**Лекция № 1**

**ОБЩЕЕ ПРЕДСТАВЛЕНИЕ О ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ**

План:

1. Понятие об информации как предмете защиты

2. Основные свойства информации как предмета защиты

3*.* Виды защищаемой информации

**1. Понятие об информации как предмете защиты**

В соответствии с терминологией закона «Об информации, информационных технологиях и о защите информации» информация - информация - сведения (сообщения, данные) независимо от формы их представления Так как информация отражает свойства материальных объектов и отношения между ними, то ее можно отнести к объектам познания, а *защищаемую информацию* - к предмету защиты.

Защите подлежит секретная и конфиденциальная информация. К секретной относится информация, содержащая государственную тайну. Ее несанкционированное распространение может нанести ущерб интересам государственных органов, организациям, субъектам и РФ в целом. Под ***конфиденциальной информацией*** понимается – это документированная (то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать) информация, доступ к которой ограничивается в соответствии с законодательством РФ.

*Информация как объект познания имеет ряд особенностей*:

- *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.

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.

**2. Основные свойства информации как предмета защиты**

*С точки зрения защиты информация обладаем рядом свойств*, основные из которых следующие:

1. **Информация доступна человеку, 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 может быть источником информации о ее физических и химических характеристиках. Когда бумага содержит семантическую информацию, ей присваивается другое имя: чертеж, документ и т. д. Чертеж детали или узла входит в состав более сложного документа - чертежа прибора, механизма или машины и т. д. вплоть до конструкторской документации образца продукции.

Следовательно, в зависимости от назначения источнику могут присваиваться различные имена. Но независимо от наименования документа защищать от хищения, изменения и уничтожения информации надо листы бумаги, которые имеют определенные размеры, вес, механическую прочность, устойчивость краски или чернил к внешним воздействиям. *Параметры носителя определяют условия и способы хранения информации*. Другие *носители, например, поля не имеют четких границ в пространстве, но в любом случае их характеристики измеряемы. Физическая природа носителя-источника информации, носителя-переносчика и носителя-получателя может быть как одинаковой, так и разной*.

Передача информации путем перемещения ее носителей в пространстве связана с затратами энергии, причем величина затрат зависит от длины пути, параметров среды и вида носителя.

2. **Ценность информации оценивается степенью полезности ее для пользователя (собственника, владельца, получателя).** *Информация может обеспечивать ее пользователю определенные преимущества: приносить прибыль, уменьшить риск в его деятельности в результате принятия более обоснованных решений* и др.

Нейтральная информация не влияет на состояние дел ее пользователя, но 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.

*Вредной является информация, в результате использования которой ее получателю наносится моральный или материальный ущерб*. Когда такая информация создается преднамеренно, то ее называют *дезинформацией*. Часто вредная информация создается в результате целенаправленной или случайной модификации ее при переносе с одного носителя на другой. Если в качестве таких носителей выступают люди, то вредная информация циркулирует *в виде слухов*. Широко практикуется способ дезинформирования людей путем использования механизма распространения слухов.

*Полезность информации всегда конкретна*. Нет ценной 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 ценная информация для одних пользователей может не представлять ценности для других. Даже информация, ценная для всего человечества, например, технология изготовления лекарств от опасных болезней, для конкретного здорового человека может не представлять интереса.

*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. (**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). Для несекретной информации, содержащей служебную тайну, вводят гриф «для служебного пользования».

Для обозначения степени конфиденциальности коммерческой информации применяют различные шкалы ранжирования. Распространена шкала: «коммерческая тайна - строго конфиденциально» (КТ-СК), «коммерческая тайна - конфиденциально» (КТ-К), «коммерческая тайна» (КТ). Известна шкала: «строго конфиденциально - особый контроль», «строго конфиденциально», «конфиденциально». Применяется также двухуровневая шкала ранжирования коммерческой информации: «коммерческая тайна» и «для служебного пользования».

*В качестве критерия для определения грифа конфиденциальности информации могут служить результаты прогноза последствий попадания информации к конкуренту или злоумышленнику, в том числе*:

- величина экономического и морального ущерба, наносимого организации;

- реальность создания предпосылок для катастрофических последствий в деятельности организации, например, банкротства.

3. Учитывая, что информация может быть для получателя полезной или вредной, что она покупается и продается, то **информацию можно рассматривать как товар.** Цена информации связана с ее ценностью, 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.

Полезная информация может быть создана ее владельцем в результате научно-исследовательской деятельности, заимствована из различных открытых источников, может попасть к злоумышленнику случайно, например, в результате непреднамеренного подслушивания и, наконец, добыта различными нелегальными путями. **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 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 технологии, приносящими 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 осознано принимает в основном жизненно важные решения.

*Для принятия любого решения нужна информация, причем, чем выше риск и цена решения, тем большего объема должна быть информация. Размышления перед принятием решения есть не что иное, как переработка человеком имеющейся у него информации.* По своему опыту каждый знает, как трудно принять ответственное решение в условиях дефицита информации или времени.

Дефицит времени при принятии решений возникает, когда недостаточно времени для восприятия (чтения) и обработки информации, необходимой для принятия обоснованного решения. При недостатке времени часть информации не учитывается, что по последствиям аналогично дефициту информации. Поэтому руководитель требует от своих помощников представлять ему информацию в обобщенном виде и форме, позволяющих воспринять ее в сжатые сроки.

Учитывая жизненную потребность в информации для любых живых организмов, природа создала механизм, заставляющий их искать информацию в случае ее дефицита. Таким общим механизмом для активизации деятельности живых существ по удовлетворению основных потребностей, в том числе информационной потребности, являются эмоции. Уровень отрицательных эмоций живого существа пропорционален дефициту информации, необходимой для принятия им решений. Алгоритм поведения живого человека формируется таким, чтобы устранить причины отрицательных эмоций, в том числе путем поиска информации.

**4. Ценность информации изменяется во времени.** *Распространение информации и ее использование приводят к изменению ее ценности и цены*. Характер изменения ценности во времени зависит от вида информации. Для научной информации эта зависимость часто имеет волнообразный вид. 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 ценность, когда появились реальные возможности практического использования атомной энергии. Новые технологии или достижения в смежных областях могут увеличить ценность давно полученных знаний. Недаром говорят, что новое - это хорошо забытое старое.

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

Си(т) ≈ С0ехр(-2.3τ/τжц),

где С0 - ценность информации в момент ее возникновения (создания);

τ - время от момента возникновения информации до момента ее использования;

τжц - продолжительность жизненного цикла информации

(от момента возникновения до момента устаревания). В соответствии с этим выражением за время жизненного цикла ценность информации уменьшается до 0,1 первоначальной величины.

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

- *оперативно-тактическая*, теряющая ценность примерно по 10% в день (например, информация выдачи краткосрочного кредита, предложения по приобретению товара в срок до одного месяца и др.);

- *стратегическая информация*, ценность которой убывает примерно 10% в месяц (сведения о партнерах, о долгосрочном кредите, развитии и т. д.).

Информация о законах природы имеет очень большое время жизненного цикла. Ее старение проявляется в уточнении законов, например, в ограничениях законов Ньютона для микромира.

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

Для определения количества информации в теории информации предложен энтропийный подход.

**(((Информацио́нная энтропи́я** — *мера неопределённости или непредсказуемости информации, неопределённость появления какого-либо символа первичного алфавита.* При отсутствии информационных потерь численно равна количеству информации на символ передаваемого сообщения.

Например, в последовательности букв, составляющих какое-либо предложение на русском языке, разные буквы появляются с разной частотой, поэтому неопределённость появления для некоторых букв меньше, чем для других. Если же учесть, что некоторые сочетания букв (в этом случае говорят об энтропии n-ого порядка, см. ниже) встречаются очень редко, то неопределённость уменьшается еще сильнее.)))

(((Энтропия (информационная) — есть мера НЕУПОРЯДОЧЕННОСТИ системы. Это величина безразмерная. Чем меньше энтропия, тем больше порядок (определенность состояния системы). Бесконечно большая энтропия характеризует полный хаос (полную неопределенность состояния системы).

**Информация — это сведения, которые способны уменьшать неопределенность. Чем большую неопределенность снимают сведения, тем большее количество информации они содержат**. Информация, количеством 1 бит способна снять неопределенность при выборе одной из двух РАВНОВЕРОЯТНЫХ альтернатив.  
*Пример:* Наш друг подбросил монетку и, поймав её, зажал её в кулаке. Вероятность выпадения орла или решки одинакова — 0,5. Но мы не знаем точно, что же именно выпало. Присутствует неопределенность в этом вопросе. Сообщая нам сведения, что выпала, например, решка, наш друг сообщает нам информацию количеством 1 бит. Эта информация, снимая неопределенность, уменьшает энтропию системы.)))

*В соответствии с ним количество информации оценивается мерой уменьшения у получателя неопределенности (энтропии) выбора или ожидания событий после получения информации. Количество получаемой информации тем больше, чем ниже вероятность события.* Такой подход хорошо разработан для определения количества информации в сообщении, передаваемом по каналам связи. Выбор при приеме осуществляется между символами алфавита сообщения. Количество информации в передаваемом по каналам связи сообщении из N символов (без учета связи между символами в сообщении) рассчитывается по известной формуле **Шеннона**:

 (Информационная **двоичная энтропия** для независимых случайных событий x с n возможными состояниями (от 1 до n, p — функция вероятности)) рассчитывается по формуле:

где Pi - вероятность появления в сообщении символа *i,*

n - количество символов в алфавите языка.

Как следует из формулы, количество информации, измеряемое в двоичных элементах (в битах, байтах), зависит только от количества и статистики символов, но не зависит от содержания сообщения. *Количество информации, определяемое по этой формуле, одинаковое при передаче бессмысленного текста или сообщения о жизненно важных для получателя сведениях.* С точки зрения передачи таких сообщений по каналам связи такой подход обоснован, так как затраты на передачу этих сообщений одинаковы. *А на что потрачены деньги отправителя сообщения и насколько оно информативно для получателя, - эти вопросы к связи отношения не имеют.*

Аналогично, когда при телефонном разговоре Ваш собеседник сообщает известные сведения, то количество полученной Вами информации мало, хотя разговор может длиться достаточно долго. В таком случае возникает вопрос, что передавалось в этом случае. Очевидно, что осуществлялась передача лишь акустических и электрических сигналов.

*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 образуются 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 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.

*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.). Но семантика информации и ее ценность при этом не учитываются*.

**6. При копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а 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, обесцвечиваются из-за воздействия яркого ультрафиолетового света цвета изображения оригинала при ксерокопировании и т. д.

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.

