные поля и электрические токи являются носителями защищаемой информации, то паразитные наводки и связи могут приводить к утечке информации. Следовательно, паразитные связи и наводки представляют

собой побочные физические процессы и явления, которые могут приводить к утечке защищаемой информации.

Возможность утечки информации через паразитные связи и наводки носит вероятностный характер и зависит от многих факторов, в том числе от конфигурации, размеров (относительно периода колебаний протекающих токов) и взаимного положения излучающих и принимающих токопроводящих элементов средств. В отличие от предусмотренных для связи функциональных антенн, конструкция и характеристики которых определяются при создании радиопередающих и радиоприемных средств, эти элементы можно назвать **случайными антеннами.**

Случайными антеннами могут быть монтажные провода, соединительные кабели, токопроводы печатных плат, выводы радиодеталей, металлические корпуса средств и приборов и другие элементы средств. Параметры случайных антенн существенно хуже функциональных. Но из-за небольших расстояний между передающими и приемными случайными антеннами (в радиоэлектронном средстве или одном помещении) они создают угрозы утечки информации.

Случайные антенны имеют сложную и часто априори неопределенную конфигурацию, достаточно точно рассчитать значения их электрических параметров, совпадающих с измеряемыми, очень сложно. Поэтому реальную случайную антенну заменяют ее моделями в виде проволочной антенны — отрезка провода (вибратора) и рамки.

Паразитные связи могут вызывать утечку информации по проводам и создавать условия для возникновения побочных электромагнитных излучений. За счет паразитных связей возникают опасные сигналы в проводах кабелей различных линий и цепей, в том числе в цепях заземления и электропитания, а также возникают паразитные колебания в усилителях, дискретных устройствах и др.

Серьезную угрозу безопасности информации создают наводки сигналов ОТСС на провода и кабели, выходящие за пределы контролируемой зоны (рис. 6.7).

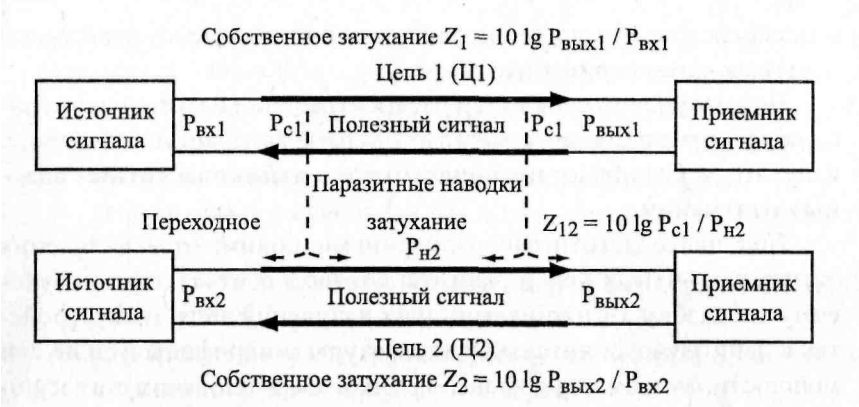



Рис. 6.7. Паразитные наводки

Когда ток проходит по проводникам первой цепи (Ц1), вокруг них создается магнитное поле, силовые линии которого пронизывают проводники вто-

рой цепи (Ц2). В результате этого по цепи Ц2 потечет помимо основного еще и переходной ток, создающий помеху основному. Защищенность от взаимных помех оценивается так называемым переходным затуханием $Z = 101gP_{c1}/P_{н2}$ , где $P_{с1}$ и $P_{н2}$ — мощность сигналов в 1-й цепи и наводки от них во 2-й цепи. Для надежной защиты информации переходное затухание должно быть не менее величины $101gP_{с}/P_{пр}$, где $P_{с}$ и $P_{пр}$ — мощность сигнала с информацией и чувствительность приемника злоумышленника, перехватывающего наведенный сигнал. Так как кабели в здании укладываются в специальных колодцах и нишах, то между кабелями за счет их достаточно близкого и параллельного на большом расстоянии расположения возникают достаточно большие паразитные связи между кабелями внутренней и городской АТС, других информационных линий связи, цепями электропитания и заземления. Так как сотрудники организации при разговоре по телефонам внутренней АТС чаще допускают нарушения режима секретности (конфиденциальности), чем во время разговора по городской АТС, то при регулярном подслушивании разговоров по внутренней АТС можно добыть ценную информацию.

Современная архитектура служебных помещений предусматривает создание между межэтажными перекрытиями и потолком (полом) свободного пространства для прокладки различных кабелей (электропитания, внутренней и городской АТС, трансляции, оперативной и диспетчерской связи, сетей передачи данных и др.). Это создает дополнительные возможности для возникновения между проводами кабелей паразитных связей и появления опасных сигналов, распространяющихся за пределы контролируемой зоны.

## 6.3. Низкочастотные и высокочастотные излучения технических средств

Большую угрозу безопасности информации создают также побочные излучения радио- и электротехническими средствами электромагнитных полей, содержащих защищаемую информацию. Источниками излучений могут быть цепи, содержащие статические или динамические заряды (электрический ток), в информационные параметры которых тем или иным способом записывается защищаемая информация. Носители защищаемой информации в виде статических или динамических зарядов могут попадать в эти цепи непосредственно, если эти цепи участвуют в обработке, передаче и хранении защищаемой информации или сами элементы цепей обладают свойствами акустоэлектрических преобразователей, или опосредованно, когда опасные сигналы проникают в излучающие цепи через паразитные связи.

Вид излучения и характер распространения электромагнитного поля в пространстве зависит от частоты колебаний поля и вида излучателя. Различают **низкочастотное и высокочастотные опасные излучения.**

Под низкочастотными излучениями понимаются излучения электромагнитных полей, частоты которых соответствуют звуковому диапазону. Источниками таких излучений являются устройства и цепи звукоусилительной аппаратуры (микрофоны, усилители мощности, аудиомагнитофоны, громкоговорители и их согласующие трансформаторы, кабели между микрофонами

и усилителями, усилителями и громкоговорителями, цепи, содержащие случайные акустоэлектрические преобразователи, телефонные аппараты и кабели внутренней АТС и др.).

Наибольшую угрозу создают средства звукофикации помещений для озвучивания акустической информации, содержащей государственную или коммерческую тайну. Эти средства включают микрофоны, усилители мощности, громкоговорители, устанавливаемые на стенах больших помещений (залов для совещаний, конференц-залов) или в спинки кресел, а также соединительные кабели. Причем часто усилители мощности размещаются в техническом помещении, удаленном на значительном расстоянии от конференц-зала. По проводам кабелей звукоусилительной аппаратуры протекают большие токи, составляющие доли и единицы ампер. Эти токи создают мощные магнитные поля, которые, во-первых, могут распространяться за пределы выделенного помещения, здания и даже организации, а во-вторых, наводить ЭДС в любых токопроводящих конструкциях, в том числе в цепях электропитания и металлической арматуре зданий.

К **высокочастотным опасным излучениям** относятся электромагнитные поля, излучаемые цепями радиоэлектронных средств, по которым распространяются высокочастотные (выше звукового диапазона) сигналы с секретной (конфиденциальной) информацией. Можно утверждать, что если не приняты специальные дополнительные меры, то источниками подобных опасных побочных ВЧ-излучений могут быть любые цепи радио - и электрических средств. К основным источникам побочных излучений с мощностью, достаточной для распространения электромагнитного поля за пределы контролируемой зоны, например помещения, относятся:

- гетеродины радио- и телевизионных приемников;
- генераторы подмагничивания и стирания аудио- и видеомагнитофонов;
- усилители и логические элементы в режиме паразитной генерации;
- электронно-лучевые трубки средств отображения защищаемой информации (мониторов, телевизоров);
- элементы ВЧ-навязывания;
- мониторы, клавиатура, принтеры и другие устройства компьютеров, в которых циркулируют сигналы в параллельном коде.

**Гетеродины радио- и телевизионных приемников** являются генераторами гармонических колебаний, необходимыми для преобразования частоты принимаемого сигнала в промежуточную частоту. Гармоническое колебание с гетеродина подается на смеситель, на нелинейном элементе (диоде или транзисторе) которого осуществляется преобразование входного (принимаемого) сигнала в сигнал промежуточной частоты. Частоты сигналов гетеродинов отличаются на величину промежуточной частоты (465 кГц — для ДВ-, СВ- и КВ-диапазонов, 10 МГц — для УКВ-диапазонов) от принимаемых сигналов и могут иметь значения от сотен кГц до десятков ГГц. Если элементы контура (индуктивность и емкость) гетеродина обладают свойствами акустоэлектрических преобразователей или в него проникают опасные сигналы от других акустоэлектрических преобразователей, то возможна амплитудная или ча-

стотная модуляция сигналов гетеродина. Мощность излучения модулированных сигналов гетеродина тем больше, чем ближе значения длины волны гармонического колебания к длине цепей, по которым протекают сигналы гетеродинов. Часто она бывает достаточной для подслушивания речевой информации в кабинете руководителя с включенным радио- или телевизионным приемником с помощью бытовых радиоприемников в соседних помещениях или даже зданиях.

**Генераторы сигналов высокочастотного подмагничивания и стирания** магнитофонов создают гармонические колебания на частотах в сотни кГц. Генераторы сигналов высокочастотного подмагничивания необходимы для обеспечения аналоговой аудио- и видеозаписи с малыми нелинейными искажениями. Зависимость остаточной намагниченности магнитной пленки от напряженности магнитного поля в головке записи нелинейная, что вызывает нелинейные искажения в записанном сигнале. Путем подачи в магнитную головку наряду с током записи дополнительного тока подмагничивания с частотой около 100 кГц и амплитудой, в 6-8 раз превышающей максимальную амплитуду тока записи, устанавливается рабочая точка для тока записи на линейном участке кривой намагничивания магнитной ленты. В результате выбора оптимального тока подмагничивания удается уменьшить нелинейные искажения сигналов записи до единиц процентов.

Генератор высокочастотного стирания обеспечивает стирание записанной на магнитную ленту информации путем размагничивания ее магнитного слоя практически до нуля. Для этого в стирающую головку аудиомагнитофона подается ток с частотой 50-100 кГц. При такой частоте тока стирания и уменьшения напряженности магнитного поля головки в результате удаления стираемого элементарного участка движущейся магнитной ленты от зазора стирающей магнитной головки происходит многократное перемагничивание участка с убывающей до нуля намагниченностью. В отличие от высокочастотного стирания уничтожение информации путем воздействия на магнитный слой магнитным полем постоянного магнита, который применяется в качестве стирающей головки в специальных диктофонах, обеспечивается путем намагниченности магнитного слоя ленты до насыщения.

**Паразитная генерация** может возникнуть при определенных условиях в усилителях и логических элементах дискретной техники. Логический элемент рассматривается в данном контексте как усилитель с очень высоким коэффициентом усиления.

Так как между элементами усилителя всегда существуют емкостные, индуктивные и гальванические паразитные связи, то на входе усилителя наряду с усиливаемым внешним сигналом присутствуют сигналы, проникшие во входные цепи через паразитную обратную связь, в том числе с выхода усилителя. Обобщенная математическая модель усилителя с обратной связью представлена на рис. 6.8.

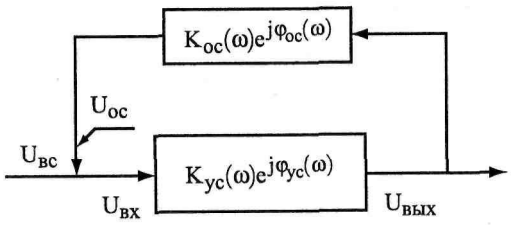



Рис. 6.8. Модель усилителя с обратной связью

Режим усиления переходит в режим генерации, когда выходной сигнал достигает максимального значения и поддерживается на этом уровне независимо от $U_{вх}$.

Например, если К = 10, то для возникновения генерации необходимо проникновение 0,1 части выходного сигнала на вход усилителя. Для усилителя с К = 100 достаточно поступления на его вход 0,01 части выходного сигнала. Эта зависимость объясняет возможность паразитной генерации в логических элементах дискретной техники. Высокий коэффициент усиления логического элемента и высокая частота спектральных составляющих фронта дискретного сигнала создают благоприятные условия для возникновения паразитной генерации в логических элементах.

Второе условие предусматривает, что изменение фазы сигнала обратной связи должно быть противоположно величине фазового сдвига усилителя. Это означает, что фазы внешнего сигнала и сигнала обратной связи должны быть приблизительно равными. Обратная связь, при которой фаза сигнала на входе усилителя совпадает с фазой сигнала обратной связи, называется **положительной,** а когда фазы этих сигналов противоположные — **отрицательной.** Если положительная обратная связь способствует паразитной генерации, то отрицательная, наоборот, повышает стабильность работы усилителя, но за счет некоторого снижения напряжения на выходе усилителя. Поэтому в усилителях с высоким коэффициентом усиления для исключения паразитной генерации создают между каскадами отрицательную обратную связь, а также применяют комплекс мер по уменьшению паразитных связей. С этой целью при монтаже используют короткие экранированные провода, элементы входных и выходных цепей разносят на максимально возможное расстояние, экранируют трансформаторы усилителей, в цепи питания предварительных каскадов устанавливают RC-фильтры низких частот, усилительные каскады размещают в одну линию и др.

Опасность паразитной генерации состоит также в том, что она часто возникает на частотах выше рабочего диапазона и без специальных исследований не обнаруживается. Действительно, с ростом частоты обрабатываемых сигналов уменьшаются значения паразитных емкостных и индуктивных сопротивлений между каскадами. В результате этого увеличиваются $K_{ос}$ и сдвиг фазы сигналов, прошедших через паразитные связи. Поэтому возможность выполнения условий генерации в усилителе на частотах, превышающих верхнюю частоту рабочего диапазона частот усилителя, повышается. Хотя на этой частоте полезные сигналы на вход усилителя не подаются, но на его входе

присутствуют сигналы, обусловленные тепловым шумом и проникшие через паразитную обратную связь. Любая шумовая реализация на входе усиливается усилителем и частично возвращается через паразитную обратную связь на его вход. При равенстве фаз величина суммарного сигнала на входе усилителя повышается, что приводит к росту сигнала на выходе усилителя. Следствием этого является увеличение сигнала $U_{ос}$ и дальнейшее увеличение сигнала на входе усилителя и т. д. Происходит лавинообразный процесс нарастания амплитуды сигнала на входе и выходе усилителя, завершаемый процессом непрерывной генерации на частоте $\omega_{рез}$. Поэтому не рекомендуется, например, применять в усилителях низкой частоты высокочастотные транзисторы, которые усиливают шумы с частотами выше верхней границы рабочего диапазона частот.

Паразитная генерация усилителя или логического элемента создает угрозу информации, если она записывается в информационные параметры паразитного колебания, т. е. происходит его модуляция информационными сигналами. Это явление возникает в случае, если цепи паразитного генератора содержат акустоэлектрические преобразователи или в них попадают опасные сигналы от других случайных акустоэлектрических преобразователей усилителя.

Люминофор электронно-лучевых трубок средств отображения под действием электронов излучает, кроме света, электромагнитное поле в широком диапазоне радиочастот с напряженностью, которая обеспечивает возможность перехвата сигналов на удалении в десятки метров. Учитывая, что сигналы управления электронным лучом трубки подаются последовательно во времени, их побочные ВЧ-излучения создают серьезную угрозу для отображаемой на экране трубки информации.

Устройства компьютера, в которых распространяются сигналы в последовательном коде (мониторы, клавиатура, принтеры и другие), также представляют собой источники опасных сигналов. Замена монитора компьютера на электронно-лучевой трубке на жидкокристаллический монитор не устраняет проблему защиты информации, отображаемой на его экране. Хотя экран жидкокристаллического монитора не создает опасные излучения, но в устройстве управления значениями пикселей строки монитора присутствуют последовательные информационные сигналы. Спектр этих сигналов имеет широкий спектр в диапазоне сотен МГц. В результате их перехвата возможно восстановление изображения.

К **излучающим элементам ВЧ-навязывания** относятся радио - и механические элементы, которые обеспечивают модуляцию подводимых к ним внешних электрических и радиосигналов. К таким элементам относятся:

- нелинейные элементы, на которые одновременно поступают низкочастотный электрический сигнал с защищаемой информацией (опасный сигнал) и высокочастотный гармонический сигнал;
- токопроводящие механические конструкции, изменяющие свой размер и переотражающие внешнее электромагнитное поле.

Если на нелинейный элемент (диод, транзистор) подаются 2 сигнала: низкочастотный сигнал $u_c(t)$, в информационные параметры, которых, записана информация, и высокочастотный (сотни кГц – единицы ГГц) гармонический сигнал $u_{вч}$ от внешнего генератора, то в токе через нелинейный элемент появятся высокочастотные составляющие, модулированные по амплитуде опасным сигналом.

Из этого следует наличие в спектре тока высокочастотных гармоник опасного сигнала, несущих защищаемую информацию. Этот ток создает электромагнитное поле, мощность которого зависит не только от мощности сигналов, но и от соотношения длины его волны и длины цепи, по которой протекает ток. Такой вариант реализуется путем подачи внешнего высокочастотного электрического сигнала в телефонную проводную линию.

Другим видом излучателя ВЧ-навязывания являются механические конструкции, способные изменять свой размер под действием акустической волны и переотражать внешнее электромагнитное поле. Такие конструкции, как правило, образуют замкнутую полость с токопроводящими поверхностями, одна из которых – тонкая и способна колебаться в соответствии с акустическим сигналом мембрана. При колебании мембраны изменяются геометрические размеры полости. Полость представляет собой колебательный контур, собственная частота которого определяется ее геометрическими размерами. При облучении конструкции электромагнитным полем с частотой колебания, равной собственной частоте контура, возникают резонансные явления и переотражается максимум энергии облучаемого поля. При колебаниях мембраны изменяются частота и напряженность переотраженного поля. После приема переотраженного поля из него можно выделить путем демодуляции электрический сигнал, соответствующий акустическому. Такой излучатель ВЧ-навязывания по существу представляет собой пассивный акустоэлектрический преобразователь подводимой энергии.

Дальность распространения излучаемого ВЧ-электромагнитного поля зависит от его мощности, частоты колебания, величины затухания поля в среде и характера распространения поля.

Характер распространения электромагнитного поля в свободном пространстве описывается 4 уравнения Максвелла, приведенными им в 1873 г. в труде «Трактат об электричестве и магнетизме». Эти уравнения явились обобщением открытых ранее законов электрического и магнитного полей.

В соответствии с первым уравнением любое магнитное поле создается электрическими токами и изменением во времени электрического поля. Второе уравнение обобщает закон электромагнитной индукции, открытый Фарадеем в 1831 г., и указывает на то, что в результате изменения магнитного поля в любой среде появляется электрическое поле. Из третьего уравнения Максвелла следует, что поток вектора электрической индукции через любую замкнутую поверхность равен сумме зарядов в объеме, ограниченном этой поверхностью. Четвертое уравнение позволяет сделать вывод о том, что число силовых линий магнитного поля, входящих в среду некоторого объема, равно

числу силовых линий, выходящих из этого объема. Это возможно при условии отсутствия в природе магнитных зарядов.

Из уравнений Максвелла также следует, что автономно (независимо) в природе могут существовать только постоянные электрические и магнитные поля. Поле, излучаемое зарядами и токами переменной частоты, является электромагнитным. В нем присутствуют электромагнитные и электрические компоненты, которые описываются взаимно перпендикулярными векторами. В зависимости от вида излучателя и расстояния от него до точки измерения характер изменения и соотношения между этими компонентами отличаются и изменяются. Характер распространения электромагнитного поля поддается точному математическому описанию для моделей излучателей в виде элементарных вибраторов. В качестве элементарного вибратора рассматривается модель излучателя, размеры которой существенно меньше длины волны излучаемого электромагнитного поля и расстояния от излучателя до точки измерения. Для такой модели параметры излучения во всех точках принимаются равными. Различают элементарные электрический вибратор и магнитную рамку. Электрический вибратор возбуждается источником переменной электродвижущей силы (источником зарядов), магнитная рамка — протекающим по рамке током.

В реальных условиях, с учетом переотражения электромагнитных волн от многочисленных преград (зданий, стен помещений, автомобилей и т. д.), характер распространения столь сложен, что в общем случае не поддается строгому аналитическому описанию.

В зависимости от соотношения геометрических размеров источников излучений и расстояния от них до точки измерения поля различают **сосредоточенные и распределенные источники.** Сосредоточенные источники имеют размеры, существенно меньшие, чем расстояние от источника до точки наблюдения. К сосредоточенным источникам относится большинство радиоэлектронных средств и их узлов, а также головки громкоговорителей. Для распределенных источников их геометрические размеры соизмеримы или больше расстояния до них. Типовые распределенные источники электромагнитного излучения – провода кабелей линий связи.

### 6.4. Утечка информации по цепям электропитания

К цепям, имеющим выход за пределы контролируемой зоны и в которые могут проникнуть опасные сигналы через паразитные связи любых видов, относятся, прежде всего, цепи электропитания. Поэтому предотвращение утечки информации по этим цепям является одной из задач инженерно-технической защиты информации.

Цепи электропитания обеспечивают передачу электрической энергии в виде переменного электрического тока напряжением 380/220 В и частотой 50 Гц от внешних источников (подстанций) подавляющему большинству устанавливаемых в помещениях радио- и электрических приборов (технических средств и систем – ТСС). Соединение источника и приемника производят при

помощи трех или четырех проводов. При трехпроводной линии передачи источники могут быть соединены как треугольником, так и звездой (рис. 6.9).

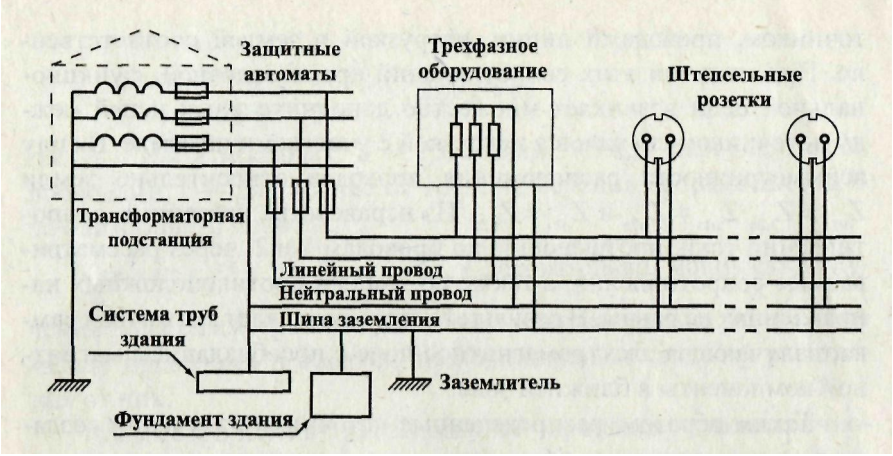



Рис. 6.9. Схема цепей электропитания здания

В последнем случае точка соединения концов обмоток трансформатора (нейтральный провод – нейтрал) остается неподключенной и схема подключения не имеет нейтрального провода. Чаще используемую четырехпроводную линию передачи электроэнергии применяют при соединении фаз источника и приемника звездой. Один из проводов соединяет точки нейтралей и заземляется (рис. 6.9). Напряжение каждой фазы относительно нейтрального провода (фазовое напряжение) при соединении звездой составляет 220 В, линейное напряжение (между фазами) больше – 380 В. Трехфазное напряжение применяется для электропитания в основном мощных электродвигателей различных технических средств, однофазное напряжение 220 В – для электропитания радиоэлектронных средств и бытовых маломощных электрических приборов (ламп освещения, вентиляторов, холодильников, электронагревательных приборов и др.).

В качестве первичных источников электропитания ТСС используются трансформаторные подстанции (ТПС) типа ТП 6-10/04 кВ или другие, понижающие трехфазное напряжение 6-10 кВ от центрального распределительного пункта (ЦРП) или главной понижающей подстанции (ГПП) до трехфазного напряжения 380 В. К потребителям электроэнергия от трансформаторной подстанции подается, как правило, по радиальной схеме, в соответствии с которой каждый потребитель или их группа питается по отдельной линии от соответствующего коммутационного узла. Линии передачи представляют собой, как правило, четырехжильные силовые кабели.

Так как цепи электропитания выходят за пределы охраняемой зоны, то распространение по ним опасных сигналов создает угрозу безопасности защищаемой информации. Существуют, по крайней мере, 4 причины появления опасных сигналов в цепях электропитания.

**Первой причиной** является наведение в них ЭДС полями НЧ и ВЧ побочных излучений ОТСС.

**Вторая причина** обусловлена модуляцией тока электропитания токами радиоэлектронного средства (РЭС). Иллюстрирующая эту причину модель представлена на рис. 6.10.

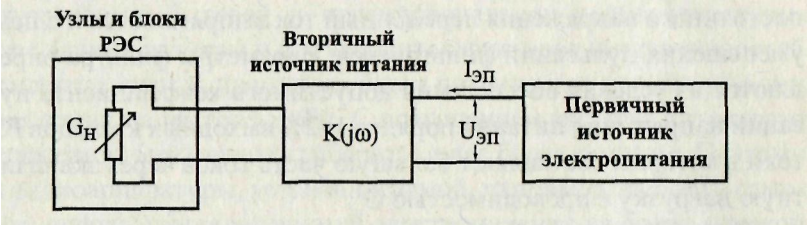



Рис. 6.10. Модель цепи электропитания

Источником электропитания радиоэлектронного средства является блок питания, который можно представить в виде передаточной функции K(jω). Нагрузкой вторичного источника электропитания являются узлы и блоки РЭС. Эту нагрузку можно представить в виде сопротивления или проводимости $G_H(t)$. Величина проводимости нагрузки меняется в соответствии с характером изменения величины обрабатываемого полезного сигнала S(t), или. $G_H(t) \equiv S(t)$. Поэтому ток в цепи электропитания блока $I_{эп}$ будет пропорционален величине обрабатываемого полезного сигнала S(t). Из анализа следует, что ток в цепи электропитания содержит составляющие с частотами полезного сигнала, которые можно выделить и с которых можно снять информацию.

Типовой вторичный источник питания (блок питания) состоит из следующих последовательно соединяемых узлов:

- сетевого трансформатора с коэффициентом трансформации п;
- выпрямителя;
- фильтра блока питания;
- стабилизатора;
- устройства для защиты блока питания от короткого замыкания.

Трансформатор преобразует напряжение 220 В в напряжение питания узла (блока) радиоэлектронного средства. Для получения постоянного напряжения переменный ток выпрямляется и с целью уменьшения пульсаций фильтруется. Параметры фильтра определяются из условия обеспечения допустимого коэффициента пульсаций напряжения питания порядка 1-2% выходных каскадов РЭС, токи в которых составляют большую часть токов через эквивалентную нагрузку с проводимостью G .

Каждый из узлов блока питания оказывает определенное влияние на K(jω). Наибольшие искажения вносят фильтр питания и стабилизатор, которые можно представить в виде фильтра низкой частоты с максимальной частотой пропускания около 30 Гц. Следовательно, типовой вторичный источник питания пропускает от РЭС в цепи электропитания сигналы в диапазоне 0-30 Гц. Если в радиоэлектронном средстве осуществляется обработка (усиление) речевых сигналов, то вторичный источник питания вырезает из его спектра участок шириной до 30 Гц и подавляет спектральные составляющие большей частоты. Учитывая, что спектр речевого сигнала лежит в диапазоне сотен Гц-единиц кГц, вторичный источник питания не пропускает спектральные составляющие речевого сигнала, но пропускает его огибающую. Огиба-

ющая речевого сигнала имеет полосу до 60-100 Гц, но его основная энергия сосредоточена в полосе до 30 Гц. Попадание огибающей речевого сигнала в цепи электропитания позволяет при ее перехвате понять смысл сообщения.

В соответствии с **третьей причиной** опасный сигнал может попасть в цепи электропитания через паразитные связи элементов схемы и элементов блока питания. Например, между первичной и вторичной обмотками сетевого (силового) трансформатора существуют индуктивная и емкостная паразитные связи, через которые опасные сигналы могут поступать от узлов и блоков РЭС в цепи электропитания без существенного ослабления его сердечником трансформатора.

**Четвертая причина** вызвана процессами в импульсных блоках питания РЭС, которые применяются вместо традиционных блоков питания с силовыми трансформаторами для частоты 50 Гц. Силовой трансформатор низкой частоты традиционного блока питания имеет большие габариты и вес, которые сдерживают миниатюризацию бытовой и профессиональной радиоаппаратуры. Также велики размеры и вес элементов фильтров (индуктивностей и конденсаторов) выпрямителя блока питания при преобразовании напряжений на частоте 50 Гц. С повышением частоты питающего напряжения уменьшаются габариты и вес блока питания. Поэтому для радиоаппаратуры, устанавливаемой, например, на борту самолетов, используются источники электропитания на более высокой частоте 400 Гц.

В современных импульсных блоках питания напряжение 220 В от первичного источника коммутируется электронным ключом, управляемым импульсным генератором с частотой повторения импульсов порядка 100 кГц. Высокочастотное питающее напряжение подается на импульсный трансформатор, выпрямитель, стабилизатор и фильтр блока питания с существенно меньшими габаритами и весом.