**3*.* Виды защищаемой информации**

*По содержанию любая информация может быть отнесена к семантической (в переводе с латинского - содержащей смысл)* 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. Кроме того, использование носителей различной физической природы позволяет подключать для ввода информации в мозг человека все многообразие его рецепторов (датчиков).

*При просмотре кинофильмов, например, основной объем информации зритель получает через органы зрения. Музыкальное сопровождение фильма через слуховой канал ввода информа­ции оказывает дополнительное воздействие на эмоциональную сферу зрите­ля. Известны попытки дополнить эти каналы воздействием на органы обоня­ния человека путем создания в кинозале соответствующих запахом.* В ситуа­циях, когда нельзя использовать для информирования человека зрительные или акустические сигналы или эти каналы перегружены, воздействуют на его тактильные рецепторы. Например, ***нательное средство для обнаружения записывающего устройства в кармане собеседника информирует о работе диктофона с помощью индикатора, создающего вибрацию****.*

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.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Виды информации | | | | |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Семантическая | | |  | Признаковая | | | | |
|  |  |  |  |  |  |  |  |  |
| На языке национального общения |  | На профессио­нальном языке |  | о видовых признаках |  | о признаках сигналов |  | о признаках веществ |

Рисунок –1 Классификация информации по содержанию

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 информации.* Если затраты на защиту информации выше ее цены, то уровень защиты неоправданно велик, если существенно меньше, то попытается ве­роятность уничтожения, хищения или изменения информации, *Для обеспече­ния рациональной зашиты 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Конфиденциальная информация |  |  |
|  |  |  |  |  |
| Об организации |  | О внутренней деятельности организации |  | О внешней деятельности организации |
| - структура  - методы управления  - финансы  - планы и программы  - проблемы и пути их решения.  - безопасность |  | - качество продукции  - себестоимость продукции  - характеристики разрабатываемой продукции  - возможности производства  - технологии  - исследовательские работы |  | - принципы, концепция и стратегия магкетинга  - каналы приобретения и сбыта  - партнеры  - конкуренты  - переговоры и соглашения |

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. л. Такая информация является **структурированной.**

Защита 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.

**Литература**

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.
3. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И.К.Корнеев, Е.А. Степанов.- М.:Проспект,2011.-336 с.
4. Зегжда Д.П., Ивашко A.M. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2009.

**Лекции № 2-3**

**ДЕМАСКИРУЮЩИЕ ПРИЗНАКИ ОБЪЕКТОВ И**

**АКУСТИЧЕСКИХ ЗАКЛАДОК**

План

1. Демаскирующие признаки

2. Демаскирующие признаки объектов

3. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра

4. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра

5. Демаскирующие признаки радиоэлектронных средств

6. Демаскирующие признаки акустических закладок

*Под демаскирующим признаком понимается свойство объекта отличаться по каким-либо характеристикам от других объектов.* Отличительные характеристики могут иметь количественную или ка­чественную меру.

**Технический демаскирующий признак объекта - характерное свойство объекта защиты, которое может быть ис­пользовано технической разведкой для обнаружения и распознава­ния объекта, а также для получения необходимых сведений о нем.** Таким образом, доступ к информации может быть осуществлен путем анализа демаскирующих признаков. Носителями демаски­рующих признаков являются прямым образом связанные с ними физические поля.

Обнаружение объекта - процесс функционирования средства технической разведки, в результате которого фиксируются техни­ческие демаскирующие признаки объекта и делается заключение о его наличии.

Различают демаскирующие признаки:

* расположения - признак, определяющий положение объекта среди других объектов и предметов окружающего пространства;
* структурно-видовой - признак, определяющий структуру и видовые характеристики группового объекта (состав, количество и расположение отдельных объектов, форму и геометрические раз­меры);
* деятельности - признак, раскрывающий функционирование объекта через физические проявления.

Технические демаскирующие признаки можно разделить на два класса:

* прямые демаскирующие признаки - признаки, связанные с функционированием объекта защиты и проявляющийся через их физические поля (электромагнитные, акустические, радиационные и т.п.), выделяющиеся по уровню на фоне физических полей окру­жающей среды (под фоном физических полей окружающей среды понимаются сигналы, не связанные с защищаемой информацией) ***К прямым демаскирующим признакам*** ***объектов в видимом диапазоне электромагнитного спектра*** относятся: форма, размер, тон или цвет, структура, текстура и тень объектов. При этом форма изображения объекта является основным признаком. Размер изо­бражения зависит от масштаба фотоснимка и в меньшей степени является информативным, поскольку требует сравнения с некото­рым эталоном;
* косвенные демаскирующие признаки - признаки, в основе кото­рых лежат последствия изменения окружающей среды как результат функционирования объекта (визуально-оптические признаки деятель­ности, геометрические размеры, контрастность освещенности, следы производственной деятельности и функционирования и т.п.). ***Они*** дополняют некоторые характеристики объектов, не входящие в состав прямых признаков. Так, например, невидимый тоннель можно определить на фото­снимке по разрыву дорожного полотна на определенном участке. Показатель эффективности защиты информации - параметр технического демаскирующего признака объекта защиты, по отно­шению к которому устанавливаются нормы по эффективности за­щиты информации.

Опасный сигнал является показателем признака объекта, кото­рый используется технической разведкой для получения секретной информации.

Для организации эффективной защиты от технических средств разведки (TCP) необходимы анализ сведений о скрываемом объек­те и учет возможности их проявления через соответствующие де­маскирующие признаки (ДП).

В каждом конкретном случае ДП и неразрывно связанные с ни­ми технические каналы утечки информации должны анализиро­ваться применительно к перечню скрываемых об объекте сведений.

Под обнаружением понимается выделение для анализа из об­щей совокупности сигналов одного или нескольких, отличающихся по своим признакам в интересующем плане от остальных сигналов. В общем случае ДП при обнаружении объектов является их кон­траст по отношению к фону. Чем больше контраст, тем вероятнее обнаружение объекта. Например, для информации, состоящей из электромагнитных сигналов, требуется контраст по мощности или частоте.

Распознавание объекта - процесс функционирования средства TP, в результате которого определяются параметры демаскирую­щего признака объекта, и делается заключение о его характеристи­ках (производится классификация). В результате распознавания обнаруженному объекту присваивается - один из известных клас­сов. У любого объекта может быть значительное число признаков, но при распознавании используется их определенный набор.

Техническое средство защиты информации - техническое сред­ство, предназначенное для устранения или ослабления демаски­рующих признаков объекта, создания ложных (имитирующих) признаков, а также для создания помех техническим средствам дос­тупа к информации.

**2. Демаскирующие признаки объектов**

К демаскирующим признакам объектов относятся:

* признаки деятельности: движение транспортных машин, зву­ки, огни, вспышки, дым, пыль;
* способность отражать и испускать различные излучения (электромагнитные, инфракрасные, тепловые), улавливаемые спе­циальными приборами;
* следы деятельности: тропы и дороги, остатки производственных материалов, бытовой мусор и т.д.;
* характерные очертания (форма), размеры и особенности рас­положения объектов;
* цвет поверхности объектов, а в некоторых случаях и блеск ее (блеск стекол, отблеск металла);
* тени, падающие от объектов, а также тени на поверхности са­мих объектов.

Тени объектов подразделяют на собственные (лежащие на объекте с теневой стороны) и падающие (отбрасываемые объектом на ок­ружающую поверхность). *Собственные тени хорошо подчерки­вают пространственные формы объекта, а падающие тени способ­ствуют определению не только формы, но и размеров объекта.*

Распознавательные демаскирующие признаки объектов можно разделить на следующие группы:

* признаки, характеризующие физические свойства вещества объекта (теплопроводность, электропроводность, структура, твер­дость и т. д.);
* признаки, характеризующие физические поля, создаваемые объектами (электромагнитные, радиационные, акустические, гра­витационные и др.);
* признаки, характеризующие форму, цвет, размеры объекта и его элементов;
* пространственные признаки, характеризующие как координа­ты объекта, так и их производные для движущегося объекта;
* признаки, характеризующие наличие определенных связей между объектами и их элементами;
* признаки, характеризующие результаты функционирования объектов (задымленность, запыленность, следы объекта на грунте, загрязнения воды и воздуха и т. д.).

При дешифровании наблюдатель имеет дело не с самими дема­скирующими признаками, а с носителями первичной информации о них, которые могут иметь различную физическую основу. Носите­лями демаскирующих признаков являются физические поля. Сле­довательно, параметры физических полей объектов и являются их демаскирующими признаками.

**3. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра**

Оптические характеристики объектов и окружающей среды иг­рают важную роль как для разведки, так и для эффективной защи­ты объектов от TCP. *Оптическое изображение объектов и их от­дельных элементов по отношению к фону отличаются контрастами по яркости, цвету, размеру, форме.* В видимом диапазоне волн ви­димость объектов определяется яркостным контрастом, при этом в видимом диапазоне дополнительной информацией является цвето­вой контраст между объектом и фоном. ­ Контраст по яркости *К* между объектом и фоном возникает в результате различной световой от­ражательной способности объекта и фона.

Контраст по яркости *К* определяется как

гдеBmin и Bmax - минимальная и максимальная яркости поверхно­стей объекта и фона.

При маскировке объекта необходимо принять меры к тому, чтобы яркости объекта и фона были максимально возможно близки друг к другу. В этом случае объект будет малозаметен на фоне ок­ружающей среды. При оценке эффективности маскировки объекта приняты следующие значения коэффициентов контраста по яркости:

*К <* 0,2 (20%) - незаметный контраст;

*К =* 0,2... 0,3 - малозаметный контраст;

*К =* 0,3... 0,6 - заметный контраст;

*К>* 0,5 - резкозаметный контраст.

Яркость поверхности предметов зависит от освещенности Е, с увеличением которой она пропорционально возрастает.

*Освещенности зависят от погодных условий, ориентации объ­ектов по отношению к солнцу и других условий. Освещенность прямыми солнечными лучами Е наклонной поверхности зависит от косинуса угла падения лучей а.*

Кроме освещенности на яркость предметов влияют и их отра­жающие свойства. В зависимости от свойств поверхности отраже­ние может быть зеркальным (направленным), диффузным (рассе­янным) или смешанным. Зеркальное отражение характерно только для гладких поверхностей с малыми размерами неровностей по сравнению с длиной волны.

При солнечном освещении такие по­верхности дают яркие блики, которые хорошо наблюдаются на большой дальности.

При диффузном отражении отраженная энергия равномерно распределяется в пределах полусферы над точкой отражения. Та­кое отражение характерно для матовых шероховатых поверхно­стей.

При смешанном, т.е. диффузно-зеркальном отражении энергия в полусфере распределена не равномерно, зависит от направления облучения и от направления наблюдения.