Однако высокочастотный ток, протекающий через ключ, имеет сложную форму и, соответственно, широкий спектр. Этот спектр может содержать составляющие, образующиеся в результате комбинаций сигналов импульсного генератора и информационных сигналов, проникающих через паразитные связи из узлов РЭС в элементы блока питания. Высокая частота этих опасных сигналов обеспечивает условия для их излучения в эфир с уровнем, достаточным для обнаружения и приема на удалении нескольких десятков метров.

# 7. Акустические каналы утечки информации

## 7.1. Основные понятия, определения и единицы измерения в акустике

Звук – колебательное движение упругой среды. Процесс распространения колебательного движения в среде называется звуковой волной. За один полный период колебания Т звуковой процесс распространяется в среде на расстояние, равное длине волны $\lambda$, которая может быть получена из соотношения:

$$\lambda = cT = c/f .$$

где c – скорость распространения звука в среде;

$f = 1/T$ – частота звукового колебания.

Ниже даны скорости распространения звука в некоторых средах [6]:

Своздух – 340м/с;
Свода – 1490 м/с;
Скирпич – 2300 м/с;
Сбетон – 3700 м/с;
Ссталь – 5200 м/с.

Изменения давления в звуковой волне относительно среднего значения называется звуковым давлением Р и измеряется в паскалях. Один паскаль это давление, создаваемое силой в один ньютон, действующей на площадь один квадратный метр:

$$P = \frac{1\,Н}{1\,м^2} = 1\,Па = \frac{1}{100000}\,АТМ.$$

В акустике принято использование относительных единиц измерения уровня звукового давления – децибел:

$$L_{дБ} = 20\lg\frac{P}{P_0}.$$

В качестве $P_0$ выбрана величина $P = P_0 = 2\cdot10^{-5}$ Па, что соответствует минимальному звуковому давлению, воспринимаемому человеческим слухом. При этом изменение уровня звукового давления на 1 дБ является минимальной, различаемой человеческим слухом величиной изменения громкости.

Следует отметить, что в акустике при частотном анализе сигналов используют стандартизированные частотные полосы шириной в 1 октаву, 1/3 октавы, 1/12 октавы. Октава – это полоса частот, у которой верхняя граничная частота в два раза больше нижней граничной частоты:

$$\Delta f = f_в - f_н = 1 \text{ окт, если } f_в = 2f_н .$$

## 7.2. Основные акустические параметры речевых сигналов

Основные звуки речи образуются следующим образом [6]:

- гласные образуются при прохождении воздуха через голосовые связки. Акустические колебания гласных звуков носят периодический, близкий к гармоническому характер и могут изменяться в значительном частотном диапазоне;

- глухие согласные (сонорные, щелевые, взрывные) образуются за счет преодоления воздухом препятствий в носовой и ротовой полостях и носят характер, как отдельных акустических импульсов, так и шумовых сигналов со сплошным спектром различной конфигурации;
- звонкие согласные образуются также как глухие, но при участии голосовых связок.

Таким образом, речевой сигнал представляет собой сложный частотно и амплитудно модулированный шумовой процесс, характеризующийся следующими основными статистическими параметрами:

- частотный диапазон;
- уровень речевых сигналов;
- динамический диапазон.

**Частотный диапазон** речи лежит в пределах 70...7000 Гц. Энергия акустических колебаний в пределах указанного диапазона распределена неравномерно. На рис. 7.1 (кривая 1) представлен вид среднестатистического спектра русской речи. Следует отметить, что порядка 95 % энергии речевого сигнала лежит в диапазоне 175...5600 Гц

Важно отметить, что информативная насыщенность отдельных участков спектра речи неравномерна. Кривой 2 на рис 7.1 представлен вклад отдельных участков спектра речи в суммарную разборчивость $S_{сл}$.

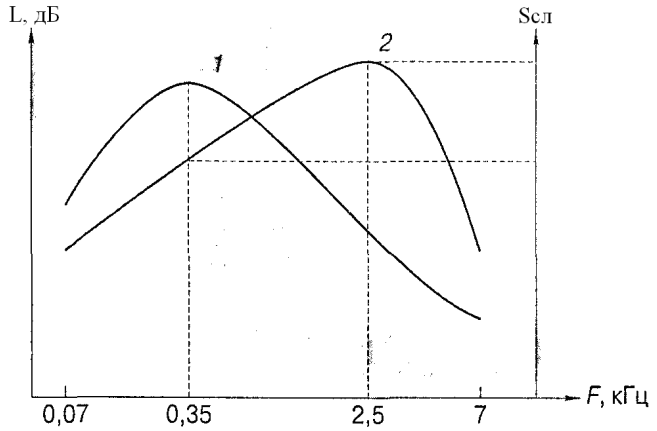



Рис. 7.1

**Уровни речевых сигналов.** В различных условиях человек обменивается устной информацией с различным уровнем громкости, при этом выделяют следующие уровни звукового давления:

- тихий шепот – 35...40 дБ;
- спокойная беседа – 55...60 дБ;
- выступление в аудитории без микрофона – 65...70 дБ.

**Динамический диапазон.** Уровень речи в процессе озвучивания одного сообщения может меняться в значительных пределах. Разность между максимальными и минимальными уровнями для различных видов речи составляет:

- дикторская речь – 25...35 дБ;
- телефонные переговоры – 35...45 дБ;
- драматическая речь – 45...55 дБ.

## 7.3. Распространение акустических сигналов в помещениях и строительных конструкциях

При своем распространении звуковая волна, доходя до какой-либо преграды (границы двух сред) и взаимодействуя с ней, частично отражается от нее, а частично продолжает распространяться по преграде. Количество акустической энергии Е, прошедшей из одной среды в другую, зависит от свойств этих сред (рис. 7.2).

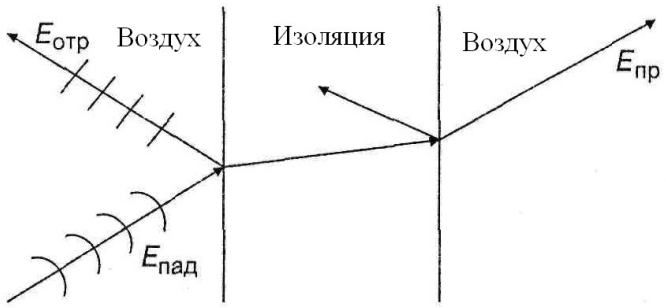



Рис. 7.2. Распространение акустической волны

В строительной акустике используются следующие основные понятия:

$$\alpha = \frac{E_{пад} - E_{отр}}{E_{пад}}$$ – коэффициент поглощения;

$$\beta = \frac{E_{отр}}{E_{пад}}$$ – коэффициент отражения;

$$\gamma = \frac{E_{пр}}{E_{пад}}$$ – коэффициент звукопроницаемости;

$$Q[дБ] = 10 \cdot \lg \frac{E_{пад}}{E_{пр}}$$ – звукоизоляция.

В таблице 7.1 приведены характеристики звукоизоляции основных строительных конструкций.

Таблица 7.1

| Тип строительной конструкции | Центральные частоты октавных полос, Гц | | | | |
|---|---|---|---|---|---|
| | 250 | 500 | 1000 | 2000 | 4000 |
| Оштукатуренная кирпичная стена толщиной 270 мм | 44 | 51 | 58 | 64 | 65 |
| Железобетонная стена толщиной 100 мм | 40 | 44 | 50 | 55 | 60 |
| Гипсобетонная перегородка толщиной 80 мм | 33 | 37 | 39 | 44 | 44 |
| Перегородка ДСП толщиной 20 мм | 26 | 26 | 26 | 26 | 26 |

## 7.4. Каналы утечки речевой информации

В случае, когда источником информации является голосовой аппарат человека, информация называется речевой.

Речевой сигнал – сложный акустический сигнал, основная энергия которого сосредоточена в диапазоне частот от 300 до 4000 Гц.

Голосовой аппарат человека является первичным источником акустических колебаний, которые представляют собой возмущения воздушной среды в виде волн сжатия и растяжения (продольных волн).

Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания. Таким образом, в своем первоначальном состоянии речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний.

Различного рода преобразователи акустических и вибрационных колебаний являются вторичными источниками. К последним относятся: громкоговорители, телефоны, микрофоны, акселерометры и другие устройства.

В зависимости от среды распространения речевых сигналов и способов их перехвата технические каналы утечки информации можно разделить на:

- акустические,
- вибрационные,
- акустоэлектрические,
- оптоэлектронные
- параметрические**.**

**Акустические каналы.**

В акустических каналах утечки информации средой распространения речевых сигналов является воздух, и для их перехвата используются высокочувствительные микрофоны и специальные направленные микрофоны, которые соединяются с портативными звукозаписывающими устройствами или со специальными миниатюрными передатчиками.

Автономные устройства, конструктивно объединяющие микрофоны и передатчики, называют **закладными устройствами** (ЗУ) перехвата речевой информации.

Перехваченная ЗУ речевая информация может передаваться по радиоканалу, сети электропитания, оптическому (ИК) каналу, соединительным линиям систем пожарной и охранной сигнализации, посторонним проводникам, инженерным коммуникациям в ультразвуковом диапазоне частот, телефонной линии с вызовом от внешнего телефонного абонента.

Прием информации, передаваемой закладными устройствами, осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн.

Использование портативных диктофонов и закладных устройств требует проникновения в контролируемое помещение. В том случае, когда это не уда-

ется, для перехвата речевой информации используются направленные микрофоны.

**Виброакустические каналы.**

В виброакустических каналах утечки информации средой распространения речевых сигналов являются ограждающие строительные конструкции помещений (стены, потолки, полы) и инженерные коммуникации (трубы водоснабжения, отопления, вентиляции и т.п.). Для перехвата речевых сигналов в этом случае используются вибродатчики (акселерометры).

Вибродатчик, соединенный с электронным усилителем называют электронным стетоскопом. Электронный стетоскоп позволяет осуществлять прослушивание речи с помощью головных телефонов и ее запись на диктофон.

По виброакустическому каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал, поэтому таки устройства часто называют радиостетоскопами. Возможно использование закладных устройств с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (по инженерным коммуникациям).

**Акустоэлектрические каналы.**

Акустоэлектрические каналы утечки информации возникают за счет преобразований акустических сигналов в электрические.

Некоторые элементы технических систем, в том числе трансформаторы, катушки индуктивности, электромагниты вторичных электрочасов, звонков телефонных аппаратов и т.п., обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС), либо к модуляции токов, протекающих по этим элементам в соответствии с изменениями воздействующего акустического поля.

Технические системы, кроме указанных элементов, могут содержать непосредственно акустоэлектрические преобразователи. К ним относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и т.д. Эффект акустоэлектрического преобразования в специальной литературе называют «микрофонным эффектом». Наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители и некоторые датчики пожарной сигнализации.

Перехват акустоэлектрических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям технических систем специальных высокочувствительных низкочастотных усилителей. Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты.

Технический канал утечки информации с использованием «высокочастотного навязывания» может быть осуществлен путем несанкционированного контактного введения токов высокой частоты от соответствующего генера-

тора в линии, имеющей функциональные связи с нелинейными или параметрическими элементами технических систем, на которых происходит модуляция высокочастотного сигнала информационным. Информационный сигнал в данных элементах появляется вследствие акустоэлектрического преобразования акустических сигналов в электрические. Промоделированный сигнал отражается от указанных элементов и распространяется в обратном направлении по линии или излучается.

Наиболее часто такой канал используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны.

**Оптико-электронный (лазерный) канал.**

Оптико-электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих под действием акустического речевого сигнала отражающих поверхностей помещений (оконных стекол, зеркал и т.д.). Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация.

Для организации такого канала предпочтительным является использование зеркального отражения лазерного луча. Однако при небольших расстояниях до отражающих поверхностей (порядка нескольких десятков метров) может быть использовано диффузное отражение лазерного излучения.

Для перехвата речевой информации по данному каналу используются сложные лазерные системы, которые в литературе часто называют «лазерными микрофонами». Работают они, как правило, в ближнем инфракрасном диапазоне длин волн.

**Параметрические каналы.**

В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов технических средств приема информации. При этом изменяется взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом. Поэтому этот канал утечки информации называется параметрическим. Наиболее часто наблюдается паразитная модуляция информационным сигналом излучений гетеродинов радиоприемных и телевизионных устройств, находящихся в помещениях, где ведутся конфиденциальные разговоры.

Параметрический канал утечки информации может быть реализован и путем «высокочастотного облучения» помещения, где установлены закладные устройства, имеющие элементы, параметры которых (например, добротность и резонансная частота объемного резонатора) изменяются под действием акустического (речевого) сигнала.

При облучении помещения мощным высокочастотным сигналом в таком закладном устройстве при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором) происходит образование вторичных радиоволн, т.е. переизлуче-

ние электромагнитного поля. А специальное устройство закладки (например, объемный резонатор) обеспечивает амплитудную, фазовую или частотную модуляцию переотраженного сигнала по закону изменения речевого сигнала.

Для реализации возможностей такого канала необходимы специальный передатчик с направленным излучением и приемник.

Рассмотрим чуть подробнее **акустические и виброакустические каналы утечки речевой информации**

На рис. 7.3 представлены основные варианты возможной утечки речевой информации из объемов, выделенных помещений. Все их можно объединить в две группы:

- это акустические каналы (обозначены буквами а, б, в), т.е. такие каналы, по которым информация может быть перехвачена с помощью микрофонов воздушной проводимости или прослушана непосредственно человеком;
- виброакустические каналы (обозначены буквами г, д, е), т.е. каналы, по которым информация может быть зафиксирована с помощью микрофонов твердой среды (виброметров, акселерометров).

Наибольшую опасность представляют технологические окна и каналы с большой площадью поперечного сечения, такие как короба коммуникаций и воздуховоды вентиляции. Эти объекты являются, по сути, акустическими волноводами, и звуковые колебания могут распространяться по ним на значительные расстояния. Так, если поперечные размеры короба сравнимы с длиной звуковых волн, затухание при распространении по нему звука составляет 5 = 0,01... 1 дБ/м и зависит от размеров короба, материала стенок и пр.

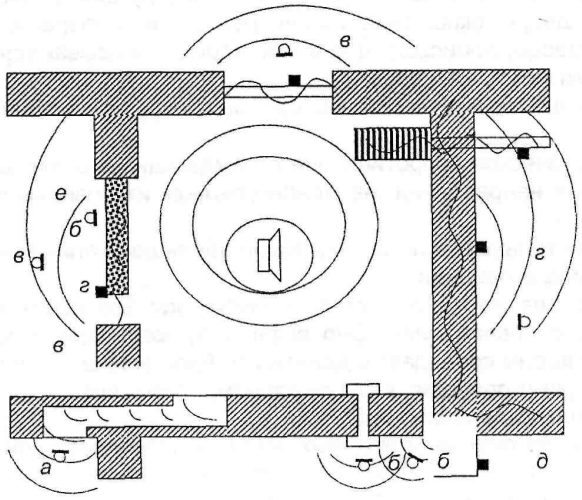



**Рис. 7.3**

Следующими по степени опасности являются звуководы с размерами значительно меньше длины звуковых волн. Таковыми могут быть отверстия электропроводки, щели и трещины в строительных конструкциях, неплотности дверных и оконных проемов. Затухание звука в таких каналах весьма значительно 5 = 1.. .20 дБ/м. Оно определяется вязкостью воздуха и зависит от поперечных размеров отверстий, шероховатости поверхности и продольной конфигурации отверстия.

Несмотря на заметную величину затухания, этого абсолютно недостаточно для обеспечения защиты информации. Так, если в стене толщиной 0,5 м имеется трещина с площадью поперечного сечения 5 мм$^2$ и длиной 0,75 м, звукоизоляция в области выхода этой трещины на поверхность будет составлять 18 дБ, в то время как при отсутствии трещины такая стена может обеспечить звукоизоляцию более 65 дБ.,

Звуковые колебания могут распространяться за пределы выделенного помещения не только за счет тех или иных воздушных каналов, но и за счет переизлучения колебаний ограждающими строительными конструкциями.

Переизлучение звука за пределы выделенного помещения происходит за счет колебаний строительных конструкций, вызванных падающими на них звуковыми волнами. Так как толщина подавляющего большинства строительных конструкций (стены, полы, потолки, двери, окна) значительно меньше их поперечных размеров, процессы, происходящие в них, хорошо описываются теорией колебания мембран и пластин.

Основные практические выводы, вытекающие из данных положений:

- акустическое сопротивление ограждающих строительных конструкций в направлении, перпендикулярном их поверхности невелико;
- строительные конструкции имеют большое количество собственных мод колебаний.

Последнее явление в строительной акустике носит название «волнового совпадения». Оно возникает, когда длина падающей звуковой волны совпадает с длиной изгибной волны в строительной конструкции и приводит к значительному снижению звукоизоляции.

Так как за счет многократных переотражений звуковой волны в помещении равновероятны любые углы падений, возбуждаются все собственные моды колебаний строительных конструкций, что приводит к существенному снижению звукоизоляции.

Как только что было показано, строительные конструкции совершают значительные колебания под воздействием акустических волн. Чтобы перехватить информацию, переносимую этими колебаниями, не обязательно регистрировать акустические колебания, переизлученные этими конструкциями, достаточно зафиксировать колебания собственно строительных конструкций. Так, например, под воздействием звука $P_{ак}$ = 70 дБ кирпичная стена толщиной 0,5 м совершает вибрационные колебания с ускорением $\alpha = 3 \cdot 10^{-5} g$. При таких условиях современными средствами может быть прослушан даже шепот. При этом переизлученный акустический сигнал будет < 10 дБ, что практически исключает возможность съема информации. Таким образом, вибрационные колебания ограждающих конструкций под воздействием звуковых волн образуют один из наиболее опасных виброакустических каналов утечки информации.

Современные строительные материалы и конструкции (монолитный железобетон, сборные железобетонные конструкции, кирпичная кладка) обладают весьма низкими показателями затухания механических колебаний в области звуковых частот. Это обеспечивает возможность распространения колеба-

ний на значительные расстояния и создает возможность перехвата информации, регистрируя вибрации не только ограждающих конструкций выделенного помещения, но и регистрируя колебания значительно удаленных (1-3 стыка) элементов здания. Например, существует реальная возможность перехвата информации по несущей стене из выделенного помещения, расположенного через 1…2 этажа от места установки аппаратуры съема информации.

В общем случае, в зависимости от конструкции здания и качества выполнения стыков между его элементами, затухание на стыках варьируется в пределах от 1…3 дБ до 10…15 дБ. Отсюда следует важная тактическая особенность и повышенная опасность виброакустического канала утечки информации – перехват информации возможен не только из смежных помещений, но и из помещений, значительно удаленных от источника информации.

Некоторые элементы строительных конструкций, как и в случае рассмотрения акустического канала, представляют собой волноводы вибрационных колебаний. К ним относятся трубы различных коммуникаций (отопления, водоснабжения, электропитания и пр.). Как и в случае воздушных волноводов, значительная разница в величинах акустического сопротивления материала труб и окружающей среды составляет 4…8 раз.

Создаются условия волноводного распространения сигналов на значительные расстояния. Данный канал становится особенно опасным, если трубопровод соединен с какой-то жесткой и развитой поверхностью, которая играет роль согласующего элемента при передаче энергии из воздуха в трубопровод. Таким согласующим элементом, например, являются современные легкие радиаторы отопления.

## 7.5. Технические средства подслушивания: акустические приемники; диктофоны; закладные устройства

**Акустические приемники.** Непосредственное (ушами) подслушивание ограничено малым расстоянием от источника звука – в лучшем случае около десяти метров. Малая дальность непосредственного подслушивания обусловлена не только малой мощностью акустических сигналов и большим затуханием их в среде распространения, но и тем, что уши человека имеют широкую диаграмму направленности (близкую к 180°), в силу чего на барабанную перепонку поступают практически все внешние акустические шумы.

Кроме того, шумы поднимают порог чувствительности слуховой системы человека. Но одновременно это физиологическое свойство слуховой системы человека позволяет ему адаптироваться к зашумленности среды обитания, например в жилых помещениях возле транспортных магистралей большого города.

Для непосредственного подслушивания в условиях города злоумышленнику необходимо приблизиться к источнику информации на несколько метров, что существенно ухудшает скрытность добывания информации.

Технические средства подслушивания расширяют и дополняют возможности слуховой системы человека за счет:

- приема и прослушивания акустических сигналов, распространяющихся в воде и твердых телах;
- повышения дальности подслушивания речевой информации по сравнению с непосредственным подслушиванием;
- коррекции спектра акустического сигнала, распространяющегося в среде с неравномерной амплитудно-частотной характеристикой коэффициента передачи или затухания;
- выделения акустического сигнала из смеси его и шумов;
- прослушивания речи, выделяемой из перехваченных радио сигналов и электрических сигналов функциональных каналов связи и из сигналов побочных излучений и наводок;
- ретрансляции добываемой речевой информации на сколь угодно большое расстояние.

Конкретный способ подслушивания реализуется с использованием соответствующих технических средств. Совокупность технических средств, обеспечивающих функции добывания семантической и признаковой акустической информации, представляет собой комплекс средств подслушивания.

Структурная схема типового комплекса средств подслушивания приведена на рис. 7.4.

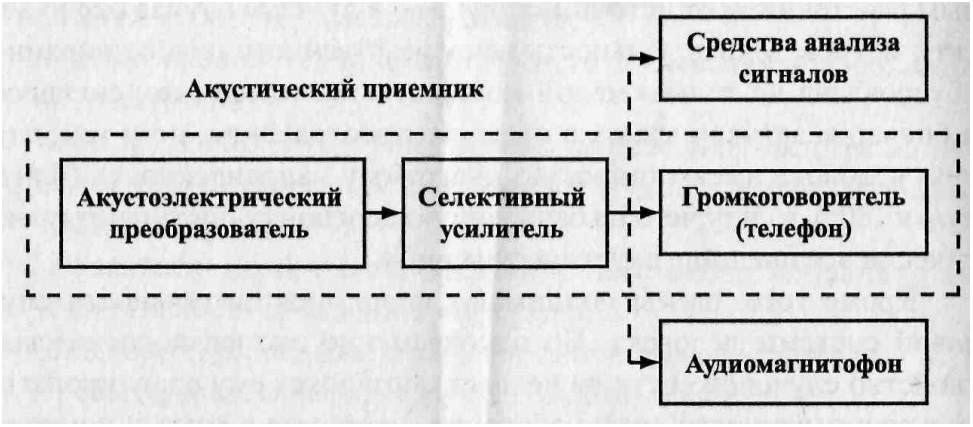



Рис. 7.4

Основной частью комплекса является акустический приемник. Он производит селекцию по пространству и частоте акустических сигналов, распространяющихся в атмосфере, воде, твердых телах, преобразует их в электрические сигналы, усиливает и обрабатывает электрические сигналы и преобразует их в акустическую волну для обеспечения восприятия информации слуховой системой человека. Акустический приемник содержит акустоэлектрический преобразователь, селективный усилитель и электроакустический преобразователь (телефон, громкоговоритель).

Акустические приемники для приема акустической волны, распространяющейся в воздухе, воде, твердой среде (в инженерных конструкциях), в грунте, отличаются видом акустоэлектрического преобразователя. Иногда по виду акустоэлектрического преобразователя называют весь акустический приемник. Акустоэлектрический преобразователь акустической волны, рас-

пространяющейся в воздухе, называется **микрофоном**, преобразователь волны, распространяющейся в твердой среде, – **стетоскопом** и **акселерометром**, в земной поверхности – **геофоном**, а в воде – **гидрофоном**. Основную долю функциональных акустоэлектрических преобразователей акустических приемников составляют микрофоны.

Так как электрические сигналы на выходе акустоэлектрических преобразователей крайне малы и могут принимать значения единиц мкВ, то для их усиления до необходимых для последующего применения величин (единиц В) используется селективный усилитель. Его селективность обеспечивается регулируемой полосой пропускания, необходимой для устранения помех на частотах вне спектра акустического сигнала. Учитывая, что затухание среды распространения акустического сигнала увеличивается с повышением его частоты, коэффициент усиления селективного усилителя соответственно повышают для более высоких спектральных составляющих принимаемого сигнала. Такая компенсация эквивалентна повышению уровня акустического сигнала в точке приема до 6 дБ.

Электрический сигнал преобразуют в акустический сигнал, воспринимаемый человеком, **громкоговорители и телефоны**. По способу преобразования электрических сигналов громкоговорители разделяются на электродинамические, электромагнитные, электростатические, пьезоэлектрические и др., по виду излучения – на громкоговорители непосредственного излучения, диффузорные и рупорные, по воспроизводимому диапазону частот – на широкополосные, низкочастотные, средне- и высокочастотные. Значения мощности громкоговорителей образуют стандартный ряд в диапазоне 0,1-50 Вт.

Чем уже диапазон частот динамической головки громкоговорителя, тем равномернее ее амплитудно-частотная характеристика, тем меньше головка искажает сигнал. Для высококачественной электроакустической аппаратуры к выходу усилителя подключают несколько динамических головок с разными диапазонами частот, перекрывающими весь звуковой диапазон (16-20000 Гц). Для воспроизводства речи средствами добывания требования к электродинамическим головкам более чем скромные: единицы Вт по мощности и по диапазону частот, соответствующему стандартному телефонному каналу (300-3400 Гц).

Для консервации акустической информации электрический сигнал с выхода акустического приемника подается на аудиомагнитофон. Для записи акустических сигналов применяют многоканальные стационарные ленточные магнитофоны, портативные лентопротяжные кассетные магнитофоны и специальные носимые лентопротяжные и цифровые диктофоны.

Сигнальные демаскирующие признаки определяются с помощью **средств технического анализа**. Если акустический сигнал на выходе приемника сильно зашумлен, то его электрический аналог подвергают для снижения уровня шума дополнительной обработке. Основу методов очистки электрического сигнала от шума составляют методы адаптивной фильтрации. Суть адаптивной фильтрации состоит в том, что на основе анализа поступающего на вход фильтра зашумленного речевого сигнала непрерывно фильтром

линейного предсказания «предсказывается» помеховый сигнал, который вычитается затем из смеси речевого сигнала и шума. В результате этого отношение сигнал/шум на выходе фильтра увеличивается.

Возможности акустического приемника характеризуются набором показателей:

- диапазоном частот принимаемого акустического сигнала;
- чувствительностью;
- динамическим диапазоном;
- массогабаритными характеристиками.

Так как речь является основным видом информации при подслушивании, то большинство акустических приемников для добывания информации работают в речевом диапазоне частот. В отдельных случаях ценной является информация, переносимая акустической волной в инфразвуковом и ультразвуковом диапазонах. К такой информации относятся звуки движущихся объектов (людей, техники, подводных и надводных кораблей и др.), акустические сигналы взрывов новых боеприпасов, разрабатываемых работающих двигателей и других объектов разведки.

Дальность подслушивания (длина простого акустического канала утечки информации) зависит от ряда факторов, в том числе от чувствительности акустического приемника. Под его чувствительностью понимается минимальная энергия акустической волны или оказываемое ею минимальное давление, при котором обеспечивается определенный уровень электрического или акустического сигналов на выходе акустического приемника.

Динамический диапазон акустического приемника характеризуется диапазоном в дБ мощности акустического сигнала на его входе (громкости звука), при котором обеспечивается требуемый или допустимый уровень сигнала на выходе акустического приемника. Учитывая, что акустический приемник при добывании информации размещается скрытно, далеко не в оптимальных условиях, его динамический диапазон является важнейшей характеристикой акустического приемника. Например, если динамический диапазон закладного подслушивающего устройства мал, то приемлемое качество добываемой речевой информации обеспечивается лишь в небольшом интервале расстояний от микрофона говорящего человека. Когда разговаривающий человек ходит по комнате, то добываемая информация может содержать участки с плохим качеством речи.

Так как акустические каналы утечки информации имеют малую протяженность и акустический приемник необходимо приблизить к источнику акустического сигнала, то большинство акустических приемников относятся к классу носимой аппаратуры с автономными источниками питания. Поэтому важное значение для практического применения акустического приемника имеют его вес и габариты, а также длительность непрерывной работы.

Для запоминания (записи) добываемой информации сигнал с выхода передается по организуемому каналу связи к запоминающему устройству или записывается в запоминающем устройстве, размещенном в месте нахождения акустического приемника. В последнем варианте к запоминающему устрой-

ству предъявляются такие же жесткие требования, как к акустическому приемнику.

Для записи речевой информации широко применяются специальные диктофоны, конструктивно объединяющие акустический приемник и запоминающее устройство (лентопротяжный и цифровой магнитофоны). Основными характеристиками запоминающих устройств являются объем памяти в МБайтах, время записи речевой информации в минутах или часах, время непрерывной работы в часах.

**Средства технического анализа** измеряют технические характеристики (сигнальные признаки) акустических сигналов, которые могут использоваться для обнаружения и распознавания их источников: частоту колебаний, характеристики спектра, амплитуду и мощность сигнала и др. Каждый объект с движущимися механическими частями имеет индивидуальную сигнальную признаковую структуру, по которой с достаточно высокой вероятностью можно обнаружить объект и распознать его отдельные свойства. Средства анализа акустических сигналов устанавливаются, например, на подводных лодках для обнаружения и распознавания типов (вплоть до номера) надводных и подводных кораблей.

**Диктофоны.** Для скрытого подслушивания речевой информации и ее регистрации широко применяются диктофоны с встроенными и вынесенными микрофонами. Скрытая запись информации производится с целью:

- «документирования» беседы или телефонного разговора для экономии времени при составлении отчета или для последующего анализа разговора;
- регистрации трудно запоминаемой во время разговора информации;
- использования записи для оказания влияния на собеседника или предоставления ее в качестве доказательства каких-либо его обещаний и высказываний, сбора материалов о конкурентах, злоумышленниках и др.;
- получения голосового образца собеседника для последующей идентификации при подслушивании;
- регистрации собственных предложений для их последующего анализа;
- записи разговора в помещении во время отсутствия владельца диктофона.

Диктофоны по принципам работы делятся на кинематические (с лентопротяжным механизмом для обеспечения записи на магнитную ленту или металлическую проволоку) и цифровые.

Кинематические диктофоны для скрытного подслушивания отличаются от бытовых или профессиональных (используемых журналистами) демаскирующими признаками с пониженной информативностью и возможностью скрытного управления режимами работы.

Запись речи в диктофонах производится на микрокассете со скоростью 2,4 или 1,2 см/с, длительность записи в зависимости от скорости и типа кассеты составляет от 15 мин до 3 часов.

Металлические корпуса диктофона и дополнительного кожуха-экрана существенно ослабляют электромагнитное излучение коллекторного двигателя, но не исключают его обнаружение на небольшом удалении в десятки см.

В цифровых диктофонах лентопротяжный механизм отсутствует, а запись речевой информации производится в цифровой форме на полупроводниковых запоминающих устройствах. Отсутствие в цифровых диктофонах лентопротяжного механизма исключает акустические шумы, но в качестве его демаскирующего признака проявляются высокочастотные излучения, создаваемые импульсами тактовой частоты аналого-цифрового преобразователя и полупроводниковой памяти.

**Закладные устройства.** Радиоэлектронные закладные устройства представляют собой организованный канал несанкционированного получения и передачи в пункт приема аудио и визуальной информации, а также информации передаваемой по сетям связи.

Закладные устройства можно классифицировать по нескольким признакам:

- радиозакладные устройства, излучающие в эфир;
- закладные устройства, не излучающие в эфир (с передачей перехваченной информации по сетям связи, управления, питания и т.д.);
- радиозакладные устройства с переизлучением;
- закладные устройства с передачей перехваченной информации по стандартному телефонному каналу.

В первую группу входят радиозакладные устройства, предназначенные для получения аудиоинформации по акустике помещения, телевизионные закладные устройства, предназначенные для получения аудио - и визуальной информации, и радиозакладные устройства в телефонных линиях связи, устройствах обработки и передачи информации, сетях питания и управления. Передача перехваченной информации происходит радио- или телевизионным радиосигналом.

К закладным устройствам с передачей информации без излучения в эфир можно отнести группу закладных устройств в линиях связи, питания, управления и охранной сигнализации с использованием этих линий связи для передачи перехваченной информации.

В ряде закладных устройств передача перехваченной информации осуществляется по стандартному телефонному каналу. Это так называемые закладки типа «длинное ухо», «с искусственно поднятой трубкой».

Существует целая группа закладных устройств, обеспечивающих получение информации по акустике помещения за счет модуляции акустическим сигналом отраженного микроволнового или ИК-сигналов от элементов, на которые воздействует акустический сигнал. Это могут быть: стекла, окна, различные перегородки, резонаторы, специальные схемы и т. д.

Проявление рассмотренных выше групп закладных устройств при их передаче перехваченной информации различно, т.к. они могут проявляться в радиодиапазоне, как радиоизлучения с различными видами модуляции или кодирования, в ИК-диапазоне, как низкочастотные излучения в линиях связи,

управления, питания, в стандартных телефонных каналах или в виде облучающих сигналов.

В зависимости от предназначения закладных устройств выделяется, прежде всего, «зона несанкционированного получения информации». Это может быть воздушное пространство (для воздушной акустической волны), несущие конструкции, трубы водопроводной или паровой сети для структурной акустической волны, элементы тракта обработки и передачи информации и т.п.

Один из ограничивающих моментов использования закладных устройств – гарантированная дальность перехвата информации. Эта дальность в ряде случаев является определяющей в организации поиска закладных устройств. Применительно к закладным устройствам, обеспечивающим перехват аудиоинформации, важна максимальная дальность перехвата либо воздушной, либо структурной волны датчиками съема подобной информации. В качестве таких датчиков используются микрофоны, стетоскопы или геофоны. Возможная дальность перехвата аудиоинформации, разговоров, передаваемых воздушной волной в пределах 10 м, структурной волной – через кирпичные и бетонные стены – 0,8…1,0 м и сейсмической волны – до 10 м при малых акустических шумах (до 5 м при средних акустических шумах).

**Радиозакладные устройства**

Перехваченная информация может быть передана по воздуху (радиозакладки), по сетям питания, управления, связи (закладные устройства).

Для выявления излучающих в эфир радиозакладок необходимо определить возможный диапазон их работы и используемые виды модуляции и закрытия. Как следует из анализа существующих радиозакладных устройств, диапазон их работы достаточно широк и имеет тенденцию к продвижению в более высокие диапазоны, к использованию устройств с «прыгающими» частотами.

В настоящее время на специальные технические средства в России для радиозакладных устройств выделен диапазон частот 415...420 МГц. Однако в эксплуатации можно встретить большое количество радиозакладках диапазона 20…2000 МГц.

В радиозакладных устройствах в основном применяется модуляция несущей частоты передатчика, однако встречаются радиозакладные устройства с модуляцией сигнала промежуточной частоты или двойной модуляции. Прием таких сигналов на обычный супергетеродинный приемник невозможен (после детектирования прослушивается обычный шум). Для приема может быть использован только специальный приемник.

В процессе появления и развития радиозакладок на нашем рынке существенное изменение претерпели и виды модуляции, используемой в них. И хотя в наше время все еще широко используются радиозакладки с WFM (широкополосной) и NFM (узкополосной) модуляцией, появился принципиально новый класс радиозакладных устройств с дельта-модуляцией. Кроме того, в наиболее профессиональных радиозакладках используют такие сложные сиг-

налы, как шумоподобные или с псевдослучайной перестановкой несущей частоты.

При кодировании перехваченной информации часто применяется аналоговое скремблирование, изменяющее характеристики речевого сигнала таким образом, что он становится неразборчивым. В ряде закладок используется преобразование речевой информации в цифровой вид и наряду с преобразованием информации в цифровой вид используется ее шифрование.

В технических характеристиках ряда радиоприемных устройств поиска радиозакладок количество возможных, для гарантированного перехвата, видов модуляции и кодирования не перекрывает возможностей, заложенных в закладных устройствах. Это существенно усложняет поиск закладных устройств по их излучению, требует постоянной модернизации радиокомплексов для обеспечения поиска и перехвата, постоянно обновляемых и появляющихся новых видов модуляции и закрытия передаваемой перехваченной закладными устройствами информации.

Существенное значение для организации каналов передачи перехваченной информации в радиодиапазоне имеет используемая в закладном устройстве антенная система. В качестве таковой могут быть использованы: собственное антенное устройство случайная антенна.

Для противодействия перехвату излучений радиозакладных устройств в последних используется включение радиозакладки только на момент проведения переговоров в помещении, где установлена радиозакладка. Это может быть осуществлено путем включения в схему радиозакладки системы управления включения передатчика от голоса. В этом случае радиозакладка работает (при отсутствии источника акустического сигнала) в дежурном режиме как приемник акустического сигнала, что требует минимального потребления от источника питания. При появлении в помещении источника акустического сигнала система включает радиопередатчик, и закладка работает в полном режиме с передачей перехваченного акустического сигнала. Включение такой системы в состав радиозакладки позволяет повысить ее скрытность и увеличивает срок ее действия.

Для этих же целей может быть использована система дистанционного управления. Как правило, эта система используется для включения и выключения передатчика радиозакладки, а также для изменения режима работы передатчика, величины излучаемой мощности и параметров излучаемого сигнала.

Это довольно сложные системы, имеющие канал приема сигналов управления. В такой системе в дежурном режиме работает только радиоприемное устройство контроля управления, после подачи сигнала управления включается передающее устройство радиозакладки. Для передачи сигнала управления используется, как правило, УКВ диапазон, сигналы управления кодируются в целях избежания ложных срабатываний.

Еще одним способом повышения скрытности передаваемой радиозакладкой информации является использование промежуточного накопления перехваченной информации. В состав такого радиозакладного устройства

входит цифровой накопитель, передатчик для ускоренной передачи накопленной информации и канал управления работой радиозакладки. В подобной радиозакладке в течение нескольких часов (6...14 ч) накапливается перехватываемая информация, а затем в течение 7...14 мин передается в эфир. Естественно, что использование возможных способов сокрытия передаваемой информации существенно сказывается на требовании к радиоприемному устройству поиска закладных устройств по их излучению.

Радиозакладные устройства выполняются в виде технологических модулей или закамуфлированными в определенные устройства.

**Радиозакладные переизлучающие устройства.**

Первые сведения о радиозакладных устройствах с переизлучением относятся к середине 1940-х годов, когда в одном из патентов было описано устройство, в конструкцию которого был определенным образом включен четвертьволновый резонатор, настроенный на частоту 330 МГц (рис. 7.5).

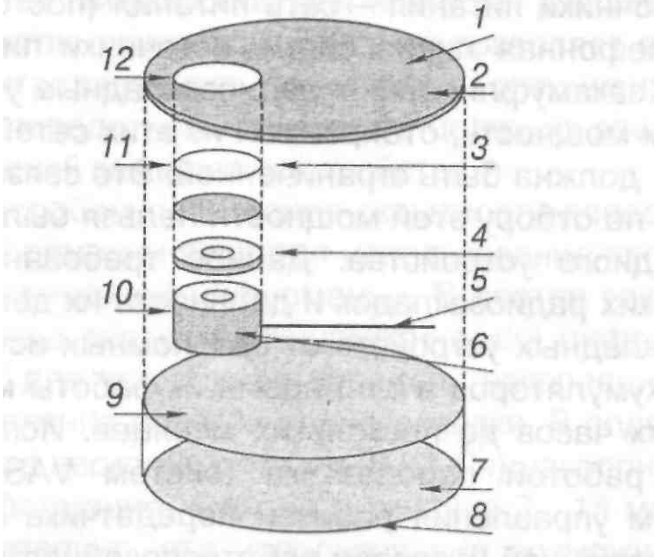



Рис. 7.5. Конструкция переизлучающей радиозакладки:

1 – крышка из диэлектрического материала;
2 – место стыковки с металлическим цилиндрическим стаканом;
3 – вставная крышка из ферритового материала;
4 – кольцо из изолятора;
5 – антенна (четвертьволновый вибратор на частоту 330 МГц);
6 – согласующий подстроечный конденсатор;
7 – специальная жидкость;
8 – стакан;
9 – слой маслянистой жидкости, реагирующей на звуковые колебания;
10 – металлический цилиндр (катушка индуктивности);
11 – металлический цилиндр;
12 – отверстие для установки резонатора с антенной

Оболочка резонатора «прозрачна» для волн УКВ диапазона и поэтому волна от внешнего источника этой частоты эффективно отражается от резонатора. С другой стороны, его расположение на слое маслянистой жидкости приводит к тому, что при возникновении акустического поля резонатор при-

ходит вместе с этим слоем в микроколебания, соответствующие акустическому (речевому) сигналу, и в такт с этими колебаниями изменяется добротность и резонансная частота резонатора.

Отраженный сигнал, таким образом, модулируется информационным акустическим сигналом и в месте приема может быть довольно легко выделен.

Промодулированный отраженный сигнал переизлучается в целях его маскировки на фоне более мощного облучающего сигнала, его частоту несколько сдвигают относительно частоты облучающего сигнала.

**Закладные устройства типа «длинное ухо».**

Отдельной по принципу работы является группа закладных устройств, относящаяся к закладкам типа «длинное (телефонное) ухо» или закладка «с искусственно поднятой трубкой». Последнее название достаточно точно определяет принцип работы этого типа закладного устройства.

При опущенной телефонной трубке на телефонную линию замкнута система вызова (механическая или электрическая), которую инициирует сигнал вызова. Когда абонент поднимает трубку, к линии подсоединяется телефонный аппарат и обеспечивается связь. Закладка с «искусственно поднятой трубкой» обеспечивает подсоединение телефонного аппарата и, следовательно, микрофона телефонной трубки (или дополнительного микрофона) к линии без механического подъема телефонной трубки.

Особенностью подобных закладных устройств является их большая дальность действия - практически по всему земному шару.

**Телефонные закладки.**

Телефонными закладками называются закладки, предназначенные для перехвата информации, передаваемой по телефонным линиям связи. Перехваченная информация может записываться на диктофоны или передаваться по радиоканалу с использованием микропередатчиков. Телефонные закладки так же, как и акустические, можно классифицировать по виду исполнения, месту установки, источнику питания, способу передачи информации и ее кодирования, способу управления и т.д.

Выполняются они или в виде отдельного модуля, или камуфлируются под элементы телефонного аппарата, например, телефонный или микрофонный капсюли, телефонный штекер или розетку и т.д. Телефонные закладки могут быть установлены последовательно в разрыв одного из телефонных проводов, параллельно или через индукционный датчик.

**Сетевые закладные устройства**

Электросеть здания и ее элементы могут быть использованы злоумышленником для установки и питания закладных устройств, а также передачи перехваченной информации. Проводные системы скрытого аудиоконтроля предназначены для негласного съема и передачи аудиоинформации по проводным линиям.

Закладные устройства, связанные с электросетью, могут быть условно разделены на две группы:

- закладные устройства, обеспечивающие контроль акустической информации помещения с передачей перехваченной информации по сети электропитания;
- радиозакладные устройства, обеспечивающие акустический контроль помещения с питанием от сети электропитания и передачей перехваченной информации по радиоканалу.

Одной из существенных особенностей подобных закладных устройств является неограниченное время их работы (пока есть сеть питания). Закамуфлированные под широко используемые в быту и работе такие приборы, как удлинители, тройники, настенные лампы и другие бытовые электроприборы, подобные закладные устройства довольно просто могут быть «внедрены» в интересующее помещение.

В подобных устройствах акустический канал микрофона выполняется как конструктивные зазоры устройства, в которые камуфлируется закладка.

Габариты устройств камуфляжа обеспечивают расположение передающих устройств и при необходимости антенных систем.

Все устройства камуфляжа сохраняют свое прямое предназначение. Включение закладных устройств обеспечивается, как правило, включением камуфлирующего устройства (удлинитель, тройник и т.п.) в сеть.

Однако для таких устройств существует ряд ограничений. Например, не рекомендуется использовать изделие для подключения приборов с большим потреблением электроэнергии (более 0,5 кВт), так как иначе может появиться сетевой фон в акустическом канале. Не рекомендуется устанавливать радиомикрофон вблизи источников акустических помех – холодильника, вентилятора, трансформатора, телевизора и т.п.

Для обеспечения большей скрытности закладных устройств используется дистанционное управление, позволяющее включать закладное устройство только на необходимое время.

С использованием сетевых закладок возможна передача информации на значительные расстояния (до 300..500 м) в пределах одного или нескольких зданий, питающихся от одной низковольтной шины трансформаторной подстанции. Несущая частота в сетевых закладках выбирается, как правило, в диапазоне 40...600 кГц. Но для передачи информации могут использоваться частоты и более высокого диапазона (например, 3…7 МГц). В этом случае принцип работы сетевой закладки мало чем отличается от принципа работы обычной радиозакладки, у которой в качестве антенны используется силовой провод. Для приема информации, передаваемой такой закладкой, не обязательно подключаться к силовой линии, достаточно поместит приемник вблизи нее.

**Электронные стетоскопы.**

Выше говорилось, что в виброакустических каналах утечки информации средой распространения речевых сигналов являются ограждающие строительные конструкции помещений (стены, потолки, полы). Для перехвата речевых сигналов в этом случае используются вибродатчики (акселерометры). Вибродатчик, соединенный с электронным усилителем называют электрон-

ным стетоскопом. Электронный стетоскоп позволяет осуществлять прослушивание речи с помощью головных телефонов и ее запись на диктофон.

Если доступ в контролируемое помещение невозможен, но не исключен доступ в соседние помещения, то для снятия информации могут использоваться радиостетоскопы. Тактика их применения аналогична применению обычных стетоскопов, но наличие радиоканала исключает необходимость присутствия агента или записывающей аппаратуры в момент снятия информации, что дает возможность скрытно устанавливать радиостетоскопы в небольших по размеру малодоступных местах. Способы установки радиостетоскопов приведены на рис. 7.6.

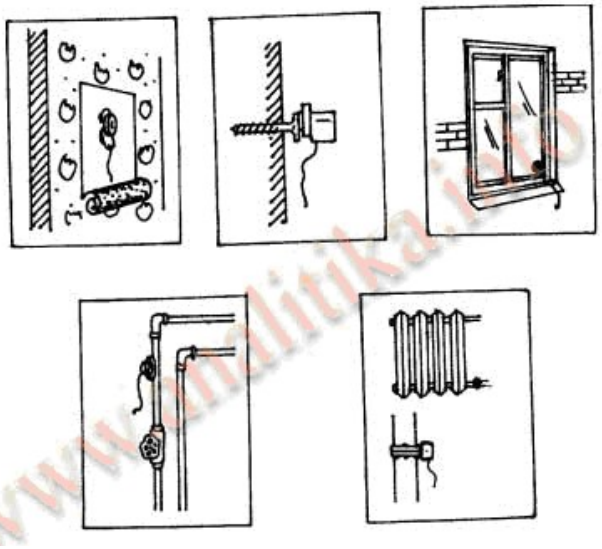


Рис. 7.6

Для съема информации с внешних оконных стекол могут использоваться сверхминиатюрные радиостетоскопы, обвалованные липкой резиновой массой и по внешнему виду напоминающие шарик или комочек грязи. Такой шарик путем броска приклеивается с наружной стороны окна и передает информацию в течение 1…2 дней. По их истечении резиновая масса высыхает, закладка отлипает от поверхности, на которой была прикреплена, и падает вниз. Для установки закладок в местах, физический доступ к которым невозможен, используются специальные бесшумные пистолеты (арбалеты), стреляющие “стрелами-радиозакладками”. Стрела с миниатюрной радиозакладкой, в ударостойчивом исполнении, надежно прикрепляется к поверхностям из любого материала: металла, дерева, пластмассы, стекла, камня, бетона и т.п. при выстреле с расстояния до 25 м.

# 8. МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ПОДСЛУШИВАНИЮ

Методы противодействия подслушиванию направлены, прежде всего, на предотвращение утечки информации в простом акустическом (гидроакустическом, сейсмическом) каналах. Кроме того, для повышения дальности подслушивания применяются составные каналы утечки информации, которые содержат наряду с простыми акустическими также радиоэлектронные (с использованием закладных устройств) и оптические (с лазерными средствами) каналы. Поэтому защита информации от подслушивания включает способы и средства блокирования любых каналов, с помощью которых производится утечка акустической информации.

В соответствии с общими методами защиты информации для защиты от подслушивания применяются следующие способы [2]:

1. Структурное скрытие, предусматривающее:
   - шифрование семантической речевой информации в функциональных каналах связи;
   - техническое закрытие электрических и радиосигналов в телефонных каналах связи;
2. Энергетическое скрытие путем:
   - звукоизоляции акустического сигнала;
   - зашумления помещения или твердой среды распространения другими звуками (шумами, помехами), обеспечивающими маскировку акустических сигналов;
3. Обнаружение, локализация и изъятие закладных устройств.

## 8.1. Структурное скрытие речевой информации в каналах связи

Так как передача речевой информации составляет основу телекоммуникации в человеческом обществе, то ее защита — важнейшая задача инженерно-технической защиты информации. Речевая информация, передаваемая по каналу связи, содержится в информационных параметрах электрических и радиосигналов. Сигналы распространяются по линиям связи в аналоговом и цифровом виде. В результате несанкционированного перехвата этих сигналов и их модуляции речевая информация может быть добыта злоумышленником.

Для структурного скрытия речевой информации в каналах связи применяют **шифрование** и **техническое закрытие.**

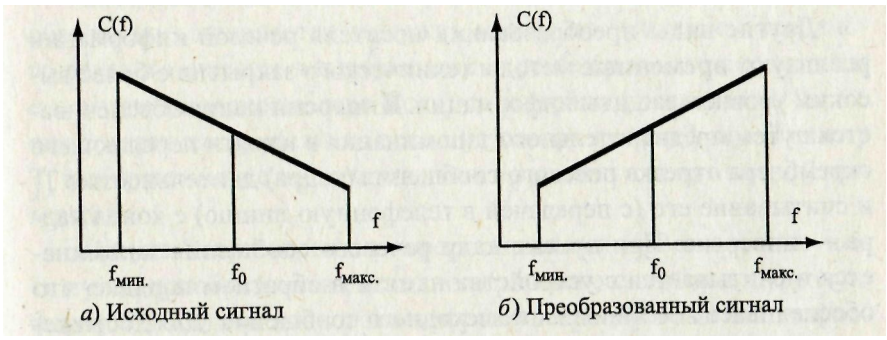
**Вопросы шифрования** рассматриваются в процессе изучения дисциплины «Криптографическая защита информации». Шифрование основано на следующем. Аналоговый речевой сигнал с выхода микрофона преобразуется с помощью аналогово-цифрового преобразователя в цифровой сигнал. При аналого-цифровом преобразовании амплитуда сигнала измеряется через равные промежутки времени, называемые шагом дискретизации. Для того чтобы цифровой речевой сигнал имел качество не хуже переданного по телефонному каналу в аналоговой форме, шаг дискретизации в соответствии с теоремой Котельникова не должен превышать 160 мкс, а количество уровней квантова-

ния амплитуды речевого сигнала — не менее 128. В этом случае один отсчет амплитуды кодируется 7 битами. Такой вид модуляции сигнала называется импульсно-кодовой комбинацией (ИКМ) и требует скорости передачи 48-64 кбит/с, существенно превышающей пропускную способность стандартного телефонного канала связи. Шифрование речевой информации в цифровой форме производится известными методами (заменой, перестановками и так далее).

Хотя развитие связи характеризуется постепенной заменой аналоговой техники на цифровую, менее дорогая аналоговая связь, особенно телефонная проводная, еще длительное время будет одним из основных видов связи. Но стандартный телефонный канал имеет узкую полосу пропускания в 3 кГц, недостаточную для передачи с высоким качеством шифрованного цифрового сигнала.

Скрытие речевого сигнала в узкополосном телефонном канале осуществляется методами **технического** или **аналогового закрытия.** По названию технических средств, обеспечивающих техническое закрытие, эти методы называются также **скремблированием** (перемешиванием). Техническое закрытие (скремблирование) отличается от криптографического тем, что при шифровании происходит скрытие речевого сообщения в символьной форме, а при техническом закрытии — скрытие речевого сигнала без преобразования его в цифровую форму. При техническом закрытии изменяются признаки (характеристики) исходного речевого сигнала таким образом, что он становится похож на шум, но занимает туже частотную полосу. Это позволяет передавать скремблированные сигналы по обычным стандартным телефонным каналам связи.

По виду преобразования сигнала различают **частотные и временные** методы технического закрытия. Наиболее простыми способами являются частотная и временная инверсии**.** В скремблере, осуществляющем инверсию спектра и называемом также **маскиратором,** осуществляется поворот спектра речевого сигнала вокруг некоторой центральной частоты $f_0$ (рис. 8.1).



*а*) Исходный сигнал *б*) Преобразованный сигнал

Рис. 8.1. Принципы инверсии частотного спектра речевого сигнала

Речевой сигнал с инверсным спектром передается по телефонному каналу связи. На приемной стороне осуществляется обратная процедура, восстанавливающая исходный спектр речевого сигнала. Неподготовленный слушатель воспринимает инверсную речь как нечленораздельный набор звуков. Од-

нако после некоторой тренировки слуховой анализатор человека способен восстанавливать преобразованную речь и воспринимать на слух семантику речевого сообщения. Легко определяемый алгоритм преобразования спектра усложняют в коммутируемом маскираторе путем передачи части речевого сигнала без инверсии и с инверсией. Низкая стоимость маскираторов и их способность устойчиво работать в каналах связи плохого качества способствуют их достаточно широкому применению.

В скремблере, выполняющем **частотные перестановки,** спектр исходного речевого сигнала разделяется на несколько частотных полос равной или неравной ширины (в современных моделях число полос может достигать 10-15) и производится их перемешивание по некоторому алгоритму — ключу (рис. 8.2). При приеме спектр сигнала восстанавливается в результате обратных процедур.

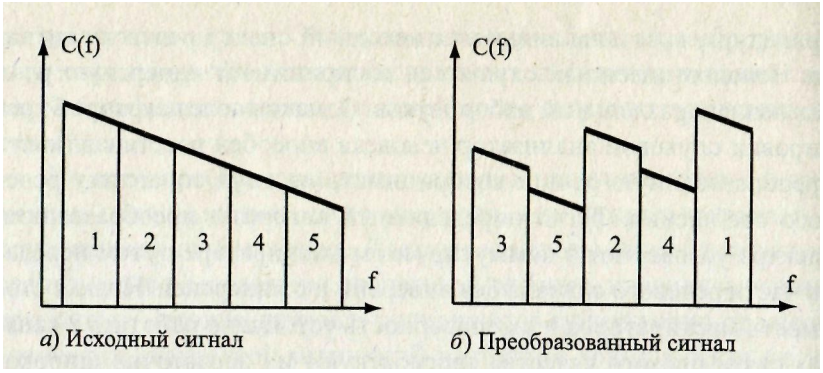



Рис. 8.2. Принципы частотной перестановки

Изменение ключа в ходе сеанса связи в скремблерах с динамическим закрытием позволяет повысить степень закрытия, но при этом требуется передача на приемную сторону сигналов синхронизации, соответствующих моментам смены ключа.

Другие виды преобразования носителя речевой информации реализуют **временные** методы технического закрытия с более высоким уровнем защиты информации. **Инверсия кадра** обеспечивается путем предварительного запоминания в памяти передающего скремблера отрезка речевого сообщения (кадра) длительностью $T_к$ и считывание его (с передачей в телефонную линию) с конца кадра — инверсно. При приеме кадр речевого сообщения запоминается и считывается с устройства памяти в обратном порядке, что обеспечивает восстановление исходного сообщения. Для достижения неразборчивости речи необходимо, чтобы продолжительность кадра была не менее 250 мс. В этом случае суммарная продолжительность запоминания и инверсной передачи кадра составляет примерно 500 мс, что может создать заметные задержки сигнала при телефонном разговоре.

В процессе технического закрытия с **временной перестановкой** кадр речевого сообщения делится на отрезки (сегменты) длительностью $\tau_c$ каждый. Последовательность передачи в линию сегментов определяется (правилом) ключом, который должен быть известей приемной стороне (рис. 8.3).

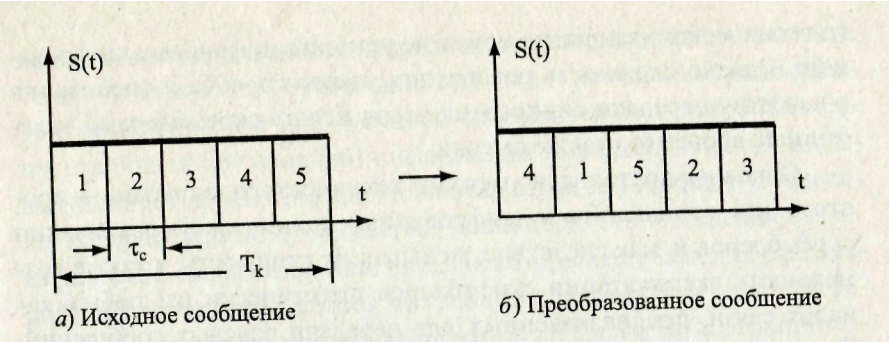



Рис. 8.3. Принципы временной перестановки

Изменением ключа в ходе сеанса связи в скремблерах с динамическим закрытием можно существенно повысить уровень защиты речевой информации. Остаточная разборчивость зависит от длительности кадра и с увеличением последнего уменьшается.

Вследствие накопления информации в блоке временного преобразования появляется задержка между поступлением исходного речевого сигнала в передающий скремблер и восстановлением его в приемном скремблере. Если эта задержка превышает 1-2 с, то она создает дискомфорт во время разговора по телефону. Поэтому $T_к$ выбирают менее этого предельного времени и делят на 4-16 сегментов.

Временные инверсия и перестановки технически реализуются путем преобразования исходного речевого сигнала в цифровую форму с помощью аналогово-цифрового преобразователя, цифровой обработки и обратного преобразования закрытого цифрового сигнала в аналоговый, который передается по телефонной линии связи. В приемной части скремблера выполняются с помощью элементов дискретной техники обратные преобразования: восстановление исходного сообщения и преобразование его из цифровой формы в аналоговую.