Видимость объекта зависит также от расстояния. По мере удале­ния объекта видимость ухудшается. Это обусловлено ослаблением потока при прохождении сквозь атмосферу за счет спектрального поглощения его слоем воздуха, что приводит к уменьшению яркости объекта и фона.

Видовые демаскирующие признаки выявляются с помощью ви­довых разведок (*фотографическая, телевизионная, радиолокацион­ная* и т.д.).

**4. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра**

К демаскирующим признакам объектов в инфракрасном диапа­зоне электромагнитного спектра относятся: собственное (естест­венное) излучение нагретых тел и отраженное объектами (искусст­венное) ИК-излучение. Естественные источники ИК-излучений бывают наземными (почва, лес и т.д.), атмосферными (облака, ат­мосферные газы) и космическими (солнце, луна, звезды). Естест­венные источники ИК-излучений создают фоновое излучение, за­трудняющее распознавание объектов

Обнаружение цели возможно за счет различий в тепловой излучательной способности объекта и фона. Каждый предмет при тем­пературе, отличной от абсолютного нуля, испускает электромаг­нитное излучение, называемое тепловым.

Излучение тел зависит от их температуры и излучательной способности, которые можно ха­рактеризовать эффективной температурой тела. Собственное теп­ловое излучение нагретых тел связано с понятием абсолютно чер­ного тела, поглощающего все падающие на него излучения во всем спектре.

Отраженное объектами ИК излучение в дневное время в основном приходится на Солнце и доля собственного излучения является пренебрежительно малой, *в то время как в ночное время преобладающим является собственное излучение.*

Ослабление ИК излучения в атмосфере обусловлено полосами поглощения водяных паров, углекислого газа и озона, а также рассеиванием излучения. При проведении разведки и мероприятий по защите объектов необходимо учитывать ослабление собственного или отраженного ИК излучения в атмосфере за счет рассеяния.

Поток энергии, прошедший через ослабляющий слой атмосфе­ры, можно представить как результат излучения при температуре, меньше эффективной.

Большая часть энергии излучения подвижных объектов лежит в диапазоне волн 2-14 мкм; окна прозрачности находятся в этом же диапазоне, что позволяет обнаруживать цели на сравнительно больших дальностях.

Опытным образом установлено, что в диапазоне длин волн ме­нее 3 мкм преобладает отраженное и рассеянное солнечное излуче­ние, значительно преобладающее над собственным тепловым излу­чением фонов. В диапазоне длин волн более 4 мкм преобладающим является собственное тепловое излучение фонов.

В реальных условиях внешнее тепловое поле человека неравно­мерно по интенсивности излучения, сложно по спектральному составу и, кроме того, может существенно изменяться в зависимости от рода деятельности, климатических и метеорологических условий.

**5.** **Демаскирующие признаки радиоэлектронных средств**

Демаскирующие признаки радиоэлектронной аппаратуры свя­заны с излучением электромагнитных волн радиодиапазона. Электромагнитные волны могут нести информацию о назначении и характеристиках технических средств и систем. Излучение возможно в основных и побочных средствах, в контрольно-измерительной аппаратуре, тренажерах, имитаторах и т.д.

Все демаскирующие признаки, связанные с радиоизлучениями, определяются техническими характеристиками радиосигналов, которые можно разделить на следующие группы:

* частотные,
* временные,
* энергетические,
* спектральные,
* пространственно-энергетические,
* фазовые,
* поляризационные.

*Частотные характеристики* радиоизлучений определяют их место в диапазоне частот. К ним относятся: несущая частота, закон несущей модуляции, количество фиксированных частот и величина разноса между ними, диапазон изменения при частотной модуляции, стабильность несущей.

К *временным характеристикам* относятся: форма огибающей импульса и его длительность, период следования импульсов, структура кодовой посылки, продолжительность излучения.

*Энергетические характеристики* дают представление как о самом источнике, так и создаваемом им в пространстве электромагнитном поле. К характеристикам относятся: мощность излучения, спектральная плотность мощности, плотность потока мощности, напряженность электромагнитного поля по электрической и магнитной составляющей, динамический диапазон изменения мощности радиоизлучений.

*Пространственно-энергетические характеристики* дают представление о распределении энергии радиоизлучений в пространстве (направление распространения излучения, направление максимума излучения, параметры диаграммы направленности антенны, характер изменения напряженности электрического поля в зависимости от расстояния).

*По спектральным характеристикам радиоизлучений* можно судить о распределение энергии между составляющими спектра. Основными спектральными характеристиками являются: ширина спектра, вид спектра (сплошной, дискретный), относительная величина отдельных спектральных составляющих, форма огибающей спектра.

*Поляризационные характеристики* определяют направление и законы изменения в пространстве вектора электрического поля радиоизлучений. К поляризационным характеристикам относятся: вид поляризации (линейная, круговая, эллиптическая), направление вращения вектора электрического поля.

*Фазовые характеристики* связаны с законом изменения фазы за время излучения. К фазовым характеристикам относятся: парамет­ры фазовой модуляции, вид фазовой модуляции, количество дис­кретных скачков фазы, длительность дискреты фазы.

Технические признаки радиоизлучений можно разделить на групповые, индивидуальные и оперативные.

Групповые технические признаки позволяют установить при­надлежность радиоэлектронных систем (РЭС) к определенному классу. Они определяются по характеристикам или совокупности характеристик, соответствующих определенным типам РЭС. К ним относятся:

* характеристики обзора пространства;
* скорость вращения антенны;
* вид излучения;
* закон и границы перестройки частоты;
* вид и закон модулирующего сигнала;
* значения параметров сигнала (несущие частоты, длительности импульсов, частоты следования импульсов и др.).

Индивидуальные технические признаки содержат информацию о конкретном образце из совокупности РЭС одного типа. Наличие у РЭС индивидуальных демаскирующих признаков обусловлено технологическим и эксплуатационным разбросом параметров сиг­нала. Индивидуальные технические признаки могут проявляться в следующих характеристиках РЭС:

* форме огибающей сигнала (форма вершины импульса, его пе­реднего и заднего фронтов);
* спектре сигналов (форма огибающей спектра сигнала, отно­шение амплитуд главного и боковых лепестков спектра);
* величине нестабильностей параметров сигнала;
* виде паразитной модуляции.

По своей природе демаскирующие признаки радиоизлучений бывают техническими и организационными. К техническим дема­скирующим признакам относятся те признаки, анализ и обработка которых позволяет распознавать источник радиоизлучения, при­надлежность его к определенному узлу связи и т.д.

*Технические демаскирующие признаки бывают индивидуаль­ные и типовые*.

К ***индивидуальным демаскирующим*** ***признакам*** относятся ко­личественные либо качественные отклонения параметров радиоиз­лучений средств связи от норм технических условий. Анализ и об­работка индивидуальных демаскирующих признаков позволяет злоумышленнику осуществлять индивидуальное распознавание средств связи.

К ***типовым демаскирующим признакам*** относятся такие при­знаки, анализ и обработка которых позволяет злоумышленнику выйти на тип средств связи (например: диапазон частот, мощность излучения, скорость передачи, длина кодовой комбинации, ее структура и т.д.)

По характеру проявления организационные демаскирующие признаки подразделяются на опознавательные и признаки состоя­ния. Анализ и обработка опознавательных демаскирующих при­знаков позволяет определить принадлежность средств связи либо к конкретному узлу связи, либо к оператору связи и т.д. Демаски­рующие признаки состояния выводят злоумышленника на измене­ние структуры сети, местоположения и временных режимов работы средств связи, интенсивности их работы и т.д.

**6. Демаскирующие признаки акустических закладок**

*Демаскирующие признаки электронных устройств перехвата информации*.

*Обнаружение электронных устройств перехвата информации (закладных устройств), так же как и любых других объектов, про­изводится по их демаскирующим признакам*.

Каждый вид электронных устройств перехвата информации имеет свои демаскирующие признаки, позволяющие обнаружить закладку.

*Наиболее* ***информативными*** *признаками проводной микрофон­ной системы* являются:

* тонкий провод неизвестного назначения, подключенный к ма­логабаритному микрофону (часто закамуфлированному и скрытно установленному) и выходящий в другое помещение;
* наличие в линии (проводе) неизвестного назначения постоян­ного (в несколько вольт) напряжения и низкочастотного информа­ционного сигнала.

***Демаскирующие признаки автономных некамуфлированных*** *акустических закладок* включают:

• признаки внешнего вида - малогабаритный предмет (часто в форме параллелепипеда) неизвестного назначения;

• одно или несколько отверстий малого диаметра в корпусе;

• наличие автономных источников питания (например, аккумуляторных батарей);

• наличие полупроводниковых элементов, выявляемых при облучении обследуемого устройства нелинейным радиолокатором;

• наличие в устройстве проводников или других деталей, определяемых при просвечивании его рентгеновскими лучами.

***Камуфлированные акустические закладки*** по внешнему виду, на первый взгляд, не отличаются от объекта имитации, особенно если закладка устанавливается в корпус бытового предмета без изменения его внешнего вида. Такие закладки можно выявить путем разборки предмета.

Закладки, устанавливаемые в малогабаритные предметы, ограничивают возможности последних. Эти ограничения могут служить косвенными признаками закладных устройств. *Чтобы исключить возможность выявления закладки путем ее разборки, места соединения разбираемых частей склеивают*.

Некоторые камуфлированные закладные устройства не отличаются от оригиналов даже при тщательном внешнем осмотре. Их можно обнаружить только при просвечивании предметов рентгеновскими лучами.

**В ряде случаев закамуфлированное закладное устройство обнаруживается по наличию в обследуемом предмете не свойственных ему полупроводниковых элементов (выявляемых при облучении его нелинейным радиолокатором).** Например, обнаружение полупроводниковых элементов в пепельнице или в папке для бумаг может указать на наличие в них закладных устройств.

*Наличие портативных звукозаписывающих и видеозаписывающих устройств в момент записи можно обнаружить по наличию их побочных электромагнитных излучений (излучений генераторов подмагничивания и электродвигателей)*.

Дополнительные демаскирующие признаки акустических радиозакладок:

* радиоизлучения (как правило, источник излучения находится в ближней зоне) с модуляцией радиосигнала информационным сиг­налом;
* наличие (как правило) небольшого отрезка провода (антенны), выходящего из корпуса закладки.

Вследствие того, что при поиске радиозакладок последние на­ходятся в ближней зоне излучения и уровень сигналов о них, как правило, превышает уровень сигналов от других РЭС, у большин­ства радиозакладок обнаруживаются побочные излучения и, в ча­стности, излучения на второй и третьей гармониках, субгармони­ках и т.д.

***Дополнительные демаскирующие признаки сетевых акустиче­ских закладок***:

* наличие в линии электропитания высокочастотного сигнала (как правило, несущая частота от 40 до 600 кГц, но возможно нали­чие сигнала на частотах до 7 МГц), модулированного информаци­онным низкочастотным сигналом;
* наличие тока утечки (от единиц до нескольких десятков мА) в линии электропитания при всех отключенных потребителях;
* отличие емкости линии электропитания от типовых значений при отключении линии от источника питания (на распределитель­ном щитке электропитания) и отключении всех потребителей.

**Дополнительные демаскирующие признаки акустических и те­лефонных закладок с передачей информации по телефонной линии на высокой частоте**:

* наличие в линии высокочастотного сигнала (как правило, не­сущая частота до 7 МГц) с модуляцией его информационным сиг­налом.

**Дополнительные демаскирующие признаки телефонных радио­закладок**:

* радиоизлучения с модуляцией радиосигнала информационным сигналом, передаваемым по телефонной линии;
* отличие сопротивления телефонной линии от " оо " при от­ключении телефонного аппарата и отключении линии (отсоедине­нии телефонных проводов) на распределительной коробке (щитке);
* отличие сопротивления телефонной линии от типового значе­ния (для данной линии) при отключении телефонного аппарата, отключении и закорачивании линии на распределительной коробке (щитке);
* падение напряжения (от нескольких десятых до 1,5...2 В) в телефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при поло­женной и поднятой телефонной трубке;
* наличие тока утечки (от единиц до нескольких десятков мА) в телефонной линии при отключенном телефоне.

**Дополнительные демаскирующие признаки акустических за­кладок типа «телефонного уха»:**

* отличие сопротивления телефонной линии от «∞» при отклю­чении телефонного аппарата и отключении линии (отсоединении телефонных проводов) на распределительной коробке (щитке);
* падение напряжения (от нескольких десятых до 1,5...2 В) в те­лефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при поло­женной телефонной трубке;
* наличие тока утечки (от единиц до нескольких десятков мА) в телефонной линии при отключенном телефоне;
* подавление (не прохождение) одного-двух вызывных звонков при наборе номера телефонного аппарата.

**Дополнительные демаскирующие признаки полуактивных аку­стических радиозакладок:**

* облучение помещения направленным (зондирующим) мощ­ным излучением (как правило, гармоническим);
* наличие в помещении переизлученного зондирующего излу­чения с амплитудной или частотной модуляцией информационным акустическим сигналом.
* Наиболее информативными признаками проводной микрофон­ной системы являются:
* тонкий провод неизвестного назначения;
* наличие в линии неизвестного назначения постоянного (в не­сколько вольт) напряжения и низкочастотного сигнала.

**Признаками не камуфлируемых акустических закладок являются**:

* внешний вид (малогабаритный предмет неизвестного назначе­ния);
* одно или несколько отверстий малого диаметра в корпусе;
* наличие автономных источников питания;
* наличие полупроводниковых элементов, выделяемых нели­нейным радиолокатором;
* наличие в устройстве проводников и радиодеталей, опреде­ляемых рентгеновским устройством.

Камуфлирование акустических закладок можно выявить путем разборки предмета, а также предыдущими методами.

Наличие портативных звукозаписывающих и видеозаписывающих устройств в момент записи можно обнаружить по наличию их побочных электромагнитных излучений.

Дополнительные признаки акустических радиозакладок:

* радиоизлучения в ближней зоне с модуляцией информацион­ным сигналом;
* наличие небольшого отрезка провода (антенны), выходящего из корпуса закладок.

**Демаскирующие признаки сетевых акустических закладок:**

* наличие в линии электропитания высокочастотного сигнала (40 ... 600 кГц; 7 МГц), модулированного низкочастотным сиг­налом;
* наличие тока утечки до нескольких десятков миллиампер в линии при отключенных потребителях;
* отличие емкости линии от типовых значений.

**Дополнительные демаскирующие признаки акустических и те­лефонных закладок с передачей на высокой частоте**:

* наличие в линии ВЧ-сигнала 7 МГц с модуляцией.

**Дополнительные признаки телефонных радиозакладок:**

* радиоизлучение с модуляцией;
* отличие сопротивления телефонной линии от бесконечности при отключении аппарата и отключении линий от распределитель­ной коробки (щитка);
* падение напряжения до 2В в телефонной линии при положен­ной и поднятой трубке;
* наличие тока утечки при отключенном телефоне.

**Литература**

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.
3. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И.К.Корнеев, Е.А. Степанов.- М.:Проспект,2011.-336 с.
4. Зегжда Д.П., Ивашко A.M. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2009.

**Лекция № 4**

**Источники и носители информации**

**Классификация источников и носителей информации**

План

1. Источники и носители информации

2. Классификация источников и носителей информации

3. Сущность записи и съема информации с носителя

**1.Источники и носители информации**

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

- люди

- документы;

- продукция;

- измерительные-датчики;

- интеллектуальные средства обработки информации;

- черновики и отходы производства;

- материалы и технологическое оборудование

Информативность **людей** как источников информации существенно различаются. 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 выступления 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 документов 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. Поэтому сведения, содержащиеся в публикациях, перед их использованием для решения своих задач проверяются.

Большинство технических средства сбора, обработки, хранения и передачи информации нельзя отнести к источникам информации, так как они представляют лишь инструмент для преобразования входной информации. Исключения составляют лишь **датчики различных измерительных устройств и интеллектуальные средства обработки, генерирующие информацию**, такие как, например, компьютер фирмы IBM, выигравший матч у чемпиона мира Г. Каспарова. Критерием отнесения технического средства к источникам 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 новостей дня радио- или телевизионные приемники. Очевидно, что источники этой информации даже не дикторы, читающие текст, а редакции компаний или конкретные люди, участвующие в передаче.

**Продукция (**без документации) является источником признаковой информации. Ноу-хау нового изделия могут содержаться во внешнем виде, например, в форме автомобиля, расцветки ткани, модели одежды, узле механизма и др., в параметрах излучаемых полей (в значениях сигналов радиостанции или радиолокатора), в 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 способами обратного инженеринга (разборки, расчленения, выделения отдельных составных частей и элементов, проведения 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. 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 психологические предпосылки сотрудников, серьезно не воспринимающих отходы как источники 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 изменения в создаваемой продукции или технологических процессах.

Таким образом, источниками конфиденциальной информации могут быть как физические лица, так и различные объекты. При решении задач ее защиты нужно учитывать каждый потенциальный источник и его информативность в конкретных условиях. 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.

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 ее смысл.*

**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.

**3. Сущность записи и съема информации с носителя**

Материализация (запись) любой информации производится путем изменения параметров носителя. Механизм запоминания и воспроизведения информации человеком в настоящее время еще недостаточно изучен и нет однозначного 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 последовательном просмотре поверхности тела зрительным анализатором человека или автомата, выделении и распознавании ими знаков, символов или конфигурации точек. Для людей, лишенных зрения, информация записывается по методу Бройля 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. Если меняются значения амплитуды аналогового сигнала, то модуляция называется амплитудная, частоты - частотная, фазы - фазовая. Частотная и фазовая модуляция мало различаются, поскольку при фазовой модуляции меняется непосредственно фаза, а при частотной  ее первая производная по времени - частота.

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

В соответствии с формулой Фурье изменение формы сигнала при модуляции приводит к изменению спектра модулированного сигнала. Чем выше максимальная частота спектра моделирующего сигнала Fc,м, тем шире спектр модулированного сигнала. Количественное значение увеличения ширины спектра этого сигнала зависит от вида модуляции и ширины спектра модулирующего (первичного) сигнала. Ширина модулированного синусоидального сигнала составляет величину:

- для АМ: ΔF ам=2Fс,м ;

- для ЧМ: ΔF чм>>Fс, м;

- для ФМ: ΔF фм ≈ F чм.

Для радиовещания ширина спектра ЧМ-сигнала составляет порядка 150 кГц вместо около 7 кГц для АМ речевого сигнала. Поэтому ЧМ 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, которая при АМ несет информацию, то ЧМ-сигналы обладают существенно большей помехоустойчивостью, чем АМ-сигналы. Это свойство ЧМ-сигналов обеспечивает высокое качество радиовещания в УКВ диапазоне. Спектры ФМ- и ЧМ-сигналов мало отличаются по ширине.

Выделение информации из модулированного электрического сигнала производится путем обратных преобразований - демодуляции его в детекторе (демодуляторе) приемника. При демодуляции выделенного и усиленного радиосигнала, наведенного электромагнитной волной в антенне, преобразуется таким образом, что сигнал на выходе детектора соответствует модулирующему сигналу передатчика. Демодуляция, как любая процедура распознавания, обеспечивается путем сравнения текущего сигнала с эталонным.

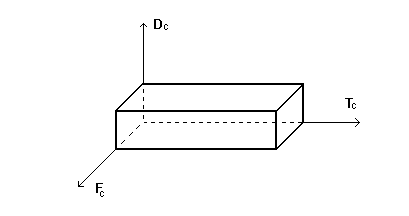
Способы выполнения этой процедуры для разных видов демодуляции существенно различаются. При демодуляции АМ-сигналов в качестве эталонной амплитуды используется усредненная амплитуда несущего колебания на выходе детектора, при ЧМ-модуляции - частота настройки контура детектора, ФМ-модуляции - фаза опорного колебания, синфазного с колебаниями несущей частоты.

Полного соответствия модулирующего и демодулированного сигналов из-за влияния помех добиться нельзя. В общем случае любые преобразования сигнала ухудшают качество записанной в нем информации, так как при этом оказываются воздействия на его информационные параметры, которые могут привести к потере информации. Но при достаточной большом превышении мощности носителя над мощностью помех искажения будут столь незначительные, что на качество информации помехи практически не влияют. Полная идентичность исходного и демодулированного сигналов обеспечивается при бесконечно большом отношении сигнал/помеха.

Помехоустойчивость дискретных сигналов выше, чем аналоговых, так как искажения дискретных сигналах возникают в тех случаях, когда изменения параметра сигнала превышают половину величины интервала между соседними значениями параметра. Если изменения параметров помехами составляют менее половины этого интервала, то при приеме такого сигнала можно восстановить исходное значение параметра сигнала.  Допустимое значения отношения мощностей или амплитуд сигнала и помехи (сокращенно - отношение сигнал/помеха), при которых обеспечивается требуемое качество принимаемой информации, определяются видом информации и характером помех.