Используя комбинацию временного и частотного скремблирования, значительно повышают степень закрытия речи. В комбинированном (частотно-временном) скремблере исходное сообщение разделяется на кадры и сегменты, которые запоминаются в памяти скремблера. При формировании передаваемого сообщения производятся временные перестановки сегментов кадра и перестановки полос спектра речевого сигнала каждого сегмента, Если при этом обеспечить динамическое изменение ключа временной и частотной перестановки, то уровень защиты такого комбинированного технического закрытия может не уступать цифровому шифрованию. Однако сложность реализации такого способа и требования к качеству передачи синхроимпульсов между скремблерами телефонных абонентов также высоки.

Основное достоинство методов технического закрытия — простота (по отношению к шифрованию) технической реализации скремблеров и, как следствие, меньшая их стоимость, а также возможность эксплуатации скремблеров практически на любых каналах связи, предназначенных для передачи речевых сообщений. Основной недостаток методов технического закрытия — более низкая стойкость закрытия информации. Кроме того, скремблеры, за

исключением простейшего (с частотной инверсией), вносят искажения в восстановленный речевой сигнал. Их появление вызвано тем, что искажаются границы частотных полос и временных сегментов при обратном преобразовании сигнала на приемной стороне, что приводит к некоторому искажению спектра восстановленного речевого сигнала. Нежелательное влияние оказывают и групповые задержки составляющих речевого сигнала. Внесенные техническими средствами искажения приводят к снижению избыточности восстановленного речевого сигнала на (3-5)%.

Однако, несмотря на указанные недостатки, методы временного и частотного скремблирования, а также их различные комбинации позволяют обеспечить защиту информации на тактическом и на приближающемся к стратегическому уровнях защиты. Для технического восстановления речи требуется запись закрытого сообщения на аудиомагнитофон, длительная и трудоемкая работа с использованием дорогостоящей аппаратуры. Техническое закрытие в основном используется в коммерческих каналах связи для защиты конфиденциальной информации.

Основным достоинством систем цифрового шифрования речевого сигнала является высокая надежность закрытия информации, так как перехваченный сигнал представляет из себя случайную цифровую последовательность. Для восстановления из нее исходного сообщения необходимо знать криптосхему шифратора и устройство вокодера.

Недостатком устройств цифрового шифрования речи являются необходимость использования модемов, техническая сложность и относительно большие габариты шифраторов, неустойчивая работа устройств в каналах с большим затуханием сигнала и с высоким уровнем помех.

Под **тактическим** (низким или закрытием с временной стойкостью) понимается уровень, обеспечивающий защиту информации от подслушивания посторонними лицами в течение от минут до нескольких дней. Для дешифрования перехваченных сообщений **со стратегическим** (высоким, с гарантированной стойкостью) уровнем защиты информации высококвалифицированному, технически хорошо оснащенному специалисту потребуется от нескольких месяцев до многих лет.

## 8.2. Энергетическое скрытие акустического сигнала

Энергетическое скрытие акустических сигналов в соответствии с рассмотренными методами защиты информации обеспечивается путем применения способов и средств, уменьшающих энергию носителя на входе акустического приемника злоумышленника или увеличивающих энергию помех.

Простейшим способом является **уменьшение громкости** речи во время разговора на конфиденциальные темы. Однако это возможно, если количество собеседников мало, а уровень шумов невелик. Громкость акустического сигнала уменьшают путем **звукоизоляции, звукопоглощения** и **глушения звука.** Для повышения уровня акустических помех применяют активные средства — **генераторы акустических помех.**

**Звукоизоляция** обеспечивает локализацию акустических сигналов в замкнутом пространстве внутри контролируемых зон. Основное требование к ней — за пределами этой зоны соотношение сигнал/помеха не должно превышать максимально-допустимые значения, исключающие добывание информации злоумышленниками. Звукоизоляция достигается за счет отражения и поглощения акустической волны.

При падении акустической волны на границу поверхностей с различными удельными плотностями большая часть падающей волны отражается. Отражательная способность поверхности преграды зависит от плотности ее материала и скорости распространения звука в ней.

Меньшая часть волны проникает в материал звукоизолирующей конструкции и распространяется в нем, теряя свою энергию в зависимости от длины пути и акустических свойств материала. Под действием акустической волны звукоизолирующая поверхность совершает сложные колебания, также поглощающие энергию падающей волны. Характер этого поглощения определяется соотношением частот падающей акустической волны и спектральных характеристик средства звукоизоляции. В области резонансных частот (до 25-45 Гц) средств звукоизоляции ослабление зависит в основном от внутреннего трения в звукоизолирующем материале, на более высоких частотах — от его поверхностной плотности, измеряемой в кг на 1 $м^2$ поверхности.

Плоский слой звукопоглощающего материала облицовок устанавливается на жестком основании, которое крепится непосредственно или с воздушным промежутком на поверхности ограждения, к потолку или стенам. Для дополнительного звукопоглощения и уменьшения числа переотражений от ограждений с целью снижения времени реверберации используются **штучные звукопоглотители.** Они представляют собой одно- или многослойные объемные звукопоглощающие конструкции (в виде куба, параллелепипеда, конуса), подвешиваемые к потолку помещения. Размеры граней штучных звукопоглотителей составляют 40-400 см.

Каналы вентиляции и систем кондиционирования также способствуют утечке информации из помещения. Передача звука через вентиляционный канал происходит по воздуху, находящемуся в полости канала, и по элементам его конструкции. Наиболее эффективной мерой предотвращения утечки информации через воздухопроводы является глушение звука.

**Глушение звука** достигается путем интенсивного поглощения энергии акустической волны при распространении ее в специальной конструкции, называемой **глушителем.** Например, в момент выхода газов из цилиндра двигателя автомобиля в выходном коллекторе создается акустическая волна большой интенсивности. Она направляется по трубе в глушитель, в котором, проходя через многочисленные преграды, теряет энергию и выходит из выхлопной трубы с энергией, сравнимой с энергией акустического фона. При прогорании глушителя или его съеме, что делают иногда на спортивных автомобилях для повышения их мощности, работа двигателя сопровождается интенсивным шумом.

Громкость звука, воспринимаемого человеком, зависит не только от его собственной интенсивности, но и от других звуков, действующих одновременно на барабанную перепонку уха. В силу психофизиологических особенностей восприятия звука человеком интенсивность маскирующих звуков обладает асимметричностью. Она проявляется в том, что маскирующий звук оказывает относительно небольшое влияние на тоны маскируемого звука ниже его собственной частоты, но сильно затрудняет восприятие более высоких звуков. Поэтому для маскировки акустических сигналов эффективны низкочастотные **акустические шумовые сигналы.** Причем речеподобными помехами обеспечивается более эффективное зашумление, чем «белым» шумом. Это объясняется большей восприимчивостью слухового анализатора к речеподобным звукам, чем к акустическому шуму с равномерным спектром.

Следует отметить, что акустическое зашумление помещения обеспечивает эффективную защиту информации в нем, если акустический генератор расположен к акустическому приемнику злоумышленника ближе, чем источник информации. Например, когда подслушивание возможно через дверь или открытое окно, то акустический генератор целесообразно разместить возле двери или на подоконнике окна. Если неизвестно местонахождение акустического приемника злоумышленника, например закладного устройства, то размещение акустического генератора между говорящими людьми, как рекомендуют некоторые фирмы, не гарантирует надежную защиту информации. Кроме того, повышение уровня шума вынуждает собеседников к более громкой речи, что создает дискомфорт и снижает эффект от зашумления.

Снижение дискомфорта, вызванного акустическими шумами в помещении, достигается использованием специальных переговорных телефонов и акустических приемников, в которых устраняется акустический шум.

Более эффективным и активным универсальным способом защиты информации, передаваемым структурным звуком, является **вибрационное зашумление.** Шум в звуковом диапазоне в твердых телах создают пьезокерамические вибраторы акустического генератора, прикрепляемые (приклеиваемые) к поверхности зашумляемого ограждения (окна, стены, потолка и др.) или твердотельного звукопровода (батареи отопления, трубы и др.). Так как уровень структурного шума, создаваемого генератором, выше уровня речевого сигнала в твердых телах, но ниже уровня слышимости, то вибрационное зашумление целесообразно применять во всех случаях, когда существует возможность утечки с помощью структурного звука.

Пассивное энергетическое скрытие акустической информации от подслушивания лазерным микрофоном заключается в ослаблении энергии акустической волны, воздействующей на оконное стекло. Оно достигается использованием штор и жалюзей, а также двойных оконных рам. Активные способы энергетического скрытия акустической информации предусматривают применение генераторов шумов в акустическом диапазоне, датчики которых приклеиваются к стеклу и вызывают его колебание по случайному закону с амплитудой, превышающей амплитуду колебаний стекла от акустической волны.

## 8.3. Обнаружение и подавление закладных устройств

### 8.3.1. Демаскирующие признаки закладных устройств

Обнаружение закладных устройств, так же как и любых других объектов, производится по их демаскирующим признакам [7]. Чем больше демаскирующих признаков в признаковой структуре и чем они информативнее, тем выше вероятность обнаружения объекта. Каждый вид закладных устройств имеет свою признаковую структуру, позволяющую с той или иной вероятностью обнаружить закладку. Распознавание закладки, т. е. определение ее вида, назначения и характеристик, проводится в результате анализа схемотехнических и конструктивных решений. Однако внешний вид закладки и способы ее оперативного применения позволяют приблизительно определить принадлежность злоумышленника к зарубежной разведке, конкуренту или криминальным элементам.

Спецслужбы используют наиболее совершенные средства добывания, как правило, отсутствующие на рынке, и тщательно готовят операцию по установке закладок. Криминальные элементы пользуются средствами, имеющимися на «черном» рынке, и действуют более грубо. Разведка коммерческих структур применяет закладки промышленного или собственного изготовления и тщательно скрывает от конкурента свои намерения получения конфиденциальной информации нелегальными способами.

Наиболее информативные прямые и косвенные признаки закладных устройств приведены в таблице 8.1.

Таблица 8.1

| Вид признака | Наименование признака |
|---|---|
| Видовой | Тонкий провод от миниатюрного микрофона в соседнее помещение, малогабаритный предмет в виде параллелепипеда, цилиндра или иной формы с проводом (антенной), одно или несколько отверстий малого диаметра в кожухе, выключатель на кожухе, свежие царапины на элементах крепления технических средств, несоответствие топологии схемы радиоэлектронного устройства документации или топологии других однотипных образцов, несоответствие рентгеновского изображения конструкции ее назначению |
| Сигнальный | Радио - и ИК-диапазон излучений, электрический сигнал в проводе частотой десятки-сотни кГц и более, АМ и ЧМ несущего колебания речевым сигналом, ширина полосы сигнала — десятки, реже сотни кГц, простые технические методы закрытия радиосигнала, случайные изменения напряжения в телефонной линии, емкости, индуктивности, дополнительные неоднородно- |

| | |
|---|---|
| | сти в телефонной линии |
| Веще-ствен-ный | Нелинейность элементов и металлические детали в малогабаритной конструкции, непрозрачность рентгеновским лучам, пустота в твердой среде с неизвестным вложением |

Камуфлированные радиозакладки по внешнему виду на первый взгляд не отличаются от объекта имитации, особенно если закладка устанавливается в корпус бытового предмета без изменения его внешнего вида. Некоторые камуфлированные закладные устройства неотличимы от оригиналов при внешнем осмотре. Например, на поверхность закладки-конденсатора наносятся заводские реквизиты — тип, величина емкости, номер серии и т. д. Назначение таких закладок можно выявить путем разборки или просвечивания их рентгеновскими лучами.

Однако следует иметь в виду, что закладки, камуфлированные под малогабаритные предметы, снижают, но не всегда, функциональные возможности этих предметов. Поэтому обнаруженные ограничения функций средств оргтехники, электробытовых устройств и др. могут служить косвенными признаками установки в них закладных устройств. Например, в шариковой авторучке закладное устройство занимает приблизительно половину ее длины, в результате чего резко укорачивается пишущий стержень и сокращается время нормальной работы ручки. Кроме того, такую ручку нельзя разобрать, например, для замены стержня, так как разбираемые части склеивают. Таким образом, закладные устройства содержат видовые, сигнальные и вещественные демаскирующие признаки, информативность которых позволяет их обнаруживать среди других объектов.

### 8.3.2. Методы обнаружения закладных устройств

В зависимости от демаскирующих признаков закладных устройств методы их поиска можно разделить на 3 группы:

- поиск закладных устройств по их видовым признакам;
- поиск закладных устройств по их сигнальным признакам;
- поиск закладных устройств по их вещественным признакам.

Поиск закладных устройств по видовым признакам осуществляется путем визуального осмотра помещения сотрудниками службы безопасности или иными сотрудниками. Визуальный осмотр требует минимальных затрат по сравнению с другими и может производиться периодически как силами службы безопасности, так и секретарем руководителя организации или иного должностного лица.

Сущность поиска закладки путем визуального осмотра состоит в тщательном осмотре помещения, предметов мебели (книжного шкафа и полок, столов, стульев, кресел, дивана, и др.), компьютера, радио- и электробытовых устройств, телефонных аппаратов, устройств громкоговорящей и диспетчерской связи, картин на стенах, портьер и жалюзей, других предметов в поме-

щении, в которых в принципе можно спрятать малогабаритное закладное устройство. Осмотр проводится без разборки рассматриваемого предмета.

В целях обеспечения полноты визуального контроля целесообразно проводить его по определенной схеме, аналогичной схеме осмотра места происшествия криминалистами: от двери по или против часовой стрелки от периферии к центру помещения. Во время осмотра обращается внимание на свежие царапины на обоях, возле сетевых и телефонных розеток и выключателей освещения, на стенах, винтах корпуса телефонного аппарата, на пылевые следы смещения картины или других предметов, на отрезки проводов и на другие следы или непонятные на первый взгляд предметы.

Для визуального осмотра при поиске закладных устройств применяют различное вспомогательное оборудование. Это оборудование, имея невысокую стоимость, позволяет повысить вероятность обнаружения закладки в ходе визуального осмотра помещения. К такому оборудованию относятся фонари, досмотровые зеркала и технические эндоскопы.

Конечно, путем визуального осмотра помещения и предметов интерьера далеко не всегда удается обнаружить скрытно установленные закладные устройства, но периодический осмотр помещения позволяет выявить закладные устройства, установленные в спешке или встроенные в предметы, ранее отсутствующие в помещении. Секретарь, наблюдающий многократно в течение рабочего дня предметы в кабинете, быстрее обнаружит изменения в помещении, чем любой другой сотрудник.

Поиск закладных устройств, вмонтированных в технические средства, производят в ходе специальных исследований путем сравнения топологии схемы исследуемого образца с эталонной, зафиксированной в документации или в топологии образца, в котором заведомо нет закладного устройства. Для обеспечения неразрушающего контроля применяются специальные рентгеновские установки, позволяющие наблюдать изображения отдельных слоев микросхем и многослойных печатных плат.

Остальные методы предусматривают поиск закладных устройств дистанционно с использованием различных технических средств, способных обнаруживать сигнальные и вещественные демаскирующие признаки закладных устройств. Так как наиболее распространены радиоизлучающие закладные устройства, то их поиск производится путем обнаружения сигнальных демаскирующих признаков радиоизлучающих закладных устройств.

Наиболее широко применяются следующие методы поиска закладных устройств по их прямым и косвенным сигнальным демаскирующим признакам:

- поиск источников радиоизлучений, мощность которых превышает мощность электромагнитного фона;
- поиск и селекция радиосигналов по частоте с последующей идентификацией их текущей признаковой структуры с эталонной признаковой структурой закладного устройства;

- поиск проводных закладных подслушивающих устройств по косвенным признакам изменений электрических характеристик линий, к которым подключены эти устройства.

Учитывая повсеместное распространение телефонов как средств коммуникаций и особый интерес злоумышленников к подслушиванию телефонных разговоров, при обеспечении защиты информации большое внимание уделяется способам и средствам контроля телефонных линий.

Способы контроля телефонных линий основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий: напряжения и тока в линии, значений емкости и индуктивности линии, активного и реактивного сопротивления. В зависимости от способа подключения подслушивающего устройства к телефонной линии (последовательного — в разрыв провода телефонного кабеля, параллельного или индуктивного) влияние подключаемого подслушивающего устройства может существенно отличаться. Так как закладное устройство использует энергию телефонной линии, величина отбора мощности закладкой из телефонной линии зависит от мощности передатчика закладки и его коэффициента полезного действия. Наилучшие возможности по выявлению этих отклонений обеспечиваются при опущенной трубке телефонного аппарата. Это обусловлено тем, что в этом состоянии в телефонную линию подается постоянное напряжение 48-60 В (для отечественных телефонных линий) и 25-36 В (для зарубежных АТС). При поднятии трубки в линию поступает от АТС дискретный сигнал, преобразуемый в телефонной трубке в длинный прерывистый тон, а напряжение в линии уменьшается до 12 В, т. е. происходит резкое изменение электрических параметров линии, существенно превышающие изменения из-за закладных устройств.

Для контроля телефонных линий применяются следующие устройства:

- устройства оповещения световым и звуковым сигналом об уменьшении напряжения в телефонной линии, вызванном несанкционированным подключением средств подслушивания к телефонной линии;
- измерители характеристик телефонных линий (напряжения, тока, емкостного сопротивления и др.), при отклонении которых от установленных норм формируется сигнал тревоги;
- «кабельные радары», позволяющие измерять неоднородности телефонной линии и определять расстояние до неоднородности (асимметрии постоянному току в местах подключения подслушивающих устройств, обрыва, короткого замыкания и др.).

Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения с индикацией изменения его значения от номинального, которое фиксируется оператором в режиме настройки вращением регулятора на лицевой панели устройства. Предполагается, что при установке номинального напряжения к телефонной линии подслушивающее устройство не подключено. Как правило, подобные устройства содержат также фильтры для защиты от прослушивания за счет «микрофонного эффекта»» в элементах телефонного аппарата и высокочастотного навязывания.

Но устройства контроля телефонной сети по изменению напряжения или тока в ней не обеспечивают надежного обнаружения подключаемых параллельно к линии современных средств подслушивания с входным сопротивлением более единиц МОм.

Повышение реальной чувствительности устройств контроля ограничено нестабильностью параметров линии, колебаниями напряжения источников электропитания на АТС, помехами в линии. Для снижения вероятности ложных тревог в более сложных подобных устройствах увеличивают количество измеряемых характеристик линии, предусматривают возможность накопления и статистической обработки результатов измерений в течение достаточно длительного времени как контролируемой линии, так и близко расположенных.

Так как любое физическое подключение к кабелю телефонной линии создает в ней неоднородность, от которой отражается посылаемый в линию сигнал, то по характеру отражения (амплитуде и фазе) и времени запаздывания отраженного сигнала оценивают вид неоднородности и рассчитывают длину участка линии до неоднородности (места подключения).

Разнообразие радиоизлучающих и проводных закладных устройств и способов их применения способствует объединению в автоматизированном комплексе средств, реализующих все способы поиска и обнаружения активных закладных устройств. Более того, в них устанавливаются генераторы прицельной помехи, настраиваемой на частоту закладного устройства и подавляющей их сигналы в свободном пространстве и в проводах кабелей. Такая тенденция обеспечивает снижение суммарной стоимости средств поиска и обнаружения закладных устройств по их сигнальным признакам и оперативность подавления их сигналов в экстремальных ситуациях, например, во время ответственного совещания, когда крайне нежелательно проводить поисковые мероприятия в помещении или зале совещания.

Поиск и обнаружение дистанционно управляемых и пассивных (параметрических) закладных устройств производятся по прямым и косвенным признакам входящих в их состав веществ. Прямыми признаками закладных устройств является наличие в них полупроводниковых и металлических элементов. Косвенные признаки установки закладного устройства в стене или иной твердой среде — наличие в них пустоты.

Так как любое радиоэлектронное закладное устройство содержит полупроводниковый элемент (транзистор, диод), то наиболее информативным признаков не излучающего во время поиска закладного устройства является наличие полупроводниковых элементов в местах, в которых не должно быть радиоэлектронных устройств. Такими местами являются стены, мебель, картины, подвесные потолки и др. Для обнаружения полупроводникового элемента используются нелинейные свойства его вольтамперной характеристики — зависимости тока, протекающего по n-p переходу полупроводника, от величины подводимого к нему напряжению. Вихревые электрические токи через n-p переходы полупроводников возникают при облучении проводника электромагнитным полем. Поле создает антенна передатчика нелинейного ло-

катора, излучающего непрерывные гармонические или импульсные сигналы на частоте f, составляющие для разных локаторов доли и единицы ГГц (400-1000 МГц). В силу нелинейности полупроводника токи в нем имеют форму, отличную от гармонического колебания, и могут быть разложены в ряд Фурье. Вихревые токи создают вторичное электромагнитное поле, содержащее кроме электромагнитной волны на основной частоте f, также волны с частотой 2f, 3f и других частотах спектра вторичного сигнала. В отличие от классического радиолокатора нелинейный локатор имеет приемник, настроенный на частоту 2f, а в некоторых типах дополнительный приемник на частоте 3f. Появление в отраженном сигнале колебаний с частотами 2f и 3f позволяет сделать вывод о наличии в области облучения зондирующей электромагнитной волны элементов с нелинейной вольтамперной характеристикой.

На практике достоверность обнаружения полупроводникового элемента снижается в связи с тем, что нелинейными свойствами обладают не только полупроводниковые элементы, но и окислы и места контактов металлических предметов и конструкций помещения и здания: ржавой арматуры железобетонных стен, гвоздей и болтов мебели, даже скрепок для бумаги. Поэтому для обнаружения полупроводников приходится учитывать различия в мощности сигналов на частотах 2f и 3f, отраженных от полупроводников и окисленных металлических конструкций и предметов. Эти различия обусловлены разной формой нелинейных вольтамперных характеристик полупроводниковых и других элементов, что приводит к различиям амплитуд гармоник спектров отраженных сигналов. Для настоящих полупроводников уровень второй гармоники в среднем на 20 дБ превышает уровень 3-й гармоники, для ложных — противоположные соотношения. Но эти отличия не столь существенны для формального однозначного принятия решения о наличии в рассматриваемой области полупроводника, а не иного элемента с нелинейной вольтамперной характеристикой. Поэтому вероятность идентификации полупроводника тем выше, чем более опытным является оператор, проводящий поиск закладного устройства. Для повышения достоверности обнаружения полупроводниковых элементов используется нестабильность вольтамперных характеристик «ложных» полупроводников при механическом воздействии (ударе) по ним. Это связано с тем, что при ударе нарушается контакт между металлическими поверхностями или разрушается пленка окисла, кроме того, при облучении работающего закладного устройства переотраженный им сигнал модулируется по амплитуде первичным информационным сигналом. Предусмотренный в современных нелинейных локаторах режим выделения огибающей переотраженного сигнала и его индикации позволяет обнаруживать и идентифицировать работающие закладные устройства с высокой достоверностью.

Проникающая глубина излучающей волны нелинейного локатора зависит от мощности и частоты излучения. В силу увеличения затухания электромагнитной волны в среде распространения с повышением частоты колебаний уровень мощности переизлученного (отраженного) сигнала тем выше, чем ниже частота локатора. Но для излучений с более низкой частотой ухудшаются возможности локатора по локализации места нахождения нелинейности,

так как при приемлемых размерах его антенны расширяется диаграмма направленности антенны локатора.

Очевидно, что чем выше мощность излучения локатора, тем глубже проникает электромагнитная волна и тем больше вероятность обнаружения помещенной в стену закладки. Но большая мощность излучения оказывает вредное воздействие на оператора. Для обеспечения его безопасности максимальная мощность излучения локатора в непрерывном режиме не превышает 3-5 Вт. При импульсном режиме работы локатора мощность в импульсе достигает 300 Вт при меньшей средней мощности, не превышающей 1,5 Вт.

Очевидно, что после обнаружения закладного устройства его необходимо изъять, разрушить или использовать для дезинформирования. Для изъятия закладного устройства из стены ее приходится долбить. Так как достоверность идентификации закладного устройства в железобетонной стене мала, то разрушения стены во время его поиска могут быть весьма существенны. Для повышения достоверности обнаружения закладных устройств в железобетонных стенах применяют также обнаружители естественных и искусственных пустот, в которых могут быть размещены закладные устройства, а также рентгеновские установки (**интерсепторы**).

Для обнаружения пустот применяются средства — обнаружители пустот, которые реагируют на отличия диэлектрической проницаемости или теплопроводности воздуха (пустоты) и бетона. Измерительная катушка генератора обнаружителя пустоты локализует место в однородной среде (стене) — пустоту, диэлектрическая проницаемость которого отличается от диэлектрической проницаемости вещества среды. Также будут отличаться температура внутри пустоты и бетона в нагретом солнечными лучами или обогревателем помещении. Границы пустот будут видны на экране тепловизора.

Большие возможности для обнаружения закладных устройств в строительных конструкциях предоставляют методы **подповерхностной локации.** В результате цифровой обработки переотраженных от исследуемой среды сигналов на экране монитора компьютера получают полутоновое изображение твердой среды, например стены на глубине 200-500 мм с разрешением около 2 см. Хотя такое разрешение недостаточно для рассмотрения детальной структуры наблюдаемой неоднородности, оно позволяет отличить длинные стержни арматуры от локализованного в пространстве закладного устройства.

Для обнаружения закладных устройств в предметах деревянной и мягкой мебели, в кирпичных стенах, в одежде человека используют обнаружители металла — **ручные металлоискатели.** Современные металлоискатели обладают высокой чувствительностью. Некоторые образцы могут обнаруживать кончик швейной иглы длиной в 5 мм на расстоянии нескольких см. Однако если закладное устройство размещено вблизи металлического гвоздя или болта, то достоверность идентификации закладного устройства резко снижается.

Наибольшую достоверность идентификации закладных устройств, скрытно установленных в отдельных предметах, обеспечивают **средства радиационной интроскопии** (рентгеновские установки). Основу этих средств

составляют рентгеновские трубки и рентгеновские электронно-оптические преобразователи (РЭОПы), изобретенные в начале 50-х годов Тевисом и Тулом. В настоящее время выпускается третье поколение РЭОПов, отличающееся от предыдущих высоким разрешением — до 3 лин/мм. Средства радиационной интроскопии делят на две группы: флуороскопические и сканирующие, реализующие методы цифровой радиографии. Для поиска закладных устройств применяются пассивные и активные флуороскопические системы. В пассивных изображения внутренней структуры объекта наблюдаются непосредственно на экране РЭОПа, в активных — первичное теневое изображение усиливается или трансформируется дополнительными электронными средствами. Пассивные флуороскопы просты по конструкции и в эксплуатации, недороги, надежны, но создают низкий уровень яркости изображения при достаточно высоких радиационных нагрузках на объект. В современных пассивных флуороскопах экран способен сохранять (запоминать) изображение после выключения высокого напряжения не рентгеновской трубке, что позволяет оператору в безопасных условиях рассматривать изображение без ограничения времени. Активные флуороскопические системы обеспечивают высокую яркость и чувствительность, превышающую в 2 раза чувствительность пассивных систем. Для контроля помещений и отдельных подозрительных объектов наибольшее применение находят флуороскопы, в которых изображение с экрана РЭОПа передается на дополнительный электронноoптический преобразователь с помощью стекловолоконного жгута, и рентгенотелевизионные комплексы. В последних первичное изображение проектируется на высокочувствительную телевизионную камеру, а изображение объекта наблюдается на экране монитора, удаленного на безопасное для оператора расстояние от рентгеновской трубки. Современные рентгенотелевизионные комплексы обеспечивают возможность наблюдения с разрешением около 800х600 пикселей объектов размером до 320 х 420 мм за стальной пластиной толщиной до 10 мм.

### 8.3.3. Методы подавления закладных устройств

Обнаружение с той или иной вероятностью закладного устройства является важным, но лишь одним из этапов предотвращения утечки через них информации. Возникает вопрос о дальнейших действиях. Если обнаружено излучение закладного устройства из помещения, где проводится совещание с участием представителей других организаций, то изъятие его в ходе совещания может рассматриваться как крайняя, но не желательная мера, так как она нарушит ход совещания и снизит рейтинг организации, не обеспечившей информационную безопасность до начала совещания. Изъятие закладного устройства не всегда целесообразно даже в условиях поисковых мероприятий, так как важно не только обнаружить его, но и выявить злоумышленника, установившего и использующего это закладное устройство. Кроме того, через него можно передавать злоумышленнику дезинформацию.

Поэтому наряду с изъятием обнаруженных закладных устройств возможны иные различные методы их **функционального** и **физического подавления** [6]. Функциональное подавление приводит к подавлению работоспособности закладного устройства в течение времени воздействия подавляющих сигналов. При физическом подавлении устройство выходит из строя.

Функциональное подавление осуществляется сигналами, проникающими во входные цепи закладного устройства и нарушающими его работоспособность.

Для функционального подавления сигналов закладных устройств применяются **заградительные** и **прицельные помехи.** Заградительные помехи имеют ширину спектра, перекрывающего частоты излучений подавляющего числа закладных устройств, — от долей до тысячи МГц. Мощность излучения не превышает 20 Вт.

Однако подобные генераторы помех эффективно подавляют радиосигналы закладки, если отношение мощности помехи и сигнала закладки в несколько раз выше отношения ширины спектра помехи и сигнала. Это требование обусловлено тем, что мощность помехи «размазывается» по диапазону частот генератора помех, в среднем, составляющем около 1000 МГц, и на долю узкополосного сигнала закладки приходится лишь незначительная часть энергии помехи, которой не хватает для эффективного искажения информационных параметров сигнала. Например, одно из устройств активной защиты информации с повышенной выходной мощностью обеспечивает максимальную мощность шума в полосе ЧМ-сигнала (150-200 кГц) порядка 40 мВт при интегральном значении выходной мощности генератора до 20 Вт. Но для узкополосного ЧМ-сигнала мощность помехи в полосе сигнала составляет доли и единицы мВт, что недостаточно для подавления сигналов закладки. Учитывая значительную долю на рынке радиозакладок с мощностью излучения порядка 10-20 мВт и тенденцию сужения полосы их кварцованных частот, применение даже достаточно мощных генераторов помех не гарантирует предотвращение утечки информации. Наращивание мощности заградительной помехи ограничивается требованиями по экологической безопасности и электромагнитной совместимости излучений помех и сигналов радиовещания и связи в зашумляемом пространстве.

## 8.4. Средства подавления диктофонов

Резкое уменьшение габаритов и усиление чувствительности современных диктофонов, а также возможность использования сотовых телефонов в режиме диктофона, привело к необходимости отдельно рассмотреть вопрос об их подавлении [6, 8].

Для подавления портативных диктофонов используют устройства представляющие собой генераторы мощных шумовых сигналов дециметрового диапазона частот. Импульсные помеховые сигналы воздействуют на микрофонные цепи и усилительные устройства диктофонов, в результате чего оказываются записанными вместе с полезными сигналами, вызывая сильные ис-

кажения информации. Зона подавления, определяемая мощностью излучения, направленными свойствами антенны, а также типом зашумляющего сигнала обычно представляет собой сектор шириной от 30 до 80 градусов и радиусом до 5 м.

Дальность подавления современными средствами сильно зависит от нескольких факторов:

- тип корпуса диктофона (металлический, пластмассовый);
- используется выносной микрофон или встроенный;
- габариты диктофона;
- ориентация диктофона в пространстве.

Отличительной особенностью рассматриваемых устройств является возможность навязывания музыкальной или речеподобной помех, что существенно понижает остаточную разборчивость исходной речи.

# 9. ОПТИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ.

## 9.1 Структура оптического канала утечки информации

Структура оптического канала утечки информации имеет вид, показанный рис. 9.1 [2].


Рис. 9.1. Структура оптического канала утечки информации

Объект наблюдения в оптическом канале утечки информации является одновременно источником информации и источником сигнала, потому что световые лучи, несущие информацию о видовых признаках объекта, представляют собой отраженные объектом лучи внешнего источника или его собственные излучения.

Отраженный от объекта свет содержит информацию о его внешнем виде (видовых признаках), а излучаемый объектом свет – о параметрах излучений (признаках сигналов). Запись информации производится в момент отражения падающего света путем изменения его яркости и спектрального состава. Излучаемый свет содержит информацию об уровне и спектральном составе источников видимого света, а в инфракрасном диапазоне по характеристикам излучений можно также судить о температуре элементов излучения. В общем случае объект наблюдения излучает и отражает свет другого источника как в видимом, так и ИК-диапазонах. Однако в конкретных условиях соотношения между мощностью собственных и отраженных излучений в видимом диапазоне волн и ИК-диапазоне могут существенно отличаться.

В видимом диапазоне мощность излучения определяется в подавляющем большинстве случаев мощностью отраженного света и содержащихся в спектре искусственных источников света. Например, габариты автомобиля в ночное время обозначаются включенными фонарями красного цвета, укрепленными по краям автомобиля. Объект наблюдения или его элементы излучают собственные электромагнитные излучения в видимом диапазоне при высокой температуре. В ближнем (0.76–3 мкм) и среднем (3–6 мкм) диапазонах собственная мощность ИК-излучения объектов значительно меньше мощности отраженного от объекта потока солнечной энергии. Однако с переходом в длинноволновую область ИК-излучения мощность теплового излучения объектов может превышать мощность отраженной солнечной энергии.

Основным и наиболее мощным внешним источником света является Солнце. При температуре поверхности около 6000° Солнце излучает огромное количество энергии в достаточно широкой полосе – от ультрафиолетового до инфракрасного (0.17–4 мкм). Видимая часть спектра излучения лежит в

диапазоне 0,4 мкм (фиолетовый цвет) до 0,76 мкм (красный цвет). Максимум солнечного излучения приходится на 0.47 мкм, в ультрафиолетовой части оно резко убывает, в инфракрасной – регистрируется в виде широкой и пологой кривой.

При прохождении через атмосферу солнечные лучи взаимодействуют с содержащимися в ней молекулами газов, частицами пыли, дыма, кристалликами льда, каплями воды. В результате такого взаимодействия часть солнечной энергии поглощается, другая – рассеивается.

Процессы рассеяния и поглощения солнечной энергии уменьшают интенсивность солнечной радиации на поверхности Земли и меняют спектр солнечного света, освещающего наземные объекты. В кривой излучения этого света, характеризующей интенсивность излучения в зависимости от длины волны, появляются участки поглощения и пропускания. Последние называются окнами прозрачности. Излучения длиной менее 0.27 мкм полностью поглощаются озоном. Атмосферное рассеяние света уменьшает прямую солнечную радиацию и повышает рассеянное (диффузное) излучение атмосферы. Рассеяние в коротковолновой части спектра сильнее, чем в длинноволновой. Особенно заметно оно в голубой и ультрафиолетовой областях. Поэтому небо имеет голубой цвет. Интенсивность рассеяния солнечного света в ближнем инфракрасном диапазоне незначительная. Задымленность приповерхностного слоя атмосферы мало влияет на излучения в ближнем ИК-диапазоне, если размеры твердых частиц дыма в атмосфере не превышают 1 мкм. Туман и облака очень сильно рассеивают ИК-излучение в этом интервале длин, так как водяные капли имеют размер около 4 мкм. Наличие облачности высоких ярусов, не закрывающих солнечный диск, повышает рассеянное излучение и при сохранении значения прямой освещенности увеличивает ее суммарную величину на (20–30)% по сравнению с освещенностью при безоблачном небе. Низкая облачность так же, как и тени облаков, снижают суммарную освещенность в 2–5 раз, в зависимости от высоты Солнца. Освещенность в дневное время земной поверхности Солнцем составляет в зависимости от его высоты, облачности атмосферы $10^4$–$10^5$ лк. Для сравнения уровней освещенности скажем, что наименьшая освещенность, воспринимаемая привыкшим к темноте глазом, составляет $10^{-9}$ лк, а свет свечи виден на расстоянии 4…9 км. Напомню, что 1 люкс освещенности равен 1 люмену светового потока на 1 квадратный метр площади. С движением Солнца к горизонту Земли, когда зенитное расстояние между ними достигает максимума, освещенность, создаваемая Солнцем, составляет приблизительно 10 лк. При этом изменяется и спектр солнечного света, так как при прохождении толщи атмосферы синие и фиолетовые лучи ослабляются сильнее, чем оранжевые и красные, вследствие чего максимум излучения Солнца смещается в красную область цвета. С заходом Солнца за горизонт и наступлением сумерек освещенность убывает вплоть до наступления астрономических сумерек, за которыми следует наиболее темное время суток – ночь.

Освещенность в лунную ночь при безоблачном небе, когда так называемую естественную ночную освещенность (ЕНО) создает отраженный от

Луны солнечный свет, составляет около 0.3 лк. Величина ЕНО, создаваемая светом Луны, в течение месяца меняется приблизительно в 100 раз в зависимости от взаимного положения Луны, Солнца и Земли. Лунный месяц разделяется по уровню освещенности на четыре части, каждая длительностью около недели. Источниками излучения в безлунную ночь при безоблачном небе, называемым звездным светом, являются солнечный свет, отраженный от планет: туманностей, свет звезд, а также свечение кислорода и азота в верхних слоях атмосферы на высоте 100–300 км. Освещенность поверхности Земли звездным светом составляет в среднем 0.001 лк.

В инфракрасном диапазоне мощность излучения объекта зависит от температуры тела или его элементов, мощности падающего на объект света коэффициента отражения объекта в этом диапазоне. Коэффициент теплового излучения для реальных объектов не постоянен по спектру и определяется соответствии с законом Кирхгофа отношением спектральной плотности энергетической яркости объекта к спектральной плотности энергетически яркости абсолютно черного тела, которое обладает максимумом энергии теплового излучения по сравнению со всеми другими источниками при той температуре. Средняя температура поверхности Земли близка к 17 градусов по Цельсию. Максимум ее теплового излучения приходится на 9.7 мкм. Объекты под действием солнечной радиации в течение дня по-разному отдают накопленное тепло в окружающее пространство. Различия в температуре излучении могут рассматриваться как демаскирующие признаки.

Объекты могут иметь собственные источники тепловой энергии, например, высокотемпературные элементы машин, дизель-электростанции и др., температура которых значительно выше температуры фона. Максимум теплового излучения таких объектов смещается в коротковолновую область, что служит демаскирующим признаком для таких объектов.

Длина (протяженность) канала утечки зависит от мощности света, от объекта, свойств среды распространения и чувствительности фотоприемника.

Среда распространения в оптическом канале утечки информации возможна трех видов:

- безвоздушное (космическое) пространство;
- атмосфера;
- вода,
- оптические световоды.

Оптический канал утечки информации, среда распространения которого содержит участки безвоздушного пространства, возникает при наблюдении за наземными объектами с космических аппаратов. Граница между космическим пространством и атмосферой достаточно условна. На высотах 200–300 км существуют еще остатки газов, проявляющиеся в тормозящем действии на космические аппараты.

Сложный состав атмосферы определяет ее пропускную способность различных составляющих света. В общем случае прозрачность атмосферы зависит от соотношения длины проходящего сквозь нее света и размеров взвешенных в атмосфере частиц. Если размеры частиц соизмеримы с длиной вол-

ны света (больше половины длины волны), то пропускание значительно ухудшается. Уровень пропускания меняется в зависимости от длины световой волны. В видимой области прохождению света препятствуют абсорбирующие молекулы кислорода и воды. Коэффициент пропускания в ней немногим более 60%. В ближней ИК-области пропускание несколько большее – до 70%. Адсорбентом в этой области являются пары воды. В средней ИК-области, в диапазоне 3–4 мкм, пропускание достигает почти 90%. Высокое пропускание имеет довольно обширный участок в дальней ИК-области (с 8 до 13 мкм). Абсорбентом в нем являются молекулы кислорода и воды, а также углекислого газа и озона в атмосфере.

Метеорологическая видимость даже в окнах прозрачности зависит от наличия в атмосфере взвешенных частиц пыли и влаги, образующих мглу и туман, капелек и кристаллов воды в виде дождя и снега, а также аэрозолей и дымов, содержащих твердые частицы. Все это вызывает замутнение атмосферы и ухудшает видимость. Призрачность атмосферы как канала распространения света оценивается метеорологической дальностью видимости. Под метеорологической дальностью понимается предельно большое расстояние, начиная с которого при данной прозрачности атмосферы в светлое время суток абсолютно черный предмет с угловыми размерами 20'x20' сливается с фоном у горизонта и становится невидимым. В зависимости от состояния атмосферы дальность видимости, определяющая протяженность оптического канала утечки, имеет значения, приведенные в таблице 9.1.

Таблица 9.1.

| Метеорологическая дальность видимости, км | Оценка видимости, балл | Визуальная оценка замутненности атмосферы и видимости |
|---|---|---|
| Менее 0.05 | 0 | Очень сильный туман |
| 0.05 – 0.2 | 1 | Сильный туман |
| 0,2 – 0.5 | 2 | Умеренный туман |
| 0.5–1.0 | 3 | Слабый туман |
| 1.0–2.0 | 4 | Очень сильная замутненность (очень плохая видимость) |
| 2.0–4.0 | 5 | Сильная замутненность (плохая видимость) |
| 4.0–10.0 | 6 | Умеренная замутненность (умеренная видимость) |
| 10.0–20.0 | 7 | Удовлетворительная видимость |
| 20.0–50.0 | 8 | Хорошая видимость |
| Более 50.0 | | Исключительно хорошая видимость |
| Более 200.0 | | Чистый воздух |

Если объект наблюдения и наблюдатель находятся на земле, то протяженность канала утечки зависит не только от состояния атмосферы, но и ограничивается влиянием кривизны Земли. Дальность прямой видимости **D** в километрах с учетом кривизны Земли можно рассчитать по формуле:

$$\mathbf{D\ [км] = 3{,}57(\sqrt{h_0} + \sqrt{h_н})}$$

Где $h_0$ – высота размещения объекта над поверхностью земли в метрах,

$h_н$ – высота расположения наблюдателя в метрах.

Например, для $h_0$ = 3 м и $h_н$ = 5 м, **D** = 14 км, что меньше метеорологической дальности при хорошей видимости. Эта формула не учитывает неровности Земли и различные инженерные сооружения (башни, высотные здания и т. д.), создающие препятствия для света. Так как параметры источников сигналов и среды распространения зависят от значений спектральных характеристик носителя информации, то протяженность оптического канала утечки ее в видимом диапазоне и ИК-диапазоне могут существенно отличаться.

До недавнего времени атмосфера, и безвоздушное пространство были единственной средой распространения световых волн. С разработкой волоконно-оптической технологии появились направляющие линии связи в оптическом диапазоне, которые в силу больших их преимуществ по отношению к традиционным электрическим проводникам рассматриваются как более совершенная физическая среда для передачи больших объемов информации. Линии связи, использующие оптическое волокно, устойчивы к внешним помехам, имеют малое затухание, долговечны, обеспечивают значительно большую безопасность передаваемой по волокну информации.

Оптическое волокно представляет собой нить диаметром около 100 мкм, изготовленную из кварца на основе двуокиси кремния. Волокно состоит из сердцевины (световодной жилы) и оболочки из оптически менее плотного кварца. Значения показателей преломления (отношений скорости света в вакууме к скорости распространения света в среде) жилы и оболочки выбираются такими, чтобы обеспечить полное отражение света, распространяющегося по световодной жиле, от границы между жилой и оболочкой. Пример изменения угла преломления света в стекле приведен на рис. 9.2.

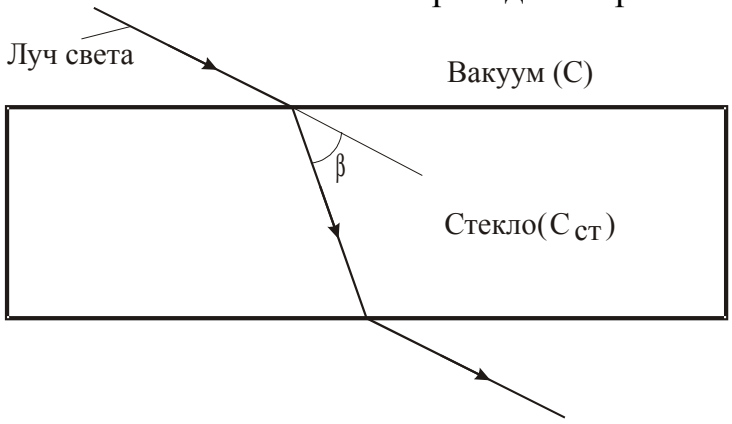



Рис. 9.2.

Показатель преломления равен величине:

$$n = \frac{C}{C_{ст}} > 1,$$

где $C$ – скорость света в вакууме;

$C_{ст}$ – скорость света в стекле.

Чем больше величина показателя преломления **n**, тем больше значение угла $\beta$. Пример распространения света в оптическом волокне приведен на рис. 9.3.

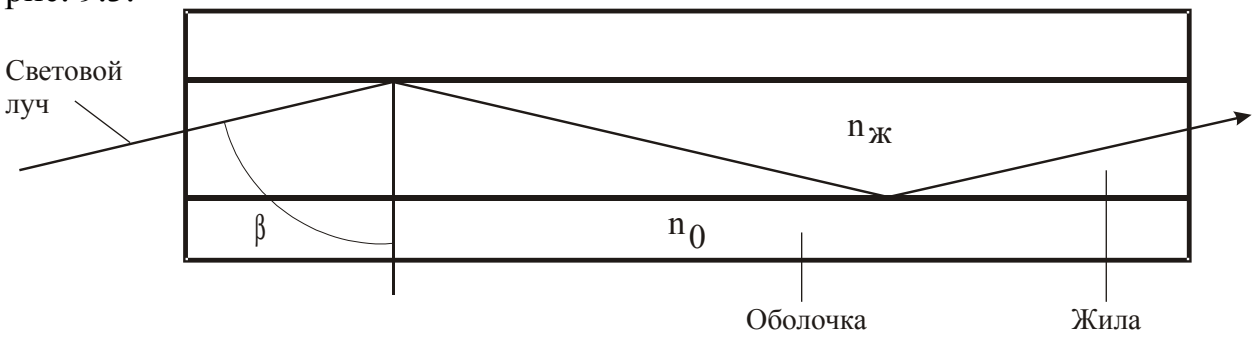



Рис. 9.3.

Предельный угол полного отражения света (угол падения света на границу раздела среды, при равенстве или превышении которого наблюдается полное отражение света от этой границы) определяется из соотношения:

$$\beta = \arcsin(n_0 / n_ж),$$

где $n_0$ – показатель преломления оболочки оптического волокна;

$n_ж$ – показатель преломления световодной жилы оптического волокна.

Волокно с постоянным показателем преломления сердцевины называется ступенчатым, с изменяющимся – градиентным. Для передачи сигналов применяются два вида волокна: одномодовое и многомодовое. В одномодовом волокне световодная жила имеет диаметр порядка 8–10 мкм, по которой может распространяться один луч (одна мода). В многомодовом волокне диаметр световодной жилы составляет 50–60 мкм, что делает возможным распространение в нем большого числа лучей.

Волокно характеризуется двумя основными параметрами: **затуханием и дисперсией.** Затухание измеряется в децибелах на километр (дБ/км) и определяется потерями на поглощение и рассеяние света в оптическом волокне. Потери на поглощение зависят от чистоты материала, а потери на рассеяние – от неоднородности показателя преломления. Лучшие образцы волокна имеют затухание порядка 0.15–0.2 дБ/км, разрабатываются еще более «прозрачные» волокна с теоретическими значениями затухания порядка 0.02 дБ/км для волны длиной 2.5 мкм, где у кварца наблюдается повышенная прозрачность. При таком затухании сигнала могут передаваться на расстояние в сотни километров без ретрансляции (регенерации).

В качестве источника света для оптических каналов связи используются лазеры. Однако лазер излучает не идеальное монохроматическое колебание, а некоторый спектр длин волн. Поэтому спектральные составляющие оптического сигнала распространяются с разными фазовыми скоростями, которые зависят от показателя преломления. В результате происходит разброс – **дис-**

**персия** моментов прихода спектральных составляющих сигнала в точку приема. Дисперсия приводит к искажению (расширению) формы сигнала при его распространении в волокне, что ограничивает дальность передачи и верхнее значение частоты спектра передаваемого сигнала.

Дисперсия волокна оценивается величиной увеличения длительности оптического сигнала $\Delta\tau$ на один километр длины или верхней граничной частотой модулирующего сигнала.

Волокна объединяют в волоконно-оптические кабели, покрытые защитной оболочкой. По условиям эксплуатации кабели подразделяются на **монтажные, станционные, зоновые и магистральные**. Кабели первых двух типов используются внутри зданий и сооружений. Зоновые и магистральные кабели прокладываются в колодцах кабельных коммуникаций, в грунтах, на опорах, под водой. Постоянные соединения отрезков оптических волокон между собой осуществляют свариванием, сплавлением или склеиванием в юстировочном устройстве. Оптические разъемы (соединители) должны допускать многократные соединения–разъединения оптических волокон. Рассогласование волокон возникает из-за имеющихся различий в числовой апертуре, профиле показателя преломления, диаметре сердцевины или из-за погрешностей во взаимной ориентации волокон при их соединении.

Основными причинами излучения световой энергии в окружающее пространство в местах соединения оптических волокон являются:

- смещение (осевое несовмещение) стыкуемых волокон (рис. 9.4,а);
- наличие зазора между торцами стыкуемых волокон (рис. 9.4,б);
- непараллельность торцевых поверхностей стыкуемых волокон (рис. 9.4,в);
- угловое рассогласование осей стыкуемых волокон (рис. 9.4,г);
- различие в диаметрах стыкуемых волокон (рис. 9.4,д).

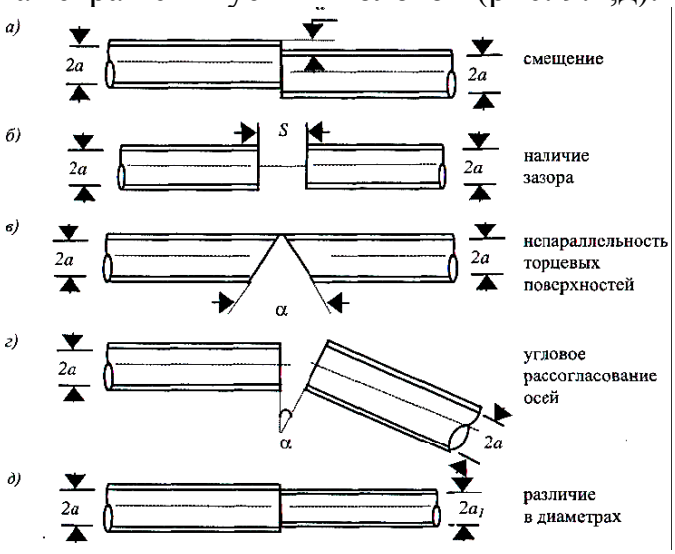



Рис. 9.4. Основные причины излучения из мест соединения световолокна в окружающее пространство.

Исследования показывают, что наиболее интенсивное излучение в окружающее пространство наблюдается при наличии сдвига соединяемых волокон относительно друг друга.

Для съема информации теоретически можно разрушить защитную оболочку кабеля, прижать фотодетектор приемника к очищенной площадке волокна и изогнуть кабель на угол, при котором часть световой энергии направляется на фотодетектор приемника.

Практически информацию из оптического волокна добывают в местах соединения кабеля с техническими средствами, или в местах соединения кабелей друг с другом.

## 9.2. Средства скрытого наблюдения в оптическом диапазоне

В оптическом (видимом и инфракрасном) диапазоне информация разведкой добывается путем визуального, визуально-оптического, фото- и киносъемки, телевизионного наблюдения, наблюдения с использованием приборов ночного видения и тепловизоров.

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, климатических и 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.

Так как физическая природа носителя информации в видимом и инфракрасном диапазонах одинакова, то различные средства наблюдения, применяемые для добывания информации в этих диапазонах, имеют достаточно общую структуру. Ее можно представить в виде, приведенном на рис. 9.5.

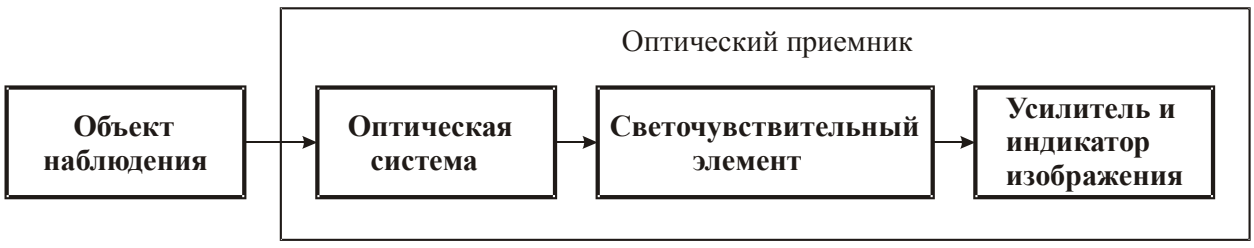



Рис. 9.5. Структурная схема оптического приемника

Большинство средств наблюдения содержит оптический приемник, включающий оптическую систему, светоэлектрический преобразователь, усилитель и индикатор. В зависимости от вида светочувствительного элемента **оптические приборы делятся на:**

- **визуально-оптические;**
- **фотографические;**
- **оптико-электронные.**

В визуально-оптических средствах наблюдения светочувствительным элементом является сетчатка глаза человека. В традиционных фотоаппаратах и киноаппаратах светочувствительным элементом является фотопленка. В оптико-электронных приборах светочувствительным элементом является мишень светоэлектрического преобразователя.

Оптическая система или объектив проецирует световой поток от объекта наблюдения на поверхность светоэлектрического преобразователя (сетчатку глаза, фотопленку, фотодиод, фототранзистор, мишень светоэлектрического 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 оптического приемника.

## 9.3. Визуально-оптические приборы

Для визуально-оптического наблюдения применяются оптические приборы, увеличивающие размеры изображения на сетчатке глаза. В результате этого повышается дальность наблюдения, вероятность обнаружения и распознавания мелких объектов. К визуально-оптическим приборам относятся:

- бинокли;
- монокуляры;
- подзорные трубы;
- специальные телескопы.

**Бинокли.** Для наблюдения за объектами наиболее распространены бинокли. Бинокль (от латинского Bini –пара и oculus – глаз) – оптический прибор из двух параллельных соединенных между собой зрительных труб (система Кеплера). В зависимости от оптической схемы зрительной трубы бинокли разделяются на обыкновенные и призменные.

Простейшая телескопическая система бинокля представляет собой двухкомпонентную систему Кеплера, изображенную на рис. 9.6.

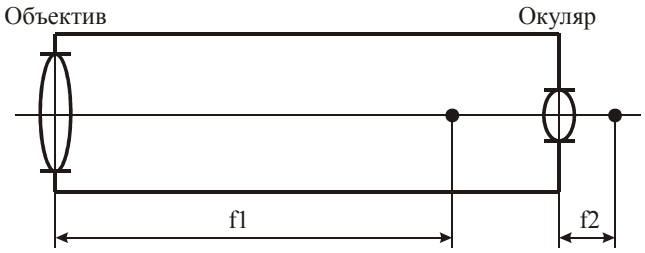



Рис. 9.6.

Кратность увеличения **Г** оптической системы Кеплера определяется отношением фокусных расстояний:

$$Г = f1/f2//$$

Основной недостаток оптической системы Кеплера – переворачивание изображений, из-за чего наблюдатель видит всё вверх ногами. Для устранения этого недостатка в систему вводят компоненты, обеспечивающие нормальное положение объекта. В качестве таких элементов вводят дополнительные линзы (зрительные трубы с дополнительными линзами называют обыкновенными, см. рис. 9.7.)

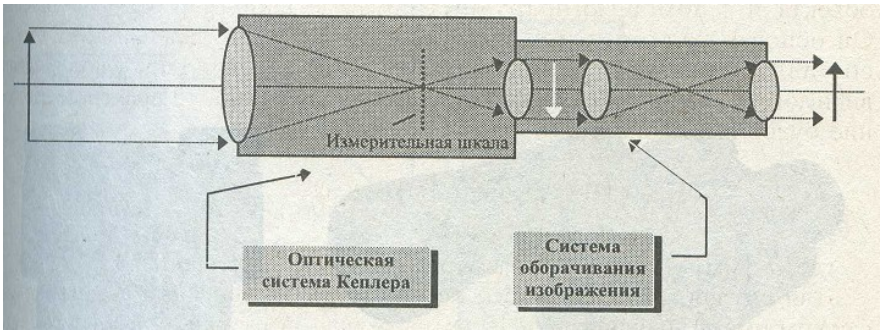



Рис. 9.7.

Для стабилизации изображения визуально-оптические приборы устанавливают на штативе или треноге. В более дорогих приборах применяют электронную стабилизацию изображения, обеспечивающую наблюдение с рук или с движущегося транспорта.

Чтобы улучшить наблюдение при тумане, ярком солнечном освещении или зимой на фоне снега, на окуляры бинокля надеваются желто-зеленые светофильтры. В некоторых биноклях для обнаружения активных инфракрасных приборов ночью применяют специальный экран, чувствительный к инфракрасным лучам.

В последнее время применяются так называемые панкратические бинокли, плавно изменяющиеся увеличение в значительных пределах (от 4 до 20 и более). При этом в обратно пропорциональной зависимости изменяется величина поля зрения. Такие бинокли наиболее удобны для наблюдения: позволяют производить поиск объектов при большом поле зрения, но малом увеличении, а изучение объекта – при большом увеличении.

Для скрытного наблюдения удаленных объектов применяют подзорные трубы и специальные телескопы, имеющие объективы с большим фокусным расстоянием.

## 9.4. Приборы ночного видения

Бинокли позволяют вести наблюдение в светлое время суток. В ночное время могут быть использованы приборы ночного видения, работающие в ближнем инфракрасном диапазоне длин волн (0,8…1 мкм). Структурная схема прибора ночного видения приведена на рис. 9.8.


Рис. 9.8

Для визуально-оптического наблюдения в инфракрасном диапазоне необходимо переместить невидимое для глаз изображение в инфракрасном диапазоне (более 0.76 мкм) в видимый диапазон. Эта задача решается в приорах ночного видения (ПНВ) [8]. Основу приборов ночного видения составляет электронно-оптический преобразователь (ЭОП), преобразующий невидимое глазом изображение объекта наблюдения в видимое изображение. Самый простой ЭОП, так называемый стакан Холста (по имени изобретателя Холста де Бургоса) состоит из двух параллельных пластин, помещенных в стеклянный стакан, из которого выкачан воздух (рис. 9.9).