Для повышения достоверности передачи информации наряду с обеспечением наряду с увеличением энергетики переносчика информации используют другие методы защиты дискретной информации от помех, прежде всего, помехоустойчивое кодирование. При помехоустойчивом кодировании каждому элементу дискретной информации (букве, цифре, любому другому знаку) ставится в соответствие кодовая комбинация, содержащая дополнительные (избыточные) символы. Эти дополнительные символы позволяют обнаруживать искажения и исправлять в зависимости от избыточности кода ошибочные символы различной кратности. Существует большое количество видов кодов, повышающих помехоустойчивость сообщений для различных условий среды распространения носителей. Однако следует иметь, что платой за повышение помехоустойчивости кодированных сигналов является уменьшение скорости их передачи.

Любое сообщение в общем случае можно описать с помощью трех основных параметров: динамическим диапазоном DсFΔ, шириной спектра частот с и длительностью передачи Тс. Произведение этих трех параметров называется объемом сигнал Vс=Dc FΔсTс. В трехмерном пространстве объем сигнала можно представить в виде параллелепипеда (см. рис. 1.9).

  
Рис. 1.9. Графическое представление объема сигнала.

Для обеспечения неискаженной передачи сообщения объемом Vс, необходимо чтобы характеристики среды распространения и непосредственно приемника соответствовали ширине спектра и динамическому диапазону сигнала. Если полоса частот среды распространения или приемника уже полосы сигнала, то для обеспечения безискаженной передачи сигнала объемом Vс уменьшают его ширину спектра. При этом для сохранения Vс=const соответственно увеличивают время передачи Тc. Для без искаженной передачи сообщения в реальном масштабе времени полоса пропускания приемника должна соответствовать ширине спектра сигнала.

**Литература**

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.
3. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И.К.Корнеев, Е.А. Степанов.- М.:Проспект,2011.-336 с.
4. Зегжда Д.П., Ивашко A.M. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2009.

**Лекция № 5-6**

**ИСТОЧНИКИ ОПАСНЫХ СИГНАЛОВ**

План:

1. Классификация источников сигналов

2. Состав основных и вспомогательных технических средств и систем.

3. Случайные акустоэлектрические преобразователи

4. Принципы возникновения побочных низкочастотных и высокочастотных излу­чений радиосредств и электрических приборов.

5. Паразитные связи и наводки

1. **Классификация источников сигналов**

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 могут быть **функциональными и случай­ными.**

1. источники функциональных сигналов (*создаются и применяются для обеспечения связи между санкционированными абонентами*):

* передатчики радио и радиотехнических средств и систем связи
* лазерные системы связи
* излучатели акустических сигналов гидролокаторов и средств подводной связи
* условные сигналы

1. источники опасных сигналов

***Источники опасных сигналов*** *- это несанкционированные сигналы с защищаемой информацией, которые возникают случайно или создаются злоумышленниками*. Их источниками могут быть радио и радиотехнические элементы и устройства любых радиоэлектронных и электрических приборов.

**2. Состав основных и вспомогательных технических средств и систем.**

Радиоэлектронные и электрические средства и системы, содержащие потенциальные источники опасных сигналов, разделяют на основные и вспомогательные. **Основные технические средства и системы (ОТСС, ТСПИ (технические средства передачи информации) обеспечивают обработку, хранение и передачу защищаемой информации,** *вспомогательные технические средства и системы (ВТСС) - остальной информации*.

К основным средствам и системам организации относятся:

- средства и информационные системы (средства вычислитель­ной техники, сети и системы),

- программные средства (операцион­ные системы, системы управления базами данных, прикладное про­граммное обеспечение),

- автоматизированные системы управления,

- системы связи и передачи данных,

- технические средства приёма, передачи и обработки информации ограниченного доступа (звуко­запись, звукоусиление, звуковоспроизведение, переговорные и те­левизионные устройства, средства изготовления, тиражирование документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации).

ВТСС включают:

- технические средства телефонной, громкоговорящей связи,

- системы:

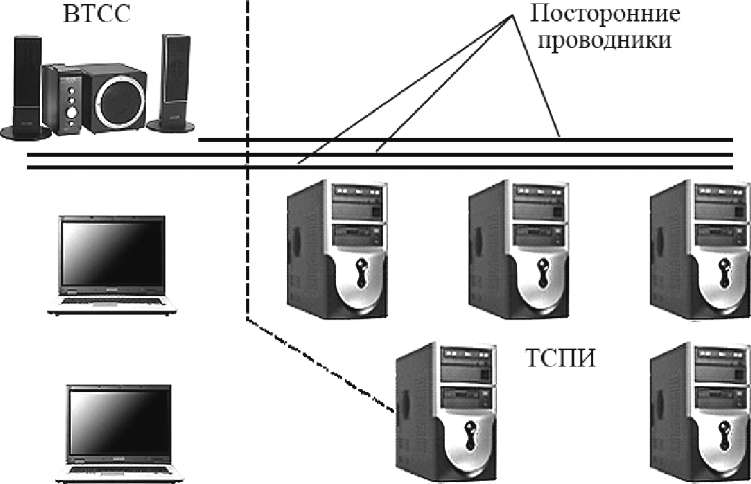
* пожарной и охран­ной сигнализации,
* радиотрансляции,
* часофикации,

- электробыто­вые приборы и т.д.,

- сами помещения, предназначенные для обработки информации ограниченного распространения.

Технические средства приёма, обработки и хранения информа­ции можно рассматривать как систему, включающую стационарное оборудование, периферийные устройства, соединительные линии, распределительные и коммуникационные устройства, системы электропитания, системы заземления.

Технические средства, предназначенные для обработки конфи­денциальной информации, включая помещения, в которых они размещаются, представляют **объект ТСПИ.**

Наибольший интерес с точки зрения образования каналов утеч­ки информации представляют ТСПИ и ВТСС, имеющие выход за пределы***контролируемой зоны* (КЗ), т.е. зоны с пропускной систе­мой.** Кроме соединительных линий ТСПИ и ВТСС за пределы кон­тролируемой зоны могут иметь выход проходящие через помещения посторонние проводники, не связанные с ТСПИ и ВТСС.

*Зона с возможностью перехвата разведывательным оборудова­нием побочных электромагнитных излучений, содержащих конфи­денциальную информацию, называется* ***опасной зоной****.* *Пространст­во вокруг ТСПИ, в котором на случайных антеннах наводится ин­формационный сигнал выше допустимого уровня, называется* ***опасной зоной 1.***

Случайными антеннами могут быть цепи ВТСС или посторон­ние проводники, воспринимающие побочные электромагнитные излучения от средств ТСПИ.

Случайные антенны бывают *сосредоточенными и распределёнными*. *Сосредоточенная случайная ан­тенна* представляет собой техническое средство с сосредоточенны­ми параметрами (телефонный аппарат, громкоговоритель радио­трансляционной сети и т.д.). *Распределённые случайные антенны* образуют проводники с распределёнными параметрами: кабели, соединительные провода, металлические трубы.

Информационные сигналы могут быть электрическими, элек­тромагнитными, акустическими и т.д. Они имеют в большинстве случаев колебательный характер, а информационными параметра­ми являются амплитуда, фаза, частота, длительность.

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:

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

**3. Случайные акустоэлектрические преобразователи**

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

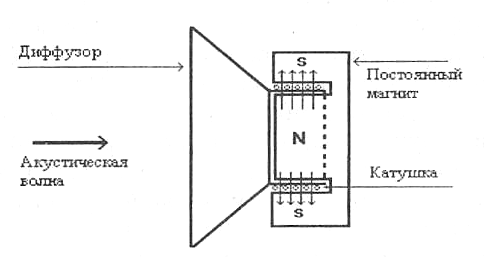
Классификация акустоэлектрических преобразователей, создающих опасные сигналы, приведена на рис.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Акустоэлектрические преобразователи |  |  |
|  |  |  |  |  |
| Индуктивные |  | Емкостные |  | Пьезоэлектрические |
| - электродинамические  - электромагнитные  - магнитострикционные |  |  |  |  |

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

Индуктивные – эл.сигналы возникают в результате перемещений под действием ак.волн индуктивностей (катушек с металлической проволокой) в полях (магнитных и электрических) или при изменениях геометрических размеров катушек и их сердечников

Наибольшей чувствительностью обладают **электродинамические' акустоэлектрические преобразователи** в виде динамических головок громкоговорителей.

Сущность преобразования состоит в следующем. Под давлением акустической волны соединенная с диффузором катушка в виде картонного цилиндра с намотанной на нем тонкой проволокой перемещается в магнитном поле, создаваемом постоянным магнитом цилиндрической формы. В соответствии с законом электромагнитной индукции в катушке (контуре) возникает электродвижущая сила (ЭДС), величина которой пропорциональна громкости звука. Опасные сигналы на концах катушки достигают величин в 5-15 мВ, достаточных для их распространения за пределы помещения, здания и даже территории. Поэтому неработающие, но непосредственно подключенные к радиотрансляционной сети громкоговорители могут выполнять функцию микрофона и передавать информацию разговоров в помещении на достаточно большое расстояние.

Э**лектромагнитные акустоэлектрические преобразователи**. К ним относятся электромагниты электромеханических звонков и капсюлей телефонных аппаратов, шаговые двигатели вторичных часов, кнопочные извещатели ручного вызова пожарной службы охраняемого объекта и др.

**В электромагнитных** (электромагниты электромеханических звонков и капсюлей телефонных аппаратов, шаговые двигатели вторичных часов) – электрический сигнал возникает в результате изменения напряженности поля при изменениях под действием ак.волны воздушного зазора между сердечником и якорем электромагнита или статора (неподвижной части) или ротора (подвижной части) электродвигателя.

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.

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

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

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

Опасные сигналы, образованные акустоэлектрическими пре­образователями, могут:

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

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

Характер поля зависит от расстояния до его источника. В ближней зоне, в которой расстояние от источника r поля менее длины волны его колебаний, преобладают в зависимости от вида излучателя электрические или магнитные компоненты так называемого поля индукции. Напряженность компонент поля индукции убывает пропорционально 1/r3 и 1/r2. В дальней зоне, начиная с расстояния от источника более примерно , преобладает поле излучения в виде электромагнитной волны, энергия которой делится поровну между электрической и магнитной компонентами. Напряженность электромагнитного изотропного поля убывает с расстоянием пропорционально 1/r.

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

**4. Принципы возникновения побочных низкочастотных и высокочастотных излу­чений радиосредств и электрических приборов.**

ПНЧИ образуются при протекании по токопроводам радиосредств (монтажным и соединительным проводам, дорожкам печатных плат) электрического тока с конф.И в звуковом диапазоне частот (ближняя зона).

*Источниками* ***ПНЧИ*** *могут быть:*

* телефоны
* устройства громкоговорящей связи
* усилители мощности.

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 токо-проводящих конструкциях, в том числе в цепях электропитания и металлической арматуре зданий.

*Источниками* ***побочных высокочастотных колебании*** *являются:*

- высокочастотные генераторы, входящие в состав многих радиотехнических средств (телевизоров, радиоприемников, аудио- и видеомагнитофонов, 3-х программных абонентных громкоговорителей);

- усилительные каскады, в которых при определенных условиях возникают паразитные высокочастотные колебания;

- нелинейные элементы (диоды, транзисторы и другие активные радиоэлементы), на которые подаются гармонические высокочастотные колебания и электрические сигналы с речевой информацией.

*Высокочастотные генераторы выполняют в радиоприемниках функции генераторов гармонических колебаний -* ***гетеродинов***, *необходимых для преобразования частоты*, в магнитофонах они создают токи стирания и подмагничивания. Колебания этих генераторов в результате акустоэлектрических преобразований в их элементах (индуктивностях, емкостях) или воздействий на генераторы электрических сигналов с информацией, могут быть промодулированы речевыми сигналами и излучаться в окружающее пространство. Например, если под действием акустической волны меняются параметры контура генератора, то происходит частотная модуляция его колебаний.

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

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

Наиболее опасные сигналы (потенциально‑информативными ПЭМИ) создает элементы ПК, в особенности в пластмассовых неметаллизированных корпусах. Ориентировочные дальности обнаружения радиоизлучений широко распространенных ПЭМИ зарубежного производства приведены в таблице:

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

Устройства компьютера, в которых распространяются сигна­лы в последовательном коде (мониторы, клавиатура, принтеры и другие), 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.

**5. Паразитные связи и наводки**

**Утечка информации по цепям электропитания и заземления**

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. Основная часть высокой цены (десятки тысяч долларов) высокоточных контрольно-измерительных при­боров фирм Hewlett Packard, Ronde & Scwarz и др. приходится на меры по уменьшению 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.**

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

- гальваническая;

- индуктивная;

- емкостная.

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

К таким цепям относятся, прежде всего, цепи питания и заземления. Цепи электропитания обеспечивают передачу электрической энергии в виде переменного электрического тока напряжением 220 В и частотой 50 Гц от вне­шних источников (подстанций) подавляющему большинству устанавлива­емых в помещениях радио- и электрических приборов.

Функциональный или опасный сигнал может при определенных условиях проникать через цепи питания прибора в сеть электропитания помещения и здания, далее через силовой щит в силовой кабель, по которому подается электроэнергия с подстанции. Кроме того, потребление энергии любым радиоэлектронным средством в текущий момент времени зависит от амплитуды токов, циркулирующих в нем, в том числе токов, несущих полезную информацию. Следовательно, ток, потребляемый средством, может содержать переменную составляющую, соответствующую информационному сигналу. Существенное различие частот электропитания 50 Гц и речевого сигнала позволяет, в принципе, выделить с помощью частотных фильтров опасный сигнал чрезвычайно малой амплитуды на фоне напряжения 220 В.

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

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

**Паразитные индуктивные связи.** Причиной таких связей являются индуктивные связи между входом уси­лителя и различными источниками переменного поля, создающими магнитные поля. Такие связи возникают главным образом при наличии в схеме усилителя входного трансформатора. Переменные магнитные поля выходных или питаю­щих трансформаторов, пересекая витки обмоток входного трансформатора, наводят в них Э.Д.С. паразитной связи. При достаточном усилении эта Э.Д.С. может быть причиной генерации усилителя (причем генерация может происхо­дить на одной или нескольких частотах в полосе усиления).

Для уменьшения паразитной индуктивной связи входной трансформатор усилителя помещают в экран, выполненный из металла или сплава, обладаю­щего малым удельным сопротивлением (медь или латунь).

Для уменьшения паразитной связи между трансформаторами усилители катушки располагаются так, чтобы их оси были взаимно перпендикулярны. Уменьшение индуктивных связей может быть также достигнуто путем рацио­нального монтажа схемы.

**Паразитная емкостная связь.** Причиной паразитной емкостной связи являются емкости между элемен­тами схемы и монтажа цепей каскадов, входа и выхода усилителя, емкость между входом усилителя и посторонними источниками переменного тока.

С целью уменьшения паразитной емкостной связи необходимо правильно размещать элементы схемы и монтажные провода. В некоторых случаях целесообразно применить электростатические экра­ны. Экраны выполняют в виде проволочной оплетки, алюминиевой фольги и т.п. и присоединяют к корпусу усилителя. В такой экран помещают в первую очередь провода и элементы схем, которые связаны со входом усилителя.

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.

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

**Литература**

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.
3. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И.К.Корнеев, Е.А. Степанов.- М.:Проспект,2011.-336 с.
4. Зегжда Д.П., Ивашко A.M. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2009.

**Лекции № 7-9**

**ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ**

План:

1. Возможные каналы утечки речевой информации

2. Воздушные технические каналы утечки информации

3. Вибрационные технические каналы

4. Электроакустические каналы утечки информации

5. Оптико-электронный технический канал утечки

6. Параметрические технические каналы утечки информации

7. Технические каналы утечки информации, обра­батываемой ТСПИ и передаваемой по каналам связи

8. Электромагнитные каналы утечки информации

9. Электрические каналы утечки информации

**Под техническим каналом утечки информации** (ТКУИ) *пони­мают совокупность объекта разведки, технического средства раз­ведки (TCP) и физической среды, в которой распространяется ин­формационный сигнал.* В сущности, под ТКУИ понимают способ получения с помощью TCP разведывательной информации об объекте.

В зависимости от физической природы сигналы распространя­ются в определенных физических средах. Средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды. К таким средам относятся воздушное пространство, конст­рукции зданий, соединительные линии и токопроводящие элемен­ты, грунт и т.п.

Противодействие промышленному и экономическому шпиона­жу является непрерывным и адекватным новым типам угроз про­цессом развития методов, средств и способов защиты информации.



Объект разведки Техническое средство

разведки

**1. Возможные каналы утечки речевой информации**

*Под акустической понимается информация, носителем которой являются акустические сигналы.* Если источником информации является человеческая речь, то акустическая информация называ­ется речевой.

*Акустический сигнал воздействует на упругую среду и вызыва­ет акустические колебания различной формы и длительности, рас­пространяющиеся от источника колебаний в окружающее про­странство в виде волн различной длины*.

**Первичными источниками** акустических колебаний являются механические колебательные системы, в том числе и органы речи человека, а **вторичными** - преобразователи различного типа, глав­ным образом электроакустические.

**Электроакустические преоб­разователи** *представляют собой устройства, преобразующие аку­стические колебания в электрические для передачи сигнала на расстояние и усиления*.

**Большинство электроакустических преобразователей способ­но выполнять и обратное преобразование электрического сигнала в акустический**. К электроакустическим преобразователям отно­сятся пьезоэлементы, микрофоны, телефоны, громкоговорители и другие устройства.

В зависимости от формы акустических колебаний различают простые (тональные) и сложные сигналы. Тональный - это сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. Сложный сигнал включает целый спектр гармонических составляющих, обусловленный как изменением частоты так и фор­мы сигнала. Речевой сигнал является сложным акустическим сиг­налом в диапазоне частот от 200...300 Гц до 4...6 кГц.

*В зависимости от физической природы возникновения инфор­мационных сигналов, среды распространения акустических коле­баний и способов их перехвата, технические каналы утечки аку­стической (речевой) информации можно разделить на воздушные, вибрационные, оптико-электронные, электроакустические и пара­метрические.*

**2. Воздушные технические каналы утечки информации**

В воздушных технических каналах **средой передачи** акустиче­ских сигналов является **воздух**, и для перехвата акустических сиг­налов используются миниатюрные высокочувствительные микро­фоны и специальные направленные микрофоны. Миниатюрные микрофоны комплексируются с портативными звукозаписываю­щими устройствами или миниатюрными передатчиками. *Устройст­ва, содержащие миниатюрные микрофоны и передатчики в едином конструктиве, называют* ***акустическими закладками***.

*Средами передачи* речевой информации закладными устройст­вами могут служить *радиоканал, оптический канал, сети перемен­ного тока, соединительные линии ВТСС, посторонние проводники* (проложенные вблизи кабели, трубы водоснабжения и канализа­ции, металлоконструкции и т.п.). Для передачи информации по трубам и металлоконструкциям могут использоваться также меха­нические ультразвуковые колебания.

Приём информации, передаваемой закладными устройствами, осуществляется на специальные приёмники, настроенные на соот­ветствующий диапазон волн. Имеются также закладные устройст­ва, позволяющие принимать информацию с обычного телефонного аппарата. Такие устройства устанавливаются или в корпусе теле­фонного аппарата, находящегося в контролируемом помещении и называемом "телефоном-наблюдателем", или скрытно подключа­ются к телефонной линии.

*Подключение информационных акустических закладок пред­полагает проникновение на контролируемое помещение*. Если это невозможно, то для перехвата речевой информации применяют на­правленные микрофоны.

В заключение перечислим **средства перехвата акустических сигналов по воздушным каналам**:

* микрофонами, комплексированными с портативными устрой­ствами звукозаписи;
* направленными микрофонами;
* микрофонами, комплексированными с устройствами передачи информации по радиоканалу;

микрофонами, комплексированными с устройствами передачи информации по сети электропитания 220 В;

* микрофонами, комплексированными с устройствами передачи информации по оптическому каналу в ИК-диапазоне длин волн;
* микрофонами, комплексированными с устройствами передачи информации по телефонной линии;
* микрофонами, комплексированными с устройствами их под­ключения к телефонной линии («телефону-наблюдателю») по сиг­налам вызова от внешнего телефонного абонента;
* микрофонами, комплексированными с устройствами передачи информации по трубам водоснабжения, отопления, металлоконст­рукциям и т.п.

**3. Вибрационные технические каналы**

*В вибрационных технических каналах утечки информации сре­дой распространения акустических сигналов являются твердые среды (стены зданий, конструкции сооружений, канализации и т.д.).* Для перехвата акустических колебаний в этом случае исполь­зуются контактные микрофоны (**стетоскопы**).

По вибрационному каналу также возможен перехват информа­ции с использованием закладных устройств. Если для передачи информации используется радиоканал, то такие устройства назы­вают **радиостетоскопами**.

Возможно использование закладных устройств с передачей ин­формации по оптическому и по ультразвуковому каналам (по ме­таллоконструкциям здания).

Перехват акустических сигналов по вибрационным техниче­ским каналам возможен:

* электронными стетоскопами;
* стетоскопами с передачей информации по радиоканалу;
* стетоскопами, подключенными к устройствам передачи ин­формации по оптическому каналу в ИК-диапазоне длин волн;
* стетоскопами, объединенными с устройствами передачи ин­формации по трубам водоснабжения, отопления, металлоконструк­циям и т.п.