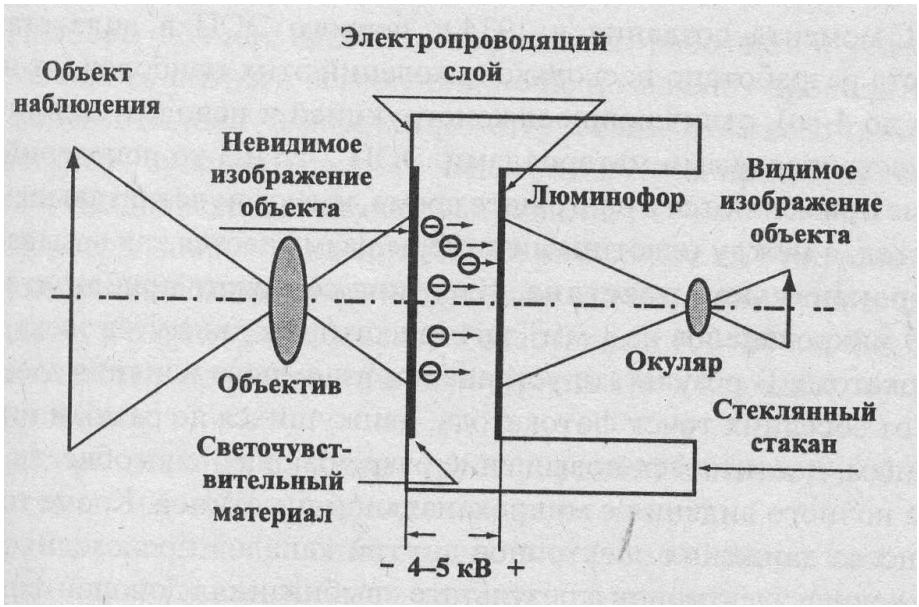



Рис. 9.9

Внешняя сторона первой пластины – фотокатода покрыта светочувствительным материалом (слоем из окиси серебра с цезием), второй представляет металлизированный экран с люминофором. Между пластинами создает сильное электрическое поле разностью электрических потенциалов 4–5 кВ.

На фотокатод объективом проецируется изображение в ИК-диапазе. В каждой точке фотокатода под действием фотонов света возникают свободные электроны, количество которых пропорционально яркости соответствующей точки изображения. Электрическое поле между пластинами вырывает свободные электроны из фотокатода и, разгоняя, устремляет их к экрану с люминофором. В моменты столкновения электронов с люминофором возникают вспышки видимого света, яркость которых пропорциональна количеству электронов. Таким образом, на экране с люминофором формируется видимое изображение, близкое исходному изображению в ИК-диапазоне.

Однако параметры (чувствительность, разрешение) рассмотренного электронно-оптического преобразователя невысокие и не обеспечивают наблюдение при низкой освещенности и, следовательно, добывание демаскирующих признаков об объекте с мелкими деталями.

С момента создания в 1934 году первого ЭОП в виде стакана Холста разработано несколько поколений этих приборов (от нулевого до 4-го). ЭОП 3 и 4-го поколений, которые используются в настоящее время, имеют чувствительный фотокатод, а между пластинами камеры размещается так называемая микроканальная пластина. Пластина содержит приблизительно 5000 микроканалов 1 мм$^2$, внутри которых движутся электроны фотокатода. В результате устранения взаимного влияния электронов от соседних точек фотокатода, движущихся по разным микроканалам, достигается повышение разрешающей способности прибора ночного видения с микроканальной пластиной. Кроме того, в процессе движения электронов внутри каналов происходит «размножение» электронов в результате выбивания их из стенки канала при столкновении с нею движущихся электронов. На основе ЭОП 2 и 3-го поколений созданы различные приборы ночного видения, включающие ночные бинокли и очки, артиллерийские приборы и прицелы для различных образцов военной техники.

Оптическая система аналогична используемым в биноклях. Электрооптический преобразователь преобразует ИК-излучение в видимое изображение, выводя его на встроенный экран. В качестве устройства фиксации изображения выступает человеческий глаз либо фотоаппарат.

Приборы ночного видения могут работать как в пассивном, так и в активном режиме. Пассивный режим применяется при наличии собственного излучения объекта и в условиях, когда освещенность области наблюдения более $10^{-5}$ лк – это уровень освещенности звездной ночи.

Активный режим используется в условиях полного отсутствия освещения. В этом случае для подсветки используется непрерывное или импульсное лазерное излучение в ближнем инфракрасном диапазоне длин волн (0,8…1 мкм).

## 9.5. Фото- и киноаппараты

Визуально-оптическое наблюдение, использующее такой совершенный оптический прибор, как глаз, является одним из наиболее эффективных

способов добывания, прежде всего, информации о видовых признаках. Однако оно не позволяет регистрировать изображение для последующего изучения или документирования результатов наблюдения. Хотя получение документов, подтверждающих тот или иной вид деятельности конкурентов, является важным элементом промышленного шпионажа.

Для этих целей применяют фотографирование и киносъемку с помощью фото и киноаппаратов.

**Фотоаппарат** представляет собой оптико-механический прибор для получения оптического изображения фотографируемого объекта на светочувствительном слое фотоматериала. Все фотоаппараты состоят из светонепроницаемого корпуса с закрепленным на его передней стенке объективом, устройства для размещения или фиксации светочувствительного материала, расположенного у задней стенки корпуса, и затвора.

Так как светочувствительный материал обеспечивает получение качественной фотографии при строго дозированной световой энергии, проецируемой на светочувствительный материал, то затвор пропускает световой поток в течение определенного времени (времени экспозиции или выдержки) от фотографируемого объекта.

Указанные части фотоаппарата являются основными. По мере конструктивного развития фотоаппарат «обрастал» различными узлами и механизмами, которые облегчали и автоматизировали процесс съемки, позволяли расширить возможности применения фотоаппарата, улучшить его технические параметры. Эти узлы и механизмы называют вспомогательными. Подробно об устройстве современных фотоаппаратов можно прочитать в [1].

Профессиональные фотоаппараты известных фирм (Nicon, Canon, Зенит, Kodak, Olympus, Contax, Pentax и др.) представляют собой сложнейшие оптико-электромеханические устройства, автоматически учитывающие все изменения в освещенности объекта во время фотосъемки.

В настоящее время на смену фотоаппаратам, использующим фотопленку, пришли цифровые фотоаппараты. Однако достоинством пленочных фотоаппаратов является возможность достижения большой разрешающей способности, до 500 лин./мм, которой обладают пленки, применяемые в аэрофотосъемке. Это соответствует цифровому фотоаппарату с максимальным разрешением 200 млн. пикселей.

**Цифровой фотоаппарат**. Цифровая фотография вошла в нашу жизнь в начале 90–х годов. Цифровой фотоаппарат представляет собой малогабаритную камеру на ПЗС-матрице (ПЗС - прибор с зарядной связью) электрические сигналы с выхода которой записываются, преобразуются в цифровой вид и запоминаются полупроводниковой памятью фотоаппарата выполненной в виде специальных карт – флэш-карт.

Цифровой электронный фотоаппарат, обладая возможностями классического электромеханического фотоаппарата, предоставляет пользователю дополнительные функции, которые существенно повышают оперативность фотографии. К ним относятся: возможность съемки в непрерывном режиме с, частотой 5–15 кадров/с; запись текстовых и звуковых комментариев; даты и

времени фотосъемки, просмотр изображений в процессе и после съемки на поворачивающемся экране (LCD-панели размером 4–5 см), отображение текущих параметров съемки (числа отснятых кадров, объем свободной памяти, текущий режим компрессии) и др.

Цифровой фотоаппарат также сопрягается с компьютером. Отснятое изображение может отображаться на экране дисплея, редактироваться с помощью графических редакторов, выводиться на печать, передаваться по сети.

Разрешение изображения цифрового фотоаппарата определяется разрешением его светоэлектрического преобразователя и в настоящее время составляет 20…30 млн. пикселей. Это гораздо меньше разрешающей способности лучших пленочных фотоаппаратов (200 млн. пикселей). Однако учитывая перспективы миниатюризации радиоэлектронных элементов, прежде всего «памяти», и повышения разрешения ПЗС, у цифровых фотоаппаратов большое будущее.

Информация о движущихся объектах добывается путем кино- и видеосъемки с помощью киноаппаратов и видеокамер. При киносъемке изображение фиксируется на светочувствительной кинопленке, при видеозаписи – на магнитной пленке.

Под киносъемкой понимают процесс фиксации серии последовательных изображений (кадров) объекта наблюдения через заданные промежутки времени, определяемые частотой кадров в секунду. Каждый кадр кинофильма содержит изображение объекта в момент съемки. Число кадров колеблется от единиц кадров в минуту и даже часов для съемки медленно текущих процессов до сотен тысяч в секунду – для сверхскоростной специальной съемки, например, для наблюдения электрического разряда или полета пули.

**Киноаппараты.** Устройство киноаппарата близко к устройству фотоаппарата с той принципиальной разницей, что в процессе киносъемки пленка скачкообразно продвигается с помощью грейферного механизма перед кинообъективом на один кадр. Закрытие объектива на время продвижения кинопленки осуществляется заслонкой (обтюратором), вращение которой перед объективом синхронизировано с работой грейфера. Киносъемка движущихся людей производится на 8 и 16-мм пленку с частотой 16–32 кадра в секунду.

**Цифровые видеокамеры.** Вместе с цифровыми фотоаппаратами в нашу жизнь в начале 90–х годов вошли и цифровые видеокамеры. В настоящее время выпускается около 600 наименований видеокамер имеющих множество особенностей. По виду используемой памяти их можно разделить на четыре класса: запись информации на магнитную ленту; – на DVD-диск; – на жесткий диск; – на флэш-карту.

## 9.6. Средства телевизионного наблюдения

Средства телевизионного наблюдения используются для дистанционного наблюдения движущихся объектов. Это наиболее совершенный способ получения конфиденциальной информации. Применение специальных миниатюрных телекамер позволяет сделать это наблюдение абсолютно незаметным, ин-

формативным и безопасным. В общем случае схема комплекса средств телевизионного наблюдения может быть представлена в виде, приведенном на рис. 9.10

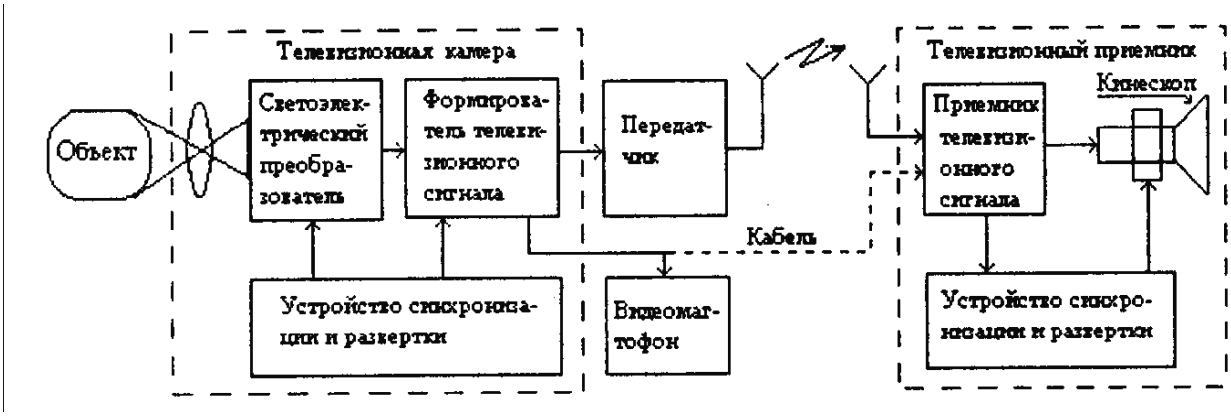



Рис. 9.10

При телевизионном наблюдении изображение объективом проецируется на светочувствительный слой фотокатода вакуумной передающей трубки или мишени твердотельного преобразователя. Фотокатод содержит вещества, из атомов которого кванты световой энергии выбивают электроны, количество которых пропорционально энергии света (яркости элемента изображения). На фотокатоде образуется изображение $Q(x,y,t)$ в виде электрических зарядов, эквивалентное оптическому $B(x,y,t)$ изображению, где $Q$ и $B$ – значения соответственно величины зарядов и яркости в точках с координатами $x$, $y$ в момент времени $t$. В вакуумных телевизионных передающих трубках производится считывание величины заряда с помощью электронного луча трубки, отклоняемого по горизонтали и вертикали магнитными полями. Эти поля создаются отклоняющими катушками, надеваемыми на горловину телевизионной трубки.

За время развития телевидения разработано много типов передающих телевизионных трубок, отличающихся чувствительностью фотокатода и разрешающей способностью. Появление достаточно простых ТВ-трубок типа «видикон» позволило создать компактные телекамеры. Миниатюрные видиконы с диаметром до 15 мм обеспечивают четкость 400–600 линий. На основе видикона разработаны различные варианты телевизионных передающих трубок: плюмбикон, кремникон, суперортикон, изокон и др., обеспечивающие качественное светоэлектрическое преобразование в широком диапазоне длин волн и освещенности.

В начале 70-х годов был открыт и реализован новый принцип построения безвакуумных, твердотельных преобразователей «свет – электрический сигнал», так называемых приборов с зарядовой связью (**ПЗС**). В основу таких приборов положены свойства структуры металл-окисел-полупроводник, называемой МОП-структурой (рис. 9.11).

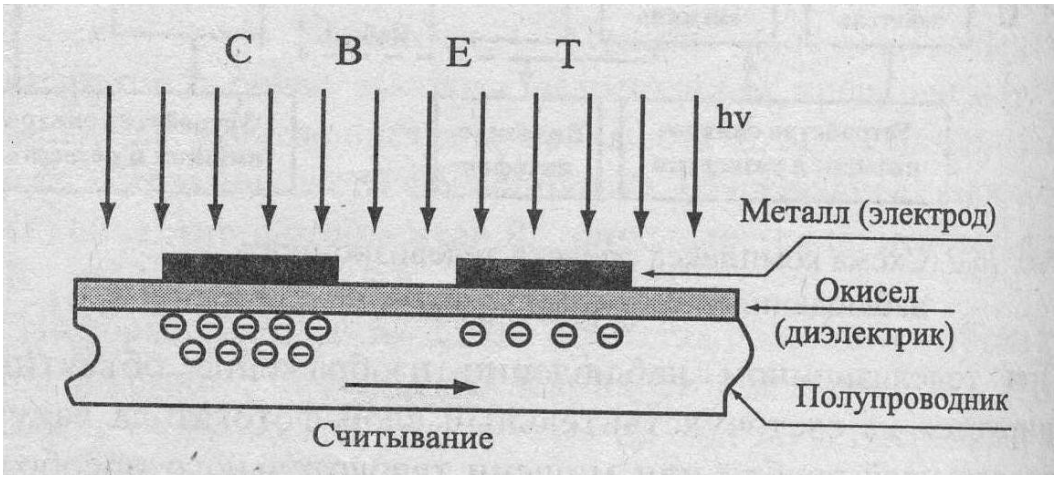



Рис. 9.11

Фотокатод или мишень ПЗС представляет линейку или матрицу из ячеек с МОП-структурами, образованными горизонтальными и вертикальными токопроводящими прозрачными электродами. Размеры каждой ячейки соответствуют размерам элемента изображения. Разрешающая способность ПЗС определяется количеством ячеек, размещающихся в поле изображения.

Считывание зарядов, образующихся в каждой ячейке ПЗС под действием света точек изображения, производится путем последовательного перекачивания зарядов с ячейки на ячейку под действием управляющих сигналов, подаваемых на электроды. В результате этого на выходе ПЗС образуется последовательность электрических сигналов, амплитуда которых соответствует величине заряда на ячейках мишени ПЗС.

Электрический сигнал с выхода вакуумной передающей трубки или ПЗС усиливается и передается по кабелю или в виде радиосигналов к телевизионному приемнику. Последний выполняет обратные функции, преобразуя электрический сигнал в изображение, яркость каждого элемента которого эквивалентна амплитуде соответствующего сигнала. Формирование изображения производится на экране приемной масочной вакуумной трубки (кинескопа) или экране плоских газоразрядных или жидкокристаллических панелей.

## 9.7. Методы противодействия наблюдению

При защите информации от наблюдения в оптическом диапазоне необходимо учитывать факторы, влияющие на вероятность обнаружения (распознавания) объектов наблюдения и ухудшающие точность измерения видовых демаскирующих признаков. Эффективность поиска объектов наблюдения определяется [2]:

- яркостью объекта;
- контрастностью объект/фон;
- угловых размеров объекта;
- угловых размеров поля обзора;
- временем наблюдения объекта;
- скоростью движения объекта.

**Яркость объекта** на входе оптического приемника определяет мощность носителя, превышение которой над мощностью помех является необходимым условием получения изображения с необходимым качеством. Современные приемники имеют чувствительность, соответствующую энергии нескольких фотонов.

**Контрастность объекта** с окружающим фоном является необходимым условием выделения демаскирующих признаков объекта и его распознавания. Рассмотрим понятие контрастности. Контрастность это отношение разности яркости объекта и фона к яркости объекта:

$$K = (B_0 - B_\phi)/B_0,$$

где $B_0; B_\phi$ – яркость объекта и фона соответственно.

Яркость это отношение силы света J, какой либо площадки к её площади $S$:

$$B = J/S.$$

Сила света измеряется в канделах (кандела–кд) и определяется как сила света источника монохроматического излучения частоты $540 \cdot 10^{12}$ Гц (около 1 мкм) излучающего 0,00146 Вт на 1 ср (1 стерадиан это телесный угол с вершиной в центре сферы, вырезающий на поверхности сферы площадь, равную площади квадрата со стороной, по длине равной радиусу этой сферы).

Относительная разность яркостей отдельных спектральных составляющих света от объекта и фона характеризует их цветовой контраст. В видимом и ближнем диапазонах света яркостной контраст на входе оптической системы средства добывания несколько снижается за счет яркости дымки, которую можно рассматривать как помеху. В дальних зонах инфракрасного излучения яркость дымки не оказывает существенного влияния на изменение этого контраста. Контраст может принимать значения в диапазоне 0—1. При К = 0,08-0,1 объект почти сливается с фоном и плохо различается на фоне. Значения цветового контраста объектов и фона могут существенно отличаться в разных длинах волн, что используется в зональной (через цветовые фильтры) аэрофотосъемке.

Например, порог контрастности различимого человеческим глазом объекта по отношению к фону составляет днем –0.01…0.03, ночью – 0.6;

**Угловые размеры.** При поиске объекта его форма не играет большой роли, а имеет значение только его площадь в пределах соотношения сторон от 1:1 до 1:10. Увеличение **угловых размеров** объекта в 2 раза сокращает время, необходимое для его обнаружения, в 8 раз.

**Время для обнаружения объектов** светлее и темнее фона при одинаковых абсолютных значениях контраста примерно одинаковое. С увеличением яркости фона время поиска объекта наблюдателем уменьшается, так как увеличивается разрешающая способность и контрастная чувствительность глаза. Если яркость фона чрезмерно велика, то возникают дискомфорт и ослепление, ухудшающие разрешение и контрастную чувствительность глаза.

С увеличением **поля обзора** увеличивается и время, необходимое для поиска объекта: двукратное увеличение поля обзора повышает время поиска

в 4 раза. При этом время поиска определяется не формой поля, а его угловыми размерами.

**Поиск движущихся объектов** имеет свои особенности: движение ухудшает видимый контраст объекта, величина которого зависит не только от угловой скорости, но и от угловых размеров объекта наблюдения. Чем меньше угловой размер объекта, тем больше влияние **скорости** на время и вероятность обнаружения объекта. Объекты, движущиеся с малой скоростью, обнаруживаются легче, чем неподвижные, а движущиеся с большой скоростью — труднее из-за ухудшения видимого контраста.

Следовательно, в интересах защиты информации об объекте (его демаскирующих признаков) необходимо уменьшать контраст объект/фон, снижать яркость объекта и уменьшать угловые размеры объекта, не допуская наблюдателя близко к объекту. Мероприятия, направленные на уменьшение величины контраст/ фон, называются **маскировкой.**

С учетом этих факторов и общих методов инженерно-технической защиты информации методы защиты информации от наблюдения в оптическом диапазоне указаны на рис. 9.12.

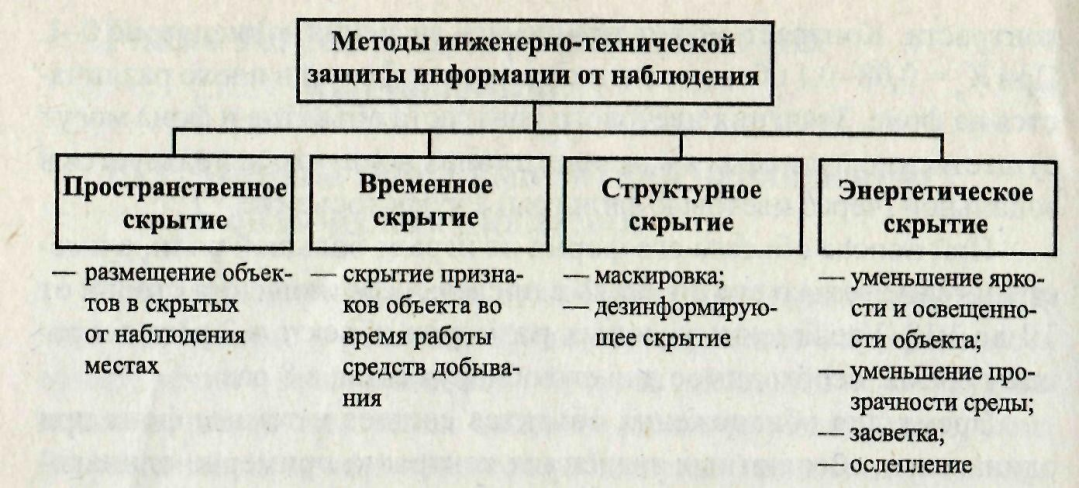



Рис. 9.12. Методы защиты информации от наблюдения

**Пространственное скрытие** обеспечивается размещением объектов защиты в точках (местах) пространства, неизвестных злоумышленнику или недоступных для наблюдения. С этой целью предприятия военно-промышленного комплекса размещали подальше от границ Советского Союза, а районы их нахождения объявлялись зонами, закрытыми для посещения иностранцами. Также для выделенных помещений в здании выбираются комнаты в отсеках с ограниченным допуском в них сотрудников.

**Временное скрытие**. Если время наблюдения известно, то достаточно эффективной мерой является перевод объекта наблюдения в состояние, в котором не проявляются видовые признаки в течение времени наблюдения. Например, при подлете разведывательного КА к полигону, на котором испытывается новая военная техника, работы, в ходе выполнения которых прояв-

ляются видовые демаскирующие признаки, прекращаются до момента выхода КА из зоны наблюдения.

**Структурное скрытие. Маскировка** представляет собой метод структурного скрытия объекта защиты путем изменения его видовых признаков под признаки других объектов (фона). Применяются следующие способы маскировки:

- использование маскирующих свойств местности;
- маскировочная обработка местности;
- маскировочное окрашивание;
- применение искусственных масок;
- нанесение на объект воздушных пен.

Использование маскирующих свойств местности (неровностей ландшафта, складок местности, холмов, гор, стволов и кроны деревьев и т. д.) является наиболее дешевым способом скрытия объектов. Однако для реализации этого способа необходимо наличие в месте нахождения объекта соответствующих естественных масок. Кроме того, маскирующие возможности растительности зависят от времени года. Эффективность маскировки оценивается отношением площади, закрываемой, например, деревьями к площади наблюдаемой зоны.

Если отсутствуют или недостаточны для маскировки природные условия, то возможна дополнительная обработка местности, повышающая ее маскирующие возможности. Она состоит в дерновании (укладке дерна) и посеве травы, создании изгородей из живой растительности, в механической и химической обработке участков местности — распятнении. Обработка местности направлена на изменение фона под основной цвет объекта: на зеленый при дерновании и посеве травы или другой цвет (бурый с различными оттенками, соломенно-желтый) при распятнении.

**Распятнение** достигается расчисткой поверхности почвы от дерна с помощью машин или химическим путем — солями (железным и медным купоросом, бертолетовой солью и др.) и гербицидами. Этот способ имеет ограниченное применение в связи с большой задержкой проявлений маскировочных свойств местности после обработки и вредным воздействием на природу. Например, трава вырастает через несколько недель после посева, а цвет растительности меняется через несколько дней после ее химической обработки.

Маскировочная обработка местности эффективна для скрытия наземных объектов и фона при наблюдении сверху, например, летного поля аэродрома для легких самолетов и вертолетов.

**Маскировочное окрашивание** применяется для изменения цвета объекта, маски или фона и производится путем:

- поверхностной окраски, при которой красочный слой наносится на окрашиваемую поверхность;
- глубинной окраски, при которой краситель пропитывает окрашиваемый материал (ткани, маскировочной сети) или вводятся пигменты при изготовлении материала (цветных цемента, штукатурки, пластмассы и др.).

При поверхностной окраске применяются различные краски, лаки, эма-

ли, битумы, пасты, при глубинной окраске — синтетические красители, порошкообразные пигменты и крупнофракционные цветные материалы (песок, молотые руды).

Различают три вида маскировочного окрашивания:

- защитное;
- деформирующее;
- имитационное.

**Защитное окрашивание** поверхности объекта проводится одноцветной краской под цвет и среднюю яркость фона окружающей местности и предметов возле маскируемого объекта. Цвета защитного окрашивания: хаки, желтовато-серый, серо-зеленоватый, голубовато-серый, оливковый относятся к так называемым универсальным, которые плохо выделяются на фоне разнообразных объектов, прежде всего ландшафта. Однотонный желто-сероватый цвет полевого обмундирования солдат армий многих государств был плохо заметен на растительном, горном, пустынном, городском фонах. Приблизительно такими же возможностями обладал грязно-зеленовато-серый цвет немецкого обмундирования во Второй мировой войне. Защитная окраска оливкового или зеленовато-грязного цвета использовалась как заводская для военной техники.

**Деформирующее окрашивание** предусматривает нанесение на поверхность объекта пятен неправильной геометрической формы 2-3 цветов, имитирующих световые пятна окружающей среды. Различают мелкопятнистую (дробящую) и крупнопятнистую (искажающую контуры) деформирующую окраску. Края цветовых пятен могут быть резко очерченными или расплывчатыми. Деформирующее окрашивание психологически искажает образ защищаемого объекта у наблюдателя и затрудняет обнаружение и распознавание им объекта по признакам его формы. Оно в настоящее время является основным видом маскировки военнослужащих и военной техники армий большинства стран. Выпускается достаточно большое количество вариантов камуфляжа для разных времен года и типов местности. Наряду с маскировочными комбинезонами применяют маскировочные маски для лица или грим, которые наносят на лицо и руки и которые входит в состав маскировочного комплекта войск специального назначения. Деформирующая окраска труднее поддается дешифрованию на пестрых фонах и обеспечивает меньшую вероятность обнаружения и опознавания маскируемых объектов.

При **имитационном окрашивании** цвет и характер пятен на поверхности объекта подбираются под расцветку окружающей местности, объектов или предметов в месте расположения защищаемого объекта. Как правило, этот вид окрашивания применяется для неподвижных объектов: долговременных огневых сооружений, зданий, гидротехнических сооружений и др. В результате маскируемый объект сливается с окружающей местностью или приобретает внешний вид другого объекта. Например, взлетно-посадочная полоса военного аэродрома может быть раскрашена под обычное шоссе или грунтовую дорогу с расположенными возле нее зданиями или иными объектами.

**Маскировочное окрашивание** просто реализуется, но эффект маскировки зависит от сезонных и иных изменений окружающей среды. Кроме того, частое перекрашивание объекта требует больших материальных и временных затрат.

Для маскировки без окрашивания создаются специальные конструкции — искусственные оптические маски, снижающие яркостной и цветовой контраст объекта защиты и фона.

**Энергетическое скрытие** демаскирующих признаков объектов достигается путем:

- уменьшения яркости источников света объекта или освещенности объекта внешними источниками;
- снижения прозрачности среды распространения света от объекта наблюдения до злоумышленника или его технического средства;
- засветки изображения объекта посторонними световыми лучами — помехами;
- ослепления зрительной системы наблюдателя или светоприемника.

Первые два метода относятся к пассивным и приводят к уменьшению уровня светового сигнала на входе оптического приемника. Так как его светочувствительные элементы имеют собственные шумы, то при уровне сигнала ниже собственных шумов обнаружение и распознавание его становятся невозможными.

К активным методам энергетического скрытия относятся **засветка изображения** или **ослепление светочувствительного приемника.** Засветка возникает, когда изображение помехи накладывается на изображение объекта и фона. При этом уменьшается контраст изображения по отношению к фону. Действительно, с учетом яркости помехи $B_п$ на фотографии и экране монитора яркостный контраст будет равен величине:

$$K_я = \frac{B_0 - B_ф}{B_0 + B_п}$$

где $B_о$ и $B_ф$, — значение яркости объекта и фона соответственно.

С увеличением мощности помехи (яркости $B_п$) контраст $K_я \to 0$.