**4. Электроакустические каналы утечки информации**

**Образование электроакустических каналов утечки информации возможно за счет преобразований акустических сигналов в электрические**. *Перехват акустических колебаний возможен через ВТСС, обладающих «микрофонным эффектом», и путем высоко­частотного навязывания.*

*Некоторые элементы ВТСС, такие как трансформаторы, катуш­ки индуктивности, электромагниты вторичных электрочасов, звон­ки телефонных аппаратов, дроссели ламп дневного света и т.д. из­меняют свои параметры (емкость, индуктивность, сопротивление) под действием акустического давления, создаваемого источником колебаний.* Модуляция параметров элементов ВТСС информаци­онным сигналом приводит к появлению на них ЭДС, изменяющей­ся по закону модулирующего информационного сигнала, или к мо­дуляции токов этих элементов. В состав некоторых ВТСС, кроме названных элементов, могут входить устройства с «микрофонным эффектом», обладающие свойством прямого электроакустического преобразования. Это такие устройства как некоторые датчики по­жарной сигнализации, динамики ретрансляционной сети и т. д. Наиболее ярко выраженным «микрофонным эффектом» обладают абонентские громкоговорители.

*Перехват акустических колебаний в электроакустическом кана­ле возможен путем непосредственного подключения специальных высокочувствительных усилителей НЧ к соединительным линиям ВТСС.*

*Технический канал утечки информации путем высокочастотно­го навязывания может быть реализован несанкционированным контактным введением высокочастотного сигнала в линии, имею­щие гальванические связи с нелинейными или параметрическими элементами ВТСС, на которых происходит модуляция ВЧ сигнала информационным.* Информационный сигнал в данных элементах ВТСС возникает вследствие «микрофонного эффекта». Так как не­линейные или параметрические элементы для ВЧ сигнала пред­ставляют собой несогласованную нагрузку для ВЧ сигнала, то промодулированный ВЧ сигнал будет от нее отражаться в виде обрат­ной волны и распространяться в противоположном направлении или излучаться. Перехват отраженных или излученных ВЧ сигна­лов осуществляется специальными приемниками с высокой чувст­вительностью. Для исключения взаимного влияния зондирующего и отраженного сигналов могут использоваться импульсные сигна­лы. При этом отраженный сигнал принимается во время пауз меж­ду зондирующими импульсами.­ *Перехват акустических колебаний возможен: через ВТСС, обладающих «микрофонным эффектом», путем подключения к их соединительным линиям; через ВТСС путем «высокочастотного навязывания».*

**5. Оптико-электронный технический канал утечки**

*Оптико-электронный технический канал утечки информации образуется путем облучения лазерным лучом вибрирующих в аку­стическом поле тонких отражающих поверхностей (стекол, картин, зеркал).* Отраженное лазерное излучение модулируется по ампли­туде и фазе по закону вибрации поверхности в соответствии с аку­стическим сигналом и принимается чувствительным приемником лазерного излучения, при демодуляции которого выделяется рече­вая информация. *Лазер и приемник могут быть установлены в од­ном или разных местах. Лазер и приемник образуют сложную ла­зерную акустическую локационную систему («лазерный микро­фон»), работающую в ближнем инфракрасном диапазоне волн.*

**6. Параметрические технические каналы утечки информации**

**Вследствие воздействия акустического сигнала меняется давле­ние на все элементы высокочастотных генераторов ТСПИ и ВТСС, находящиеся в акустическом поле.** *В результате этого незначи­тельно изменяется взаимное расположение элементов схем, прово­дов в катушках индуктивности, дросселей и т. п., что может при­вести к изменениям параметров высокочастотного сигнала генера­тора (чаще всего частоты) по закону модуляции его информацион­ным сигналом*. **Поэтому этот канал утечки информации называется параметрическим.** Воздействие акустического поля на кон­денсаторы также приводит к частотной модуляции высокочастот­ного сигнала генератора из-за изменения расстояния между пла­стинами, а, следовательно, и изменения емкости конденсатора. Наиболее существенно подвержены паразитной модуляции инфор­мационным сигналом излучения гетеродинов радиоприемных и телевизионных устройств, имеющих конденсаторы переменной емкости с воздушным диэлектриком в колебательных контурах ге­теродинов.

Модулированные информационным сигналом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы специальными приемниками средств радиоразведки.

Параметрический канал утечки информации может быть орга­низован также и при высокочастотном облучении помещения с установленными полуактивными закладными устройствами, неко­торые характеристики которых модулируются по закону изменения акустического сигнала. Так, например, при облучении мощным на­правленным высокочастотным сигналом помещения, в котором находится такое закладное устройство, в последнем при взаимо­действии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором или объемным резонатором) происходит образование вторичных радиоволн, т.е. переизлучение электромагнитного поля. Полуак­тивные закладные устройства подобного типа могут обеспечивать амплитудную, фазовую или частотную модуляцию переотраженно­го сигнала по закону изменения речевого сигнала. Для перехвата информации по данному каналу кроме закладного устройства не­обходимы специальный передатчик с направленной антенной и приемник.

Перехват акустических сигналов в параметрических техниче­ских каналах утечки информации возможен:

* путем приема и детектирования электромагнитных излучений (ЭМИ) на частотах ВЧ генераторов ТСПИ и ВТСС, модулирован­ных информационным сигналом;
* путем «высокочастотного облучения» специальных полуактив­ных закладных устройств

**7. Технические каналы утечки информации, обра­батываемой ТСПИ и передаваемой по каналам связи**

В настоящее время для передачи информации используют в ос­новном KB, УКВ, радиорелейные, тропосферные и космические каналы связи, а также кабельные и волоконно-оптические линии связи. В зависимости от вида каналов связи технические каналы перехвата информации можно разделить на *электромагнитные, электрические и параметрические.*

**Электрические линии связи**

*Средства передачи электрических сигналов.* Работа любого электронного устройства основана на получении, обработке и пере­даче информации, представленной в виде электрических сигналов. В передаче электрического сигнала участвуют источник, средства передачи и приемник сигнала. **Устройства передачи электрических сигналов от источника к приемнику называют *электромагнитными линиями связи* или кратко - *линиями связи.*** Линии связи используют в качестве средства передачи энергию электрического поля, маг­нитного поля, электромагнитного поля излучения, электрические проводники и волноводы.

*Напряженность электрического и магнитного полей в про­странстве убывает обратно пропорционально квадрату расстояния от элемента, являющегося источником поля.*

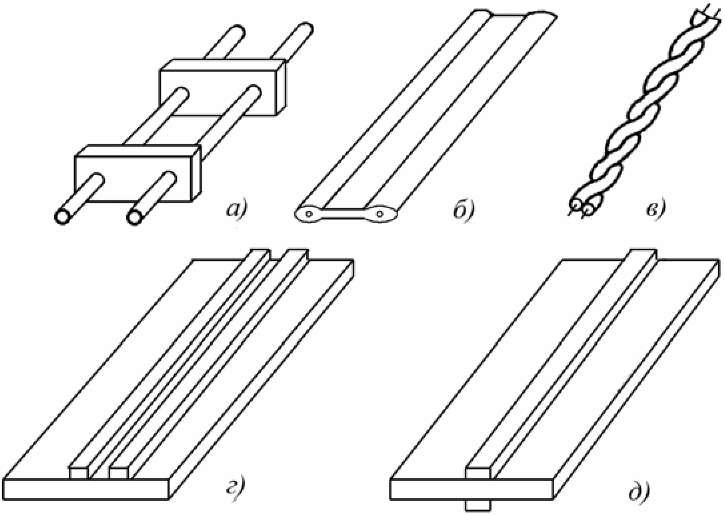
*В электронных устройствах конденсаторы и ка­тушки индуктивности используют как средства для формирова­ния требуемых частотных и фазовых характеристик линий связи.*

*Электромагнитная волна (ЭМВ) излучения представляет собой совокупность электрического и магнитного полей, распространяю­щихся в пространстве со скоростью света.*

*В электронных устройствах применяют преимущественно проводные линии связи.*

*При дефектах конструирования может возникнуть ЭМВ из­лучения, создающая помехи работе других устройств, или могут воз­никнуть условия, при которых принимается ЭМВ излучения из ок­ружающего пространства другими устройствами, что будет соответ­ствовать образованию канала утечки информации*.

*Виды проводных электрических линий связи.* Проводные ли­нии связи подразделяются на симметричные, несимметричные, коак­сиальные.

Симметричные двухпроводные линии связи (рис. 1.4) имеют два провода, по одному из которых течет прямой ток, а по другому - обратный. Симметричные двухпроводные линии могут быть реа­лизованы в виде двух параллельных проводов, закрепленных на изолирующих распорках (рис. 1.4,а ), или иметь непрерывную гибкую оболочку (рис. 1.4,6) из диэлектрика, или в виде двух свитых про­водов (рис. 1.4,в), или в виде двух одинаковых печатных проводни­ков, расположенных с одной (рис. 1.4,г) или с двух (рис. 1.4,д) сто­рон печатной платы. Линии связи (ЛС), выполненные на печатной плате, называют полосковыми.

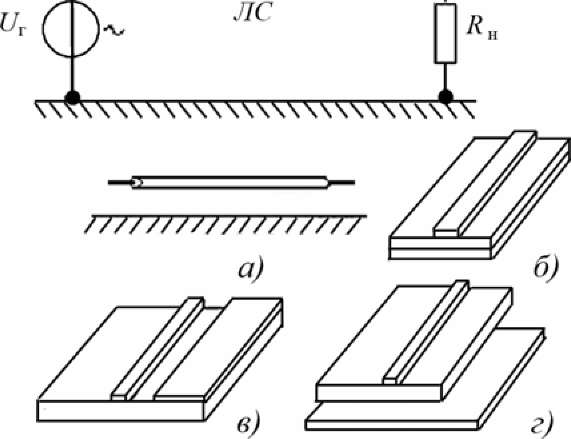
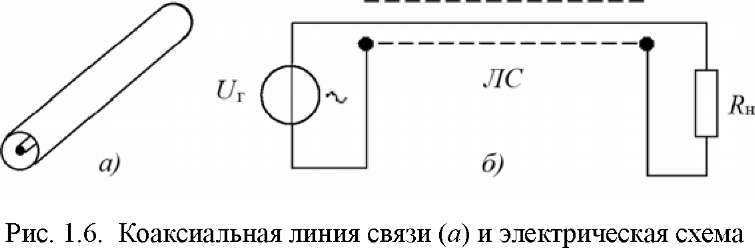
Несимметричные однопроводные линии связи (рис. 1.5) состоят из одного провода, по которому проходит прямой ток. В качестве обратного провода могут использоваться корпус блока, земляная шина, шина питания или провод, общий для нескольких линий связи.