Засветка происходит, когда солнечные лучи попадают на экран монитора компьютера или при наблюдении объектов через освещаемые светом стекла окон помещения или салона автомобиля. При наблюдении через стекло изображение формируется суммой лучей, отраженных от объектов наблюдения и от стекла. Свет от стекла представляет собой помеху. Световой поток от объекта наблюдения уменьшается стеклом, вследствие чего яркость помехи становится больше яркости объекта и фона. Эту разницу увеличивают применением тонированных (затемненных) или «зеркальных» (с алюминиевым или медным напылением) стекол. Тонированные стекла уменьшают $B_о$ и $B_ф$ , а «зеркальные» увеличивают $B_п$. В результате этого контрастность объекта наблюдения уменьшается до величин, при которых объект не виден.

**Засветка.** При превышении мощности помехи на входе приемника значения, соответствующего его динамическому диапазону, возникают искажения информации вплоть до ее полного разрушения. Чрезмерно большая мощ-

ность помехи может привести к необратимым изменениям в светочувствительных элементах. Например, высокочувствительные телевизионные камеры, позволяющие наблюдать за обстановкой при очень малом освещении, могут выйти из строя при попадании на ПЗС-матрицу прямых лучей солнечного света.

Классическим примером ослепления может служить применение наступающими советскими войсками ночью в Берлинской операции 1945 г. 142 прожекторов, свет которых лишил фашистов возможности видеть наступающие войска и эффективно обороняться. Наиболее естественным способом энергетического скрытия является проведение мероприятий, требующих защиты информации о них, ночью. Яркость объектов, имеющих искусственные источники света, снижается путем их выключения или экранирования светонепроницаемыми шторами и экранами.

Энергетическое скрытие объектов, наблюдаемых в отраженном свете, обеспечивают естественные и искусственные маски, а также аэрозоли в среде распространения.

Так как спектральные характеристики объектов и среды различаются для видимого и ИК-диапазонов, то при организации защиты информации от наблюдения в оптическом канале необходимо учитывать диапазон частот носителя информации. Хотя параметры средств визуально-оптического наблюдения (по разрешению, дальности, цвету изображения) в ИК-диапазоне значительно более низкие, чем в видимом, но при наблюдении в нем появляется дополнительный демаскирующий признак объектов, не обнаруживаемый в видимом, — температура поверхности объекта относительно температуры фона.

Естественный фон в ИК-диапазоне можно рассматривать как сложный источник ИК-излучения, характеристики которого зависят от условий освещения, географической широты и долготы, сезона и температуры среды, метеоусловий, природы подстилающей поверхности, времени года и дня и т. п. Отражающая способность ряда природных фонов, таких как трава и листва деревьев, возрастает со смещением максимума излучений в область более длинных волн. Например, отражающая способность травы и листвы в диапазоне волн 0,76-12 мкм выше отражающей способности в видимом диапазоне приблизительно в 5-10 раз, коры — в 3-5 раз. Поэтому объекты, окрашенные маскирующей краской для видимого диапазона, могут хорошо наблюдаться в ИК-диапазоне. Следовательно, при выборе краски необходимо учитывать характер изменения ее коэффициента отражения от длины волны падающего на объект света, в том числе и в ИК-диапазоне.

Кроме того, на яркость объекта с собственными источниками тепла и, следовательно, на его контраст с фоном в ИК-диапазоне влияет температура поверхности объекта. Для его информационной защиты применяются различные теплоизолирующие экраны, в том числе листья деревьев и кустарников, сено, брезент и др. материалы. Хорошими теплоизолирующими свойствами обладают воздушные пены.

# 10. РАДИОЭЛЕКТРОННЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

## 10.1. Виды радиоэлектронной разведки

**Радиоэлектронную разведку** принято делить по следующим видам [2]:

- радиоразведку;
- радиотехническую разведку;
- радиолокационную разведку;
- радиотепловую разведку;
- разведку побочных электромагнитных излучений и наводок (ПЭМИН).

**Радиоразведка** – самый старый вид радиоэлектронной разведки. Она нацелена против различных видов радиосвязи. Основное содержание радиоразведки – обнаружение и перехват открытых, засекреченных, кодированных передач связных радиостанций, пеленгование их сигналов, анализ и обработка добываемой информации с целью вскрытия ее содержания и определения местонахождения источников излучения. Сведения радиоразведки о неприятельских станциях, системах их построения и о содержании передаваемых сообщений позволяют выявлять планы и замыслы противника, состав и расположение его группировок, установить местонахождение их штабов и командных пунктов управления, место размещения баз и стартовых площадок ракетного оружия и др.

**Радиотехническая разведка** – вид радиоэлектронной разведки по обнаружению и распознаванию радиолокационных станций (РЛС), радионавигационных систем и систем связи, использует методы радиоприема, пеленгования и анализа радиосигнала. Средства радиотехнической разведки позволяют:

- Установить несущую частоту передающих радиосредств;
- Определить координаты источников излучения;
- Измерить параметры импульсного сигнала (частоту повторения, длительность и другие параметры);
- Установить вид модуляции сигнала (амплитудная, частотная, фазовая, импульсная);
- Определить структуру боковых лепестков излучения радиоволн;
- Измерить поляризацию радиоволн;
- Установить скорость сканирования антенн и метод обзора пространства РЛС;
- Проанализировать и записать информацию.

**Радиолокационная разведка** – предназначена для получения радиолокационного изображения (обстановки). В радиолокаторе формируется зондирующий узкий, сканирующий по горизонтали и вертикали луч электромагнитной волны, которым облучается пространство с объектом наблюдения. Отраженный от поверхности объекта радиосигнал принимается радиолокатором и модулирует электронный луч электронно-лучевой трубки его индикато-

ра, который, перемещаясь синхронно с зондирующим лучом, «рисует» на экране изображение объекта.

**Радиотепловая** разведка добывает информацию о признаках объектов, проявляющихся через их собственные электромагнитные излучения в радиодиапазоне.

**Разведка ПЭМИН** использует ту же радиоаппаратуру и методы, что и радиоразведка. Только эта аппаратура предназначена для улавливания очень слабых сигналов, то есть она более чувствительная.

**Особенности радиоэлектронной разведки** заключаются в следующем:

- Действует без непосредственного контакта с объектами разведки;
- Охватывает большие расстояния и пространства, пределы которых определяются особенностями распространения радиоволн разных частот;
- Функционирует непрерывно в разное время года и суток и при любой погоде;
- Обеспечивает получение достоверной информации, поскольку она исходит непосредственно от противника (за исключением случаев радиодезинформации);
- Добывает большое количество информации различного характера и содержания;
- Получает информацию в кратчайшие сроки и чаще всего в реальном масштабе времени;
- Малоуязвима и во многих случаях недосягаема для противника;
- Действует скрытно. Противник, как правило, не в состоянии установить факт разведки.

Радиоэлектронная разведка в зависимости от ее целевого назначения подразделяется на **стратегическую и тактическую разведки**.

**Стратегическая** радиоэлектронная разведка ведется в интересах правительственных органов и высшего военного командования с целью добывания всесторонней информации о разведываемой стране через его радиоэлектронные средства. Такая информация необходима для подготовки вооруженных сил и ресурсов страны к войне, принятия решения о начале военных действия и умелого ведения стратегических операций.

**Тактическая** радиоэлектронная разведка считается одним из основных видов обеспечения войск информацией путем непрерывного слежения за электромагнитным излучением многочисленных военных устройств и система противника. Она в состоянии добывать важные сведения для ведения боевых действий силами соединений, частей и подразделений. Различают наземную, морскую, воздушную и космическую радиоэлектронную разведку.

По своему содержанию информация, добываемая этим видом разведки, делится на оперативную и техническую.

Оперативная информация включает сведения, которые необходимы для решения оперативных задач военного командования. К ним относятся:

- открытая или зашифрованная смысловая информация, передаваемая противоборствующей стороной по различным каналам радиосвязи;

- тактико-технические данные и особенности разведываемых активных радиоэлектронных систем (частота настройки, вид модуляции и манипуляции, диаграммы направленности антенн, мощность излучения и т.п.), составляющие их «электронный почерк»;
- типы радиоэлектронных систем: радиосвязи, радиолокации, радионавигации, наведения ракет и дальнего обнаружения, различные телеметрические системы передачи данных;
- количество обнаруживаемых радиоэлектронных систем противника;
- местоположение и территориальная плотность размещения источников излучения электромагнитной энергии противника.

Изучая технические характеристики и особенности радиоэлектронных систем противника, можно определить область их применения и принадлежность. Сопоставляя эти данные с уже известными, полученными разведкой по другим каналам, можно сделать вывод о назначении разведываемых технически средств. Зная это и определяя типы и количество радиоэлектронных средств противника, можно установить дислокацию войсковых частей, военных баз, аэродромов и других объектов. Так, например, зная число радиолокационных станций наведения управляемых зенитных ракет в какой-либо зоне ПВО противника, можно сделать правильные выводы о количестве батарей зенитных ракет, установленных в этой зоне.

Для анализа и обработки добываемой информации очень важное значение имеют точная фиксация времени начала и конца работы излучающих радиоэлектронных средств и правильное определение их местоположения. Эти данные позволяют установить степень активности противника в определенной территориальной зоне. Указывается, что перед запуском межконтинентальных баллистических ракет с мыса Каннаверал наблюдалось заметное увеличения числа источников электромагнитных излучений в этом районе за счет повышения активности работы радиолокационных станций сопровождения и наведения, средств радиосвязи и передачи данных, а также телеметрических сетей. Техническая информация содержит сведения о новых системах оружия и управления радиоэлектронными устройствами и об их электрических характеристиках, используемыми разведываемой страной впервые.

Целью добывания технической информации является своевременная разработка аппаратуры и методов радиоэлектронной разведки новых систем оружия и средств управления противника. По мнению американских специалистов, техническая информация о новой радиоэлектронной аппаратуре потенциальных противников особенно нужна для создания эффективных технических средств и методов радиопротиводействия и контрадиопротиводействия. Для получения такой информации средствами радиоэлектронной разведки ведется систематическая разведка новых, ранее неизвестных источников радиопередач, отличающихся диапазоном частот, видами модуляции и манипуляции, параметрами импульсного сигнала, диаграммой направленности антенны и другими характеристиками.

**Наиболее важными источниками радиоэлектронной разведки**, по мнению зарубежных авторов, являются следующие:

- активные средства радиосвязи, используемые во всех видах вооруженных сил и в интересах управления государством;
- РЛС разных типов и назначений, применяемые, главным образом, в противовоздушной обороне;
- автоматизированные системы управления, слежения и наведения ракетного и противоракетного оружия, а также космических объектов;
- радионавигационные системы, используемые в морской, воздушной и космической навигации;
- различные телеметрические системы передачи информации. Телеметрия это передача информации от объектов по каналам радиосвязи, удалённых от пункта управления на большие расстояния.

## 10.2. Виды радиоэлектронных каналов утечки информации

В радиоэлектронном канале передачи носителем информации является электрический ток и электромагнитное поле с частотами колебаний от звукового диапазона до десятков ГГц.

Радиоэлектронный канал относится к наиболее информативным каналам утечки в силу следующих его особенностей:

- независимость функционирования канала от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими каналами от метеоусловий;
- высокая достоверность добываемой информации, особенно при перехвате ее в функциональных каналах связи (за исключением случаев де информации);
- большой объем добываемой информации;
- оперативность получения информации вплоть до реального масштаб времени;
- скрытность перехвата сигналов и радиотеплового наблюдения.

В радиоэлектронном канале производится перехват радио и электрических сигналов, радиолокационное и радиотепловое наблюдение. Следовательно, в рамках этого канала утечки добывается семантическая информация видовые и, сигнальные демаскирующие признаки. Радиоэлектронные каналы утечки информации используют радио, радиотехническая, радиолокационная и радиотепловая разведка.

Структура радиоэлектронного канала утечки информации в общем случае включает источник сигнала или передатчик, среду распространения электрического тока или электромагнитной волны и приемник сигнала (рис. 10.1).


Рис. 10.1

В радиоэлектронных каналах утечки информации источники сигналов могут быть четырех видов:

- передающие устройства функциональных каналов связи;
- источники побочных электромагнитных излучений и наводок;
- объекты, отражающие электромагнитные волны в радиодиапазоне;
- объекты, излучающие собственные (тепловые) электромагнитные волны в радиодиапазоне.

Средой распространения радиоэлектронного канала утечки информации являются атмосфера, безвоздушное пространство и направляющие электрические провода различных типов и волноводы. Носитель в виде электрического тока распространяется по проводам, а электромагнитное поле – в атмосфере, в безвоздушном пространстве или по направляющим – волноводам.

В приемнике производится выделение (селекция) носителя с интересующее получателя информацией по частоте, усиление выделенного слабого сигнала и съем с него информации – демодуляция.

При перехвате сигналов функциональных каналов связи передатчики этих каналов являются одновременно источниками радиоэлектронных каналов утечки информации. В общем случае направления распространения электромагнитной волны от передатчика к санкционированному получателю и злоумышленнику отличаются. В функциональных каналах связи максимум излучения энергии электромагнитной волны ориентируют в направлении расположения приемника санкционированного получателя. Поэтому мощность источника сигналов радиоэлектронного канала утечки информации, как правило, существенно меньше мощности излучения в функциональном канале связи. В зависимости от способа перехвата информации различают два вида радиоэлектронного канала утечки информации.

В канале утечки 1-го вида производится перехват информации, передаваемой по функциональному каналу связи (рис. 10.2).

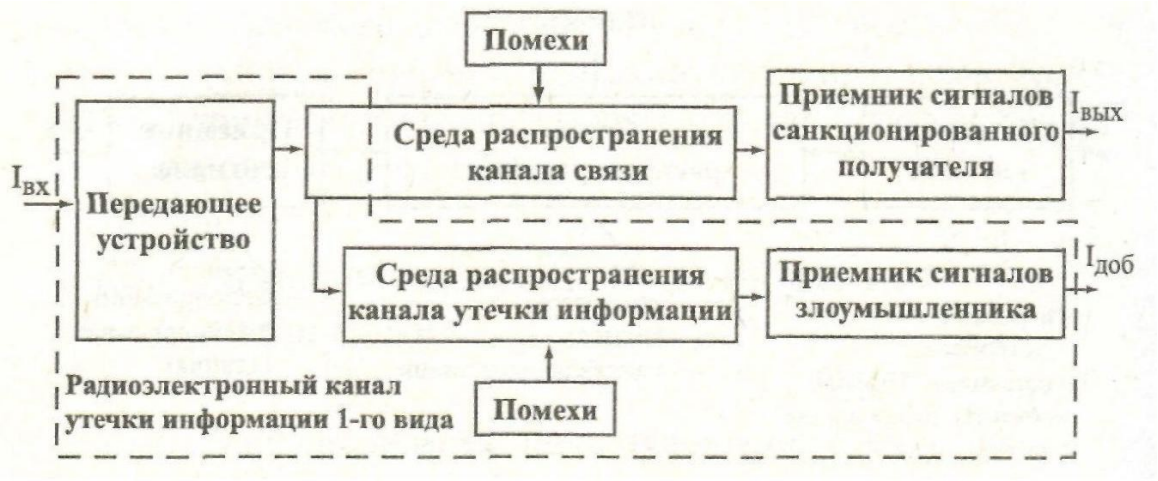



Рис. 10.2

С этой целью приемник сигнала канала утечки информации настраивается на параметры сигнала функционального радиоканала или подключается (контактно или дистанционно) к проводам соответствующего функционального канала. Такой канал утечки имеет общий с функциональным каналом источник сигналов – передатчик. Так как места расположения приемников функционального канала и канала утечки информации в общем случае не совпадают, то среды распространения сигналов в них от общего передатчика различные или совпадают, например, до места подключения приемника злоумышленника к проводам телефонной сети.

Радиоэлектронный канал утечки 2-го вида имеет собственный набор элементов: передатчик сигналов, среду распространения и приемник сигналов (рис. 10.3).


Рис. 10.3

Передатчик этого канала утечки информации образуется случайно (без участия источника или получателя информации) или специально устанавливается в помещении злоумышленником. В качестве такого передатчика применяются источники опасных сигналов и закладные устройства. Опасные сигналы, как отмечалось ранее, возникают на базе акустоэлектрических преобразователей, побочных низкочастотных и высокочастотных полей, паразитных связей и наводок в проводах и элементах радиосредств. Предпосылки для них создаются в результате конструктивных недоработок при разработке радиоэлектронного средства, объективных физических процессов в их элементах, изменениях параметров в них из-за старения или нарушений правил

эксплуатации, не учете полей вокруг средств или токонесущих проводов при их прокладке в здании и так далее. Особенностями передатчиков этого канала являются малые амплитуда электрических сигналов – единицы и доли мВ и мощность радиосигналов, не превышающая десятки мВт (для радиозакладок). В результате этого протяженность таких каналов невелика и составляет десятки и сотни метров. Поэтому для добывания информации с использованием такого канала утечки приемник необходимо приблизить к источнику на величину длины канала утечки или установить ретранслятор. Среда распространения и приемники этого вида каналов не отличаются от среды и приемников каналов первого вида.

## 10.3. Распространение электрических и радиосигналов в радиоэлектронном канале утечки информации

Среда распространения радиоэлектронных каналов утечки существенно различается для **электрических** и **радиосигналов**.

**Электрические сигналы** как носители информации могут быть аналоговыми или дискретными, их спектр может содержать частоты от десятков Гц до десятков ГГц. Электрические сигналы распространяются по **направляющим линиям связи,** связывающим источники и приемники сигналов как внутри организации, так внутри населенного пункта, города, страны, земного шара в целом. Способы и средства передачи электрических сигналов по проводам рассматриваются теорией и техникой проводной связи.

Направляющие линии связи делятся на воздушные проводные линии связи, кабельные линии связи, волноводные линии связи.

**Воздушные проводные линии** связи образуют провода, натянутые в воздушном пространстве между опорами. В зависимости от типа несущих конструкций они делятся на **столбовые и стоечные линии.** Столбовыми называются линии, несущими конструкциями которых являются деревянные или железобетонные опоры. Опорами столбовых линий служат металлические стойки, установленные, например, на крышах зданий. Для изоляции проводов воздушных линий друг от друга и относительно земли их укрепляют на фарфоровых изоляторах. Воздушные линии имеют малый частотный диапазон и подвержены воздействию климатических факторов, например обледенению.

Более широко применяются **кабельные линии** связи. Кабельные линии связи получили доминирующее развитие при организации объектовой, городской и междугородной телефонной связи. Они составляют более 50% телефонных линий России. Наиболее распространены кабели на витой паре и коаксиальные кабели.

**Витая пара** относится к симметричным кабелям и представляет собой два изолированных провода с одинаковыми электрическими параметрами, скрученные вместе. Провода покрываются изоляционным материалом (чаще поливинилхлоридом или полиэтиленом). Тип и толщина слоя изоляционного материала определяют емкость между проводами в кабеле. Телекоммуника-

ционные кабели могут содержать от двух до 3000 витых пар, полностью покрытых изоляционной оболочкой. Витую пару можно представить в виде электрической модели из двух сопротивлений, параллельно одному из которых подключена емкость. Входное сопротивление витой пары зависит от частоты сигнала. В диапазоне частот стандартного телефонного канала оно принимается равным 600 Ом. С увеличением частоты входное сопротивление уменьшается и на высоких частотах определяется как корень квадратный отношения распределенных индуктивности и емкости.

**В коаксиальном кабеле** один проводник концентрически расположен внутри другого проводника, имеющего форму полого цилиндра. Внутренний проводник изолируется от внешнего с помощью различных изоляционных материалов и конструкций. Для изоляции коаксиальных пар кабеля применяется полиэтилен, фтор-лан (фторопласт), полипропилен, резина, неорганическая изоляция. Внешний проводник высококачественной коаксиальной пары образуется фольгой и оплеткой из медной или железной сетки. Для защиты от внешних воздействий он покрывается слоем изолятора (полихлорвинила). Входное сопротивление для подсоединения радиоаппаратуры обычно равно 50 Ом, а для передачи телевизионных сигналов и в связи — 75 Ом. Коаксиальный кабель имеет большую пропускную способность, чем симметричный. Стандартный коаксиальный кабель 1,2/4,4 (с диаметрами внутреннего и внешнего проводников 1,2 и 4,4 мм соответственно) обеспечивает передачу 900-960 телефонных каналов на расстояние до 9 км или 3600 каналов на расстояние 1,5 км. При увеличении диаметров проводников кабеля до 2,6/9,5 число телефонных каналов для длины участка 1,5 км возрастает до 10800. Для повышения частотного диапазона требуется дальнейшее увеличение диаметра коаксиального кабеля. Например, кабель РК 50-17-51 с наружным диаметром изоляции (внешнего проводника) 17,3 мм имеет номинальный коэффициент затухания 0,012, 0,035 и 0,05 дБ/м на частотах 200, 450 и 900 МГц соответственно.

Коаксиальный кабель на высоких частотах имеет лучшие электрические характеристики, чем витая пара. В нем практически отсутствуют перекрестные помехи и намного меньше затухание. Несколько жил, объединенных единым изолятором в виде ленты, образуют **ленточные кабели** или **полосковые линии.**

Основными параметрами проводных линий связи являются **ширина пропускаемого** ими **спектра частот** и **собственное затухание**. Если сопротивление проводников на низких частотах (в звуковом диапазоне) определяется удельным сопротивлением материала и площадью поперечного сечения проводника, то на более высоких частотах начинается сказываться влияние **поверхностного эффекта.** Сущность его заключается в том, что переменное магнитное поле, возникающее при протекании по проводнику тока, создает внутри проводника вихревые токи, В результате этого плотность основного тока перераспределяется по сечению проводника (жилы): уменьшается в центре и возрастает на периферии. Глубина проникновения (в миллиметрах) тока в медную жилу $\theta = 67/\sqrt{f}$, где f – частота колебаний в Гц. На частоте f = 60

кГц глубина проникновения составляет приблизительно 0,3 мм, а на частоте 250 кГц – на порядок меньше, всего около 0,03 мм. Следовательно, ток с этой частотой распространяется по гипотетической тонкой медной трубке с существенно меньшей площадью сечения и, соответственно, большим сопротивлением.

На величину затухания линии влияют также электрические характеристики диэлектрика, наносимого на металлические провода. За счет их удается расширить полосу пропускания линии. При передаче по воздушным линиям со стальными проводами ширина пропускания составляет около 25 кГц, с медными проводами – до 150 кГц, по симметричным кабелям – до 600 кГц. Расширению спектра частот, передаваемых по симметричным цепям, препятствуют возрастающие наводки. Например, удовлетворительным для телефонных линий считается значение переходного затухания порядка 60…70 дБ.

**Металлические волноводы** представляют собой трубы прямоугольного или круглого сечения, внутри которых может распространяться электромагнитное поле от излучателя, установленного в торце одной из сторон волновода. Волноводы применяются для передачи электромагнитного поля с длиной волны короче 10…15 см. Отражаясь от внутренней поверхности волновода, электромагнитное поле концентрируется в волноводе и при движении повторяет его изгибы. С целью уменьшения затухания электромагнитного поля внутренние стенки волновода покрывают тонким слоем серебра. Кроме медных и алюминиевых волноводов находят применение волноводы из пластических масс с металлизированными изнутри стенками.

Основным носителем информации в радиоэлектронном канале является электромагнитное поле.

**Электромагнитное поле** представляет форму движения материи в виде взаимосвязанных колебаний электрического и магнитного полей. Электромагнитное поле возникает при протекании по проводам источника радиосигнала электрического тока переменной частоты и распространяется с конечной скоростью в окружающем пространстве. Векторы напряженности электрического и магнитного полей взаимно перпендикулярны и перпендикулярны направлению распространения электромагнитной волны. Электромагнитная волна характеризуется **частотой колебания, мощностью** и **поляризацией.**

В соответствии с Регламентом радиосвязи, утвержденным на Всемирной административной конференции в Женеве в 1979 г. используется частотная классификация электромагнитных волн (табл. 10.1).

Таблица 10.1

| *Диапазон длин волн* | *Наименование волн* | *Обозначение и наименование частот* | *Диапазон частот* |
|---|---|---|---|
| *1* | *2* | *3* | *4* |
| > 100 км | – | ELF — чрезвычайно низкие | Доли Гц–3 кГц |
| 10–100 км | Мириаметровые | VLF(ОНЧ) — очень низкие | 3–30 кГц |
| 1–10 км | Километровые (длинные) | LF(НЧ) — низкие | 30–300 кГц |
| 100–1000 м | Гектаметровые (средние) | MF(СЧ) — средние | 300–3000 кГц |
| 10–100 м | Декаметровые (короткие) | HF(ВЧ) — высокие | 3–30 МГц |
| 1–10 м | Метровые | (ОВЧ) — очень высокие | 30–300 МГц |
| 10–100 см | Дециметровые | UHF(УВЧ) — ультравысокие | 300–3000 МГц |
| 1–10 см | Сантиметровые | SHF(СВЧ) — сверхвысокие | 3–30 ГГц |

Поляризация электромагнитной волны определяется направлением вектора напряженности электрического поля. Если вектор электрического поля лежит в вертикальной плоскости, то поляризация вертикальная, когда он находится в горизонтальной плоскости, то – горизонтальная. Промежуточное положение характеризуется углом поляризации между плоскостями поляризации и распространения. **Плоскостью поляризации** называется плоскость, в которой находятся вектора электрического поля и вектор распространения электромагнитной волны.

**Мощность излучения** электромагнитного поля тем выше, чем ближе частота колебаний в распределенном контуре, образованном индуктивностью проводников и распределенной емкостью между ними и землей, к частоте сигнала. Эффективное преобразование энергии электрических сигналов в электромагнитную волну выполняется **антеннами.**

Характер поляризации электромагнитной волны зависит от конструкции и расположения излучающих элементов антенны. Несоответствие поляризации электромагнитной волны пространственной ориентации элементов приемной антенны, в которых наводятся электрические заряды, приводит к уменьшению величины этих зарядов.

Радиоволны в зависимости от характера распространения делятся на **земные (поверхностные), прямые, тропосферные** и **ионосферные (пространственные).**

**Земными** называются радиоволны, которые распространяются в непосредственной близости от поверхности Земли и частично огибают ее поверхность в результате дифракции. **Прямыми** названы радиоволны, распространяющиеся прямолинейно в атмосфере и космосе. Радиоволны, которые распространяются в тропосфере – приземной неоднородной области атмосферы не выше 10-12 км от поверхности Земли, называются тропосферными. В тропосфере происходит рассеивание, а также частичное искривление траектории и отражение радиоволн от неоднородностей тропосферы.

**Ионосферными** называют радиоволны, распространяющиеся в результате преломления их в ионосфере и отражений от земной поверхности. Ионосферу образуют ионизированные под действием ультрафиолетового излучения Солнца верхние слои атмосферы.

В ионосфере происходит преломление, отражение и поглощение радиоволн. Преломление радиоволн обусловлено изменениями диэлектрической проницаемости, и, следовательно, показателя преломления по высоте слоев. По мере распространения радиоволн от наземного источника через более высоко расположенные слои показатель преломления уменьшается, траектория электромагнитной волны искривляется и при определенных условиях волна возвращается на Землю.

Преломление радиоволн на той или иной высоте ионосферы зависит от частоты радиоволн и угла их падения на слой. При прочих равных условиях, чем больше угол падения волны, отсчитываемый от вертикальной линии в точке падения, тем более пологая траектория луча в ионосфере и тем меньшая электронная концентрация потребуется для возвращения луча на Землю. Минимальное значение угла падения, при котором еще возможно отражение радиоволн заданной частоты от ионосферы, называется **критическим.** При угле падения меньше критического, радиоволны проходят через ионосферу в космос.

Так как коэффициент преломления уменьшается с увеличением частоты, то длинные волны преломляются сильнее, чем короткие, а для УКВ преломление недостаточно для возвращения волн на Землю и они уходят в космическое пространство. Наивысшая частота, при которой электромагнитная волна еще может возвратиться на Землю, называется **максимально применимой частотой** и составляет примерно 20…40 МГц**.** Но значение этой частоты неоднозначно вследствие зависимости ее от угла падения. Поэтому вводят понятие **критической частоты,** которая является максимально применимой частотой при угле падения 0 градусов и составляет около 10 МГц. Из определения следует, что эта частота представляет собой наименьшую частоту из всех максимально применимых частот.

За счет многократного преломления радиоволн в ионосфере и отражения от земной поверхности электромагнитная волна может распространяться на большие расстояния, вплоть до огибания Земли. Но при таком распространении волны на земной поверхности возникают зоны молчания, в которые не попадают отраженные от ионосферы электромагнитные волны. В зонах приема происходит интерференция волн, прошедших разный путь от излучателя и

имеющих, следовательно, различные фазы. Случайный характер изменения фаз приводит к случайному изменению амплитуды результирующей волны, которое называется **замиранием** или **федингом.**

Кроме замираний существуют зоны молчания, когда поверхностная волна уже не доходит, а пространственной волны еще нет из-за наличия критического угла.

Степень поглощения радиоволн в атмосфере увеличивается при повышении плотности ионизации, частоты колебания и пути, проходимой радиоволной в ионосфере. Зимой, когда концентрация электронов в связи с понижением солнечной радиации уменьшается, поглощение радиоволн снижается, и дальность распространения увеличивается.

В зависимости от частоты колебания радиоволн характер их распространения имеет следующие особенности.

**Километровые** (длинные 30…300 кГц) волны подвержены дифракции, сравнительно слабо поглощаются земной поверхностью и могут распространяться поверхностным лучом на расстояние до 3000 км. В ионосфере они затухают сильнее, но могут отражаться от слоя Е и распространяться пространственным лучом на большее расстояние. К преимуществам электромагнитной волны в этом диапазоне как носителя информации относится, кроме большой дальности распространения, сравнительное постоянство напряженности поля в пункте приема в течение суток и года, что обеспечивает устойчивость связи. Эти волны применяются также для связи под водой, где сильно затухают волны более высоких частот.

Недостатком длинноволновой радиолинии является плохая излучательная способность антенн даже при больших размерах, достигающих несколько сотен метров, высокий уровень атмосферных и промышленных помех и малая пропускная способность.

**Гектометровые** (средние 300…3000 кГц) волны могут распространяться поверхностным и пространственным лучами. Энергия средних волн поглощается земной поверхностью сильнее, чем длинноволновых, поэтому дальность связи поверхностным лучом составляет примерно 500-1500 км. Однако для средних волн создаются более благоприятные условия распространения пространственным лучом, для которого прием сигналов возможен до 4000 км.

Условия распространения средних волн существенно изменяются в зависимости от времени суток. В ночные часы за счет преломления в ионосфере дальность распространения выше, чем в дневные, когда преобладают поверхностные волны. В этом диапазоне наблюдаются замирания в результате интерференции земных и поверхностных волн или пространственных волн с различными путями распространения, высокий уровень атмосферных и промышленных помех. Антенны в среднем диапазоне по устройству в основном такие же, как и антенны в длинноволновом, но в силу большей близости их геометрических размеров к длинам волн имеют больший коэффициент усиления. Радиоволны в этом диапазоне используются для радиовещания и связи, на флоте и в авиации.

**Короткие волны.** При распространении коротких (3…30 МГц) волн дальность поверхностного луча невелика из-за резкого возрастания поглощения энергии землей. Поле в точке приема создается в основном за счет преломления в различных слоях ионосферы. В результате флюктуации плотности и высоты слоев и взаимодействия лучей на коротких волнах, как правило, наблюдаются глубокие замирания и даже полное пропадание связи в течение единиц и десятков секунд. Для обеспечения круглосуточной связи в условиях суточного изменения ионосферы необходимо производить периодическую смену частот. Определение оптимальных частот производится специальными службами наблюдения за ионосферой по результатам вертикального и вертикально-наклонного зондирования ее радиоимпульсами. Наиболее благоприятные условия прохождения волн днем чаще складываются на волнах в интервале 10…25 м, а ночью – 35…70 м.

В диапазоне коротких волн на напряженность поля и характер ее изменения в точке приема влияют другие явления, такие как «вспышки» на Солнце, рассеяние волн на мелких неоднородностях ионосферы, поворот плоскости поляризации. Достоинством коротких волн является возможность обеспечения связи на очень большие расстояния при сравнительно малых мощности передатчика и габаритах антенны, а также малое влияние атмосферных и промышленных помех. Они применяются для связи, радионавигации, радиовещания и радиолюбителями.

**Ультракороткие волны.** В диапазоне ультракоротких (метровых, декаметровых, сантиметровых 30…30000 МГц) волн практически отсутствует дифракция. Поэтому они распространяются в пределах прямой видимости. Радиоволны в этих диапазонах являются основными носителями информации в сетях телекоммуникаций в силу следующих особенностей:

- имеют широкий частотный диапазон (см. табл. 4.1), обеспечивающий возможность передачи большого объема информации, в том числе путем использования широкополосных каналов;
- низкий уровень атмосферных и промышленных помех, позволяющих использовать приемные устройства с высокой чувствительностью, что повышает дальность приема;
- слабое влияние станционных помех на работу других радиосистем вследствие ограниченности их радиуса видимости;
- возможность создания небольших антенн с узкой диаграммой направленности, позволяющих осуществлять радиосвязь при относительно малой мощности передающих устройств.

Основной недостаток радиоволн рассматриваемого диапазона – существенно большее поглощение их в атмосфере, в том числе природными осадками (дождем, туманом, снегом, градом), особенно в сантиметровом диапазоне, и, как следствие, относительно малая дальность распространения.

Электрические сигналы как носители информации могут быть аналоговыми или дискретными, их спектр может содержать частоты от десятков Гц до десятков ГГц.

Наиболее широко применяются сигналы, ширина спектра которых соответствует ширине спектра стандартного телефонного канала. Такие сигналы передают речевую информацию с помощью телефонных аппаратов и распространяются по направляющим линиям связи, связывающим абонентов как внутри организации, так внутри населенного пункта, города, страны, земного шара в целом.

Повышение дальности связи в УКВ-диапазоне обеспечивается путем:

- подъема передающей или приемной антенн с помощью инженерных конструкций (матч, башен) и аэростатов;
- ретрансляции радиосигналов с помощью наземных и космических ретрансляторов;

Передающие антенны на башнях устанавливаются для постоянного обеспечения связи, радио- и телевизионного вещания в городах, районах и областях. Для периодического и эпизодического приема сигналов от отдаленных источников в качестве носителей приемников сигналов используют также привязные аэростаты. Информация с них на землю передается по кабелю или радиоканалу.

Для передачи информации в УКВ-диапазонах частот на большие расстояния широко применяются ретрансляторы. С помощью наземных ретрансляторов создаются **радиорелейные линии (РРЛ),** представляющие собой цепочку приемно-передающих станций, каждая из которых устанавливается в пределах прямой видимости соседних. Все станции РРЛ разделяются на **оконечные, промежуточные** и **узловые.** Оконечные радиорелейные станции располагаются в начале и конце линии. На этих станциях вводится и выделяется информация, обеспечивается распределение информации между потребителями. Промежуточные станции предназначены для ретрансляции сигналов. Узловые радиорелейные станции – это промежуточные станции, на которых происходит разветвление принимаемых сигналов по различным направлениям, выделение части передаваемой информации (например, программ телевидения) и введение новой информации.

Диапазоны частот, предназначенных для передачи информации одного вида, объединяются в радиочастотный ствол: телевизионный, телефонный и т. д. Существующие отечественные РРЛ могут содержать до 8 стволов, а один ствол, например, телефонный – до 1920 телефонных каналов. Для каждого ствола с целью исключения взаимного влияния выделяются две рабочие частоты – для передачи и приема. Принятые каждой станцией сигналы на частоте приема усиливаются и преобразуются в частоту передачи, на которой излучаются в направлении следующей станции. Радиорелейная связь обеспечивает около 30% телефонных каналов России.

Для повышения дальности в **тропосферных линиях связи** используют явление рассеяния ультракоротких радиоволн в неоднородностях тропосферы. К таким неоднородностям относятся области тропосферы с резко изменившимися значениями диэлектрической проницаемости. Неоднородности вызываются неравномерностью состояний различных точек тропосферы, непрерывным перемешиванием и смещением воздушных масс в результате не-

равномерного разогрева Солнцем различных участков поверхности Земли и слоев тропосферы. Для устойчивой тропосферной радиосвязи применяют антенны с высоким коэффициентом усиления (40-50 дБ), мощные передатчики (1-10 кВт) и высокочувствительные приемники. Тропосферные линии связи чаще всего имеют протяженность 140-500 км.

Ретрансляторы, устанавливаемые на **искусственных спутниках Земли (ИСЗ),** наиболее широко используются для обмена информацией между абонентами, удаленными друг от друга на тысячи километров. Они являются элементами (звеньями) спутниковых систем связи, которые содержат также оконечные наземные передающие и приемные станции. Естественно, что связь возможна лишь в том случае, если спутники находятся в зоне видимости обеих земных станций. Для ретрансляции радиосигналов применяются **космические аппараты (КА)** на геостационарной (стационарной) и эллиптической орбитах, а также низкоорбитальные КА.

При распространении радиоволн в городе характер их распространения существенно искажается по сравнению с распространением на открытых пространствах за счет многочисленных переотражений от стен зданий и помещений и затухания в них. Эти обстоятельства необходимо учитывать при оценке пространственной ориентации и возможностей каналов утечки информации. Экранирующие свойства некоторых элементов здания приведены в таблице. 10.2.

Таблица 10.2

| *Тип здания* | *Ослабление, дБ на частоте* | | |
|---|---|---|---|
| | *100 МГц* | *500 МГц* | *1 ГГц* |
| Деревянное здание с толщиной стен 20 см | 5–7 | 7–9 | 9–11 |
| Кирпичное здание с толщиной стен 1,5 кирпича | 13–15 | 5–17 | 16–19 |
| Железобетонное здание с ячейкой арматуры 15 × 15 см и толщиной 160 мм | 20–25 | 18–19 | 15–17 |

Указанные в таблице данные получены для стен, 30% площади которых занимают оконные проемы с обычным стеклом. Если оконные проемы закрыты металлической решеткой с ячейкой размером 5 см, то эффективность экранирования увеличивается на 30-40 %. Экранирующие свойства кирпичных и железобетонных стен зданий в 2-3 раза выше, чем деревянных.

## 10.4. Средства перехвата радиосигналов

Перехват электромагнитного, магнитного и электрического полей, а также электрических сигналов с информацией осуществляют органы добывания

радио- и радиотехнической разведки [2, 9]. При перехвате решаются следующие основные задачи:

- поиск в пространстве и по частоте сигналов с нужной информацией;
- 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. 10.4.

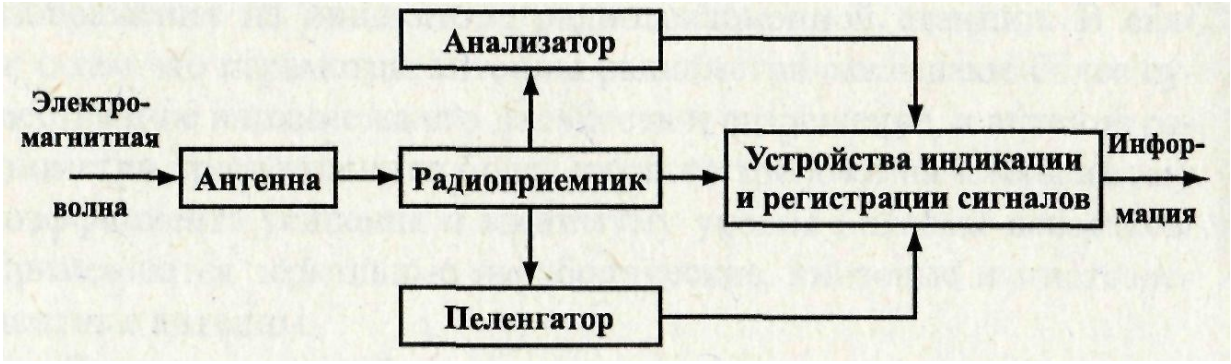



Рис. 10.4

Типовой комплекс включает:

- приемные антенны;
- радиоприемник;
- анализатор технических характеристик сигналов;
- радиопеленгатор;
- регистрирующее устройство.

Антенна предназначена для пространственной селекции и преобразования электромагнитной волны в электрические сигналы, амплитуда, частота и фаза которых соответствуют аналогичным характеристикам электромагнитной волны.

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.

Для анализа радиосигналов после частотной селекции и усиления они подаются на входы измерительной аппаратуры анализатора, определяющей параметры сигналов: частотные, временные, энергетические, виды модуляции, структуру кодов и др.

Радиопеленгатор предназначен для определения направления на источник излучения (пеленг) или его координат.

Регистрирующее устройство обеспечивает запись сигналов для документирования и последующей обработки.

**Приемные антенны.** Антенны представляют собой электромеханические конструкции из токопроводящих элементов, размеры и конфигурация которых определяют эффективность преобразования электрических сигналов в радиосигналы (для передающих антенн) и радиосигналов в электрические сигналы (для приемных антенн).

Возможности антенн, как приемных, так и передающих, определяются следующими электрическими характеристиками:

- диаграммой направленности и ее шириной;
- коэффициентом полезного действия;
- коэффициентом направленного действия;
- коэффициентом усиления;
- полосой частот.

**Диаграмма направленности** представляет собой графическое изображение уровня излучаемого (принимаемого) антенной сигнала в зависимости от направления излучения в горизонтальной и вертикальной плоскостях. Диаграммы изображаются в прямоугольных и полярных координатах (см. рис. 10.5).

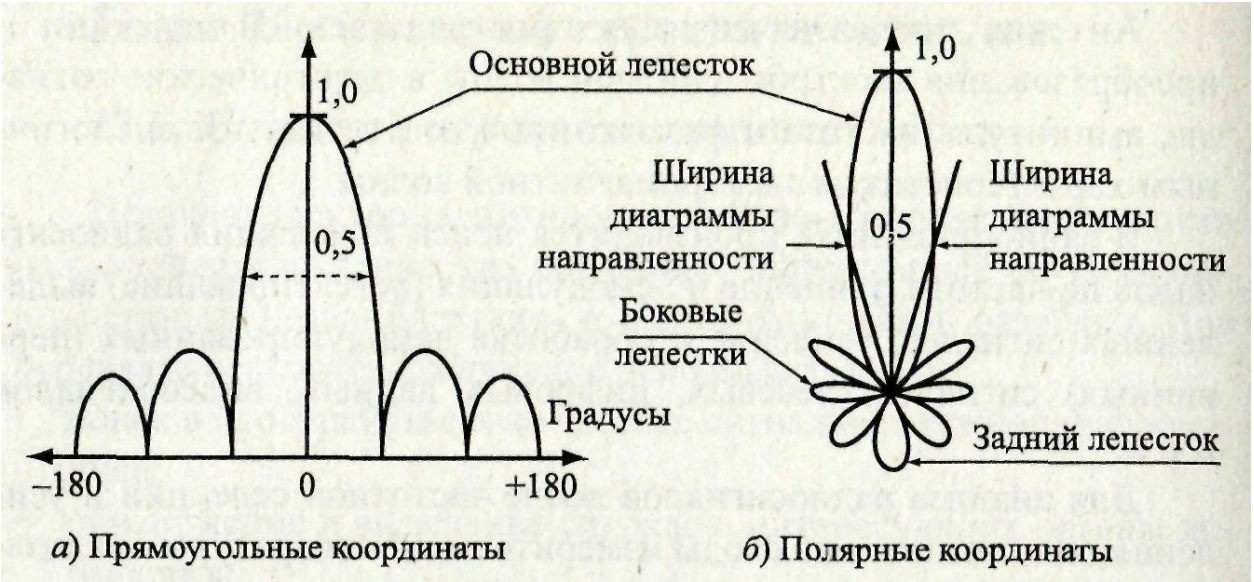



Рис. 10.5

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 мощности основного лепестка по сравнению с остальными характеризует направленные свойства антенны. Ширина главного лепестка диаграммы измеряется углом между прямыми линиями, проведенными из начала полярных координат до значений диаграммы, соответствующих

половине максимальной мощности излучения или 0,7 напряжения электрического сигнала приемной антенны. Чем меньше 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 антенной.

Потери электрической энергии в антенне оцениваются **коэффициентом полезного действия (КПД),** равного отношению мощности сигнала на выходе реальной антенны к мощности сигнала идеальной антенны без потерь.

Произведение этих двух коэффициентов определяет **коэффициент усиления** антенны (КУ). Так как КНД > 1, а КПД < 1, то коэффициент усиления в зависимости от значений сомножителей может теоретически принимать значения как меньше, так и больше 1. Чем выше КУ, тем больший энергетический эффект обеспечивает антенна, но тем точнее необходимо ориентировать направление основного лепестка на источник излучения.

Для обеспечения эффективного излучения и приема в широком диапазоне используемых радиочастот создано большое количество видов и типов антенн, классификация которых представлена на рис. 10.6.

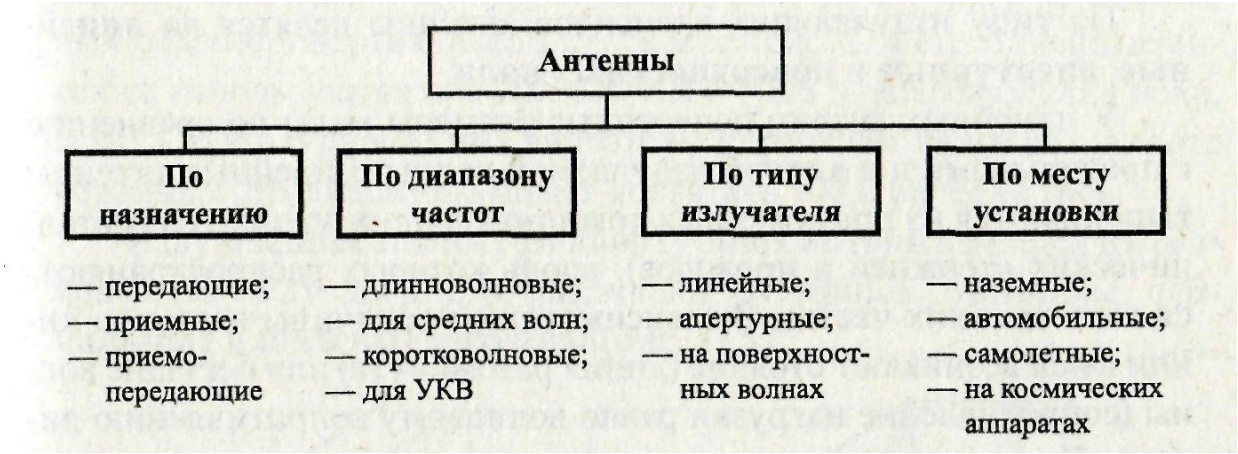



Рис. 10.6

Назначение передающих и приемных антенн ясно из их наименований. По своим основным электрическим параметрам они не различаются. Многие из них в зависимости от схемы подключения (к передатчику или приемнику) могут использоваться как передающие или приемные, например антенны радиолокационных станций. Однако если к передающей антенне подводится большая мощность, то в ней принимаются специальные меры по предотвращению пробоя между элементами антенны, находящимися 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 $\lambda/4$, где $\lambda$ – длина волны электромагнитного колебания. Разме-

ры и конструкция антенн различаются 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 ($\lambda/4$) 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 данным [2], укорочение длины этой антенны в 2 раза уменьшает её эффективность до 60%, в 5 раз (до 50 см) – до 10%, а эффективность антенны, укороченной в 10 раз, составляет всего около 3% от рационального варианта.

**Радиоприемники.** Радиоприемник – основное техническое средство перехвата, осуществляющее 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.

**В приемниках прямого усиления** сигнал на входе приемника (выходе антенны) селектируется и усиливается без изменения его частоты. Структурная схема приемника прямого усиления (рис. 10.7) включает в себя входную цепь, усилитель высокой частоты (УВЧ), детектор (Д) и усилитель низкой частоты (УНЧ).

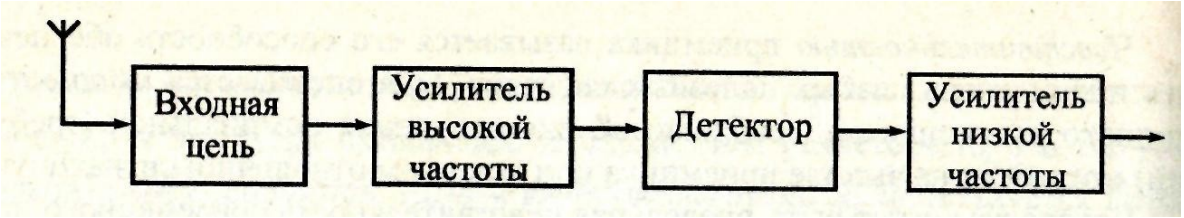



Рис. 10.7

Входная цепь и УВЧ составляют высокочастотный тракт приемника и содержат системы резонансных контуров, которые выделяют требуемый сигнал из множества других сигналов и помех. УВЧ, кроме высокочастотной селекции сигнала, осуществляет его усиление. В некоторых случаях при достаточной мощности принимаемого сигнала УВЧ может отсутствовать. Такие приемники применялись ранее (в начале 20-го столетия) и носили название «де-

текторных», поскольку в них не осуществлялось усиление ни на высокой, ни на низкой частотах и принятый антенной сигнал поступал непосредственно на амплитудный детектор. В настоящее время детекторные приемники используются в измерительной или регистрирующей технике СВЧ диапазона.

Термин «приемник прямого усиления» подчеркивает ту его особенность, что селекция и усиление производятся на несущей частоте принимаемого радиосигнала. Приемник прямого усиления имеет ряд существенных недостатков. В частности, для обеспечения высокой избирательности приходится увеличивать число высокодобротных резонансных контуров, что усложняет перестройку приемника по диапазону. Поэтому приемники прямого усиления находят ограниченное применение.

Сложность проблемы обеспечения избирательности в радиоприемниках прямого усиления обусловлена техническими трудностями создания одновременно перестраиваемых по частоте узкополосных фильтров с высокими показателями по селективности, в особенности при их промышленном производстве.

**В супергетеродинном приемнике** проблема одновременного обеспечения высоких значений чувствительности и селективности решена путем преобразования принимаемого высокочастотного сигнала после его предварительной селекции и усиления в усилителе высокой частоты в сигнал постоянной частоты, называемой промежуточной частотой (рис. 10.8).


Рис. 10.8

Усиление и селекция сигналов после преобразования выполняются на промежуточной частоте. Для постоянной промежуточной частоты задачи по обеспечению высокой избирательности и чувствительности решаются проще и лучше.

Преобразователь частоты состоит из гетеродина и смесителя. Гетеродин представляет собой перестраиваемый вручную или автоматически высокочастотный генератор гармонического колебания с частотой, отличающейся от частоты принимаемого сигнала на величину промежуточной частоты. Процесс преобразования частоты происходит в смесителе, основу которого составляет нелинейный элемент (полупроводниковый диод, транзистор, радиолампа). На него поступают принимаемый сигнал с частотой $f_C$ и гармониче-

ский сигнал гетеродина с частотой $f_Г$, На выходе смесителя возникает множество комбинаций гармоник принимаемого сигнала и колебаний гетеродина, в том числе на промежуточной частоте $f_П = f_С – f_Г$. Селективные фильтры усилителя промежуточной частоты пропускают только сигналы промежуточной частоты, которые усиливаются до величины, необходимой для нормальной работы детектора. В длинноволновом и средневолновом радиовещательном диапазонах $f_П$ = 465 кГц, в УКВ – 10 МГц и более.

Однако супергетеродинному приемнику присущ ряд недостатков, вызванных процессом преобразования частоты. Основной из них состоит в том, что фильтры усилителя промежуточной частоты пропускают не только полезные сигналы, частота которых равна $f_С = f_Г + f_П$, но и ложные с частотой $f_С = f_Г – f_П$ симметричной («зеркальной») по отношению к частоте гетеродина. Помехи на «зеркальной» частоте ослабляются путем двойного или даже тройного преобразования частот в супергетеродинном приемнике. Промежуточная частота каждого последующего преобразования понижается. В результате этого первую промежуточную частоту можно без ущерба для избирательности приемника выбрать достаточно высокой. При больших значениях промежуточной частоты «зеркальная» частота существенно отличается от сигнала и подавляется входными фильтрами радиоприемника.

Основными техническими характеристиками радиоприемника являются:

- диапазон принимаемых частот;
- чувствительность;
- избирательность;
- динамический диапазон;
- качество воспроизведения принимаемого сигнала (уровни нелинейных и фазовых искажений);
- эксплуатационные параметры.

**Диапазон принимаемых частот** обеспечивается шириной полосы пропускания селективных элементов входных фильтров и интервалом частот гетеродина. Настройка приемника на нужный диапазон или поддиапазон частот производится путем переключения элементов входных контуров и контура гетеродина, а настройка на частоту внутри диапазона (поддиапазона) – путем изменения частоты гетеродина. В радиоприемниках все шире в качестве гетеродина используется устройство – синтезатор частот, создающее множество (сетку) гармонических колебаний на стабилизированных фиксированных частотах с интервалом, соответствующих шагу настройки частоты приемника.

**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). Такая чувствительность называется реальной. Предельная чувствительность соответствует мощности (напряжения) входного сигнала, равного мощности (напряжению) шумов входных цепей радиоприемника. Информация полезного сигнала мощностью менее мощности шумов радиоприемника настолько сильно ими

искажается, что передача информации возможна только при кодировании ее специальными помехоустойчивыми кодами.

В диапазонах дециметровых и более коротких волн чувствительность измеряют в ваттах или децибелах по отношению к уровню в 1 мВт (дБм), на метровых и более длинных – в микровольтах (мкВ). Реальная чувствительность современных профессиональных супергетеродинных приемников дециметровых и сантиметровых волн составляет $10^{-12...}10^{-15}$ Вт, приемников метровых и более длинных волн – 0,1…10 мкВ.

**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). Практически реализовать это требование чрезвычайно трудно, так как спектр сигналов с различной информацией имеет изрезанную постоянно меняющуюся форму, и существуют большие технически проблемы при формировании амплитудно-частотной характеристики сложной заданной формы. В качестве идеальной АЧХ рассматривается П-образная форма с шириной, равной средней ширине спектра сигнала.

Основными показателями избирательности являются избирательность по соседнему каналу и избирательность по зеркальному каналу приема. Для бытовых приемников этот показатель должен соответствовать 60 дБ.

Избирательность реального приемника оценивается двумя основными показателями: шириной полосы пропускания и коэффициентом прямоугольности АЧХ радиоприемника, реальная форма которой имеет колоколообразный вид.

Ширина полосы пропускания измеряется на уровне 0,7 по напряжению, а коэффициент прямоугольности оценивается отношением полосы пропускания на уровне 0,1 к полосе пропускания на уровне 0,7. Чем более пологой является АЧХ радиоприемника, тем шире полоса пропускания на уровне 0,1 по отношению к уровню 0,7 и тем больше величина коэффициента прямоугольности. Коэффициент пропускания позволяет количественно оценить пологий характер амплитудно-частотной характеристики радиоприемника. Чем ближе коэффициент прямоугольности АЧХ к 1, тем круче ее скаты и тем меньше помех «пролезет» по краям полосы пропускания. С целью уменьшения мощности помех, прошедших в тракт приемника, ширину его полосы пропускания устанавливают соответствующей ширине спектра сигнала. В приемниках для приема сигналов, существенно отличающихся по ширине, например речи и телеграфа, ширину полос пропускания различных селективных цепей изменяют путем коммутации селективных элементов (катушек индуктивности, конденсаторов).

Так как активные элементы усилительных каскадов радиоприемника (транзисторы, диоды и др.) имеют достаточно узкий интервал значений вход-

ных сигналов, при которых обеспечивается их линейное преобразование, то при обработке сигналов с амплитудой вне этих интервалов возникают их нелинейные искажения, в результате которых искажается информация. Возможность приемника обрабатывать с допустимым уровнем нелинейных искажений входные радиосигналы, отличающиеся по амплитуде, характеризуется **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 в радиоприемнике вызываются неодинаковыми изменениями с оставляющих спектра входного сигнала. Из-за частотных искажений сигнал на входе демодулятора искажается, что приводит к изменению содержащейся в нем информации.

Фазовые искажения сигнала возникают из-за нарушений фазовых соотношений между отдельными спектральными составляющими сигнала при прохождении его цепями тракта приемника.

Искажения, проявляющиеся в появлении в частотном спектре выходного сигнала дополнительных составляющих, отсутствующих во входном сигнале, называются нелинейными. 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 к его динамическому диапазону. Эти виды искажений приводят к изменению информационных параметров сигнала на входе демодулятора и, как следствие, к искажению информации после демодуляции.

Традиционные аналоговые радиоприемники постепенно вытесняются цифровыми, в которых сигнал преобразуется в цифровой вид с последующей его обработкой средствами вычислительной техники.

## ЛИТЕРАТУРА


1. Хореев А.А. Технические средства и способы промышленного шпионажа – М: ЗАО «Дальснаб», 1997. – 230 с.
2. Инженерно-техническая защита информации: Учебное пособие для вузов / А. А. Торокин. - М.: Гелиос АРВ, 2005. – 958 с.
3. Методологические, организационные и правовые основы информационной безопасности: Коллективная монография. / Под общей редакцией В.Н. Ильюшенко / Ильюшенко В.Н., Бацула А.П., Загоскин В.В., Андык В.П.– Томск: Издательство Института оптики атмосферы, 2005. – 500 с.
4. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Гаудеамус, 2-е изд. – 2004. – 544 с.
5. РД 78.36.006-2005 (ВЫБОР И ПРИМЕНЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАННОЙ, ТРЕВОЖНОЙ СИГНАЛИЗАЦИИ И СРЕДСТВ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ УКРЕПЛЕННОСТИ ДЛЯ ОБОРУДОВАНИЯ ОБЪЕКТОВ).
6. Защита от утечки информации по техническим каналам: Учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М.: Горячая линия-Телеком, 2005. – 416 с.
7. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. – М.: Россиск. гос. гуманит. ун-т, 2002. – 399 с.
8. Сидорин Ю.С. Технические средства защиты информации: Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2005. – 141 с.
9. Большая энциклопедия промышленного шпионажа / Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко – СПб.: ООО «Издательство Полигон», 2000. – 896 с.