Рис. 1.5. Электрическая схема и варианты конструктивного исполнения несимметричных однопроводных линий связи: а — объемный проводник; б — печатный проводник на двусторонней плате; е — печатный проводник на односторонней плате с общим прово­дом на плате; *г* — печатный проводник вблизи токопроводящего корпуса, используемого в качестве общего провода

Несимметричные однопроводные линии могут быть реализованы в виде одиночного объемного (рис. 15,а) или печатного (рис. 1.5,6- г) проводников. В несимметричных однопроводных JIC токи, теку­щие по прямому и обратному проводам, в общем случае не равны между собой.

Коаксиальный кабель, представляющий собой экранирован­ный провод состоит из двух цилиндрических проводов, вставленных концентрично один в другой (рис. 1.6,а). Прямой ток проходит по центральному проводу, обратный - по оболочке (рис. 1.6, б).

*Помехи (наводок) в каналах связи.* При работе электрон­ных устройств имеют место *паразитные связи, помеха, элементы.*

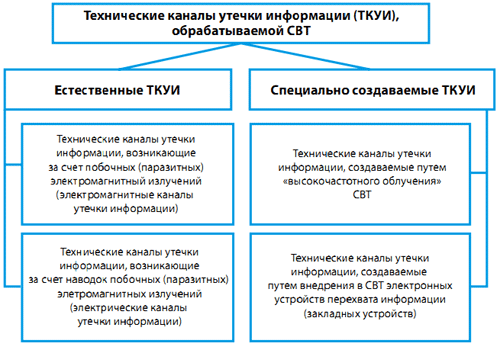
***Паразитная связь*** обусловлена не предусмотренной электри­ческой схемой и конструкцией изделия связью между элементами устройства или устройством и внешней средой, приводящая к появ­лению помехи.

***Помехи*** представляют собой электрические сигналы, не преду­смотренные электрической схемой изделия. Помехи подразделяются на *шумы и наводки*. ***Наводки*** - это помехи, возникающие из-за паразитных связей. ***Шумы*** - это электрические сигналы (помехи), обу­словленные в электронных приборах их внутренними свойствами независимо от наличия внешних связей и сигналов.

Паразитные связи обусловлены неидеальностью конструирования электрической схемы, поэтому значения наводок в основном опре­деляются конструкцией изделия.

***Паразитными*** называют ***элементы***, появившиеся в резуль­тате неидеальности практической реализации электрической схемы из-за невозможности создания проводников и линий связи, не об­ладающих сопротивлением, индуктивностью и емкостью.

*Канал связи может являться как источником, так и прием­ником помех. Если два канала связи имеют взаимную паразитную связь, то и наводки, а, следовательно, и утечка информационных сигналов, возникают в обоих каналах взаимно. Уровень наводок и их влияние на работу канала связи зависит от относительного уровня сигналов в каналах.*

****

**8. Электромагнитные каналы утечки информации**

**К *электромагнитным* относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений ТСПИ**.

*Побочные электромагнитные излучения (ПЭМИ)* - *это паразитные электромагнитные излучения радиодиапазона, соз­даваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными*.

К побочным электромагнитным излучениям ТСПИ относятся:

* излучения элементов ТСПИ;
* излучения на частотах работы высокочастотных (ВЧ) генера­торов ТСПИ;
* излучения на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

**Электромагнитные излучения элементов ТСПИ**

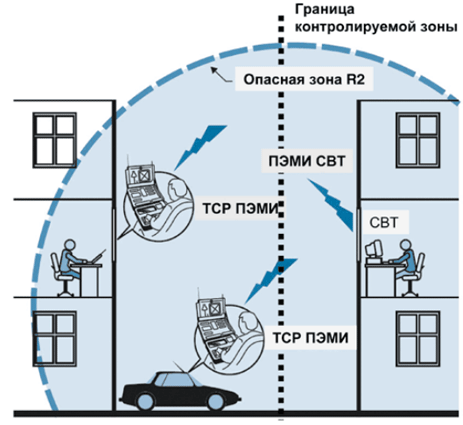
В ТСПИ носителем информации является электрический ток, характеристи­ки которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электриче­ского тока по проводникам ТСПИ вокруг них в окружающем про­странстве возникает электрическое и магнитное поле. По этой при­чине элементы ТСПИ можно рассматривать как излучатели элек­тромагнитного поля, составляющие которого модулированы также по закону изменения информационного сигнала.

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодиро­вания.

*Данный канал перехвата информации наиболее широко исполь­зуется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи*.

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными за пределами контролируемой зоны.

*Зона, в которой возможен перехват побочных электромагнит­ных излучений с помощью разведывательного приемника с после­дующей расшифровкой содержащейся в них информации (т.е. зона, в пределах которой отношение "информационный сигнал/помеха" превышает допустимое нормированное значение), называется* **(опасной) *зоной 2.***

** Зона R2 для каждого СВТ определяется инструментально-расчётным методом при проведении специальных исследований СВТ на ПЭМИ и указывается в предписании на их эксплуатацию или сертификате соответствия.

Таким образом, для возникновения электромагнитного канала утечки информации необходимо выполнение двух условий:

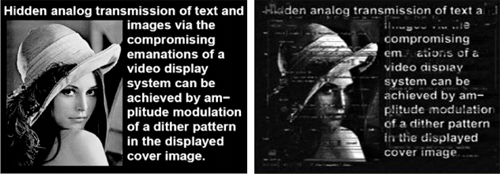
* первое - расстояние от СВТ до границы контролируемой зоны должно быть менее зоны R2 R < R2);
* второе - в пределах зоны R2 возможно размещение стационарных или перевозимых (переносимых) средств разведки ПЭМИН.

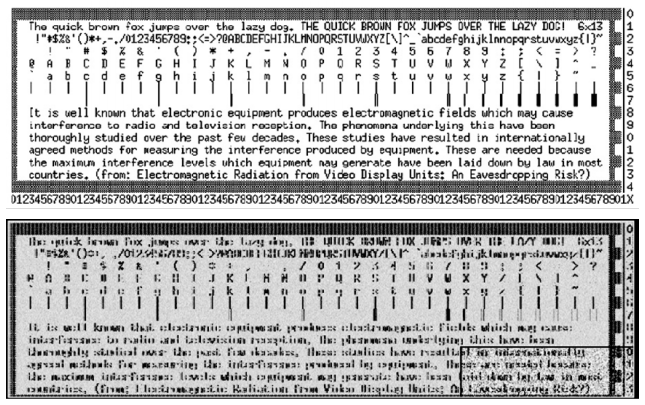
**9. Электромагнитные излучения персональных компьютеров**

Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники:

* вывод информации на экран монитора;
* ввод данных с клавиатуры;
* запись информации на накопители;
* чтение информации с накопителей;
* передача данных в каналы связи;
* вывод данных на периферийные печатные устройства - принтеры, плоттеры; запись данных от сканера на магнитный носитель и т.д.

Согласно оценочным данным по каналу ПЭМИН (побочных элек­тромагнитных излучений и наводок) может быть перехвачено не более 2% процентов данных, обрабатываемых на персональных компьютерах и других технических средствах передачи информа­ции (ТСПИ). На первый взгляд может показаться, что этот ка­нал менее опасен по сравнению, например, с акустическим, по ко­торому из помещения может быть перехвачена речевая информа­ции в полном объеме. Но необходимо помнить, что в настоящее время наиболее важная информация, содержащая государственную тайну или технологические секреты, обрабатывается на персо­нальных компьютерах. Специфика канала ПЭМИН такова, что те самые два процента информации, уязвимые для технических средств перехвата - *это данные, вводимые с клавиатуры компью­тера или отображаемые на мониторе*.

*Рис. Тестовое изображение, выведенное на экран монитора (а) и изображение, перехваченное средством разведки ПЭМИ (б)*

*Рис. Исходный текст, выведенный на экран монитора (режим работы VGA монитора 800\*600 @ 75Hz, тактовая частота Fm= 49,5МГц, размер букв 6 x 13 пикселей) (а) и текст, перехваченный  
 средством разведки ПЭМИ (DFпр = 200 МГц) (б)*

Компьютеры порождают электромагнитные излучения, кото­рые не только создают помехи для радиоприема, но также создают технические каналы утечки информации. Соединительные кабели (линии связи), обладающие индуктивностью и емкостью, образуют резонансные контуры, излучающие высокочастотные электромаг­нитные волны, модулированными сигналами данных.

Уровни побочных электромагнитных излучений ВТ регламен­тированы по условиям электромагнитной совместимости целым рядом зарубежных и отечественных стандартов. Так, например, согласно публикации N22 CISPR (специальный международный комитет по радиопомехам) для диапазона 230... 1000 МГц уровень напряженности электромагнитного поля, излучаемого оборудова­нием ВТ, на расстоянии 10 м не должен превышать 37 дБ. Однако, излучения такого уровня могут быть перехвачены на значительных расстояниях. Следовательно, соответствие электромагнитных из­лучений средств ВТ нормам на электромагнитную совместимость не обеспечивает сохранение конфиденциальности обрабатываемой в них информации. Кроме того, надо иметь в виду, что значитель­ная часть парка ПК в России не отвечает даже нормам по электро­магнитной совместимости, так как в страну ввозилась техника, не имеющая сертификатов качества.

**10. Электрические каналы утечки информации**

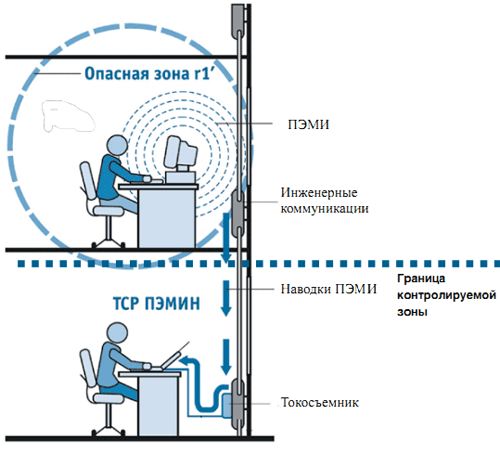
Электрические каналы утечки информации образуются за счет:

* наводок электромагнитных излучений ТСПИ на соединитель­ные линии ВТСС и посторонние проводники, выходящие за преде­лы контролируемой зоны;
* просачивания информационных сигналов в цепи электропита­ния ТСПИ;
* просачивания информационных сигналов в цепи заземления ТСПИ.

**Наводки электромагнитных излучений ТСПИ**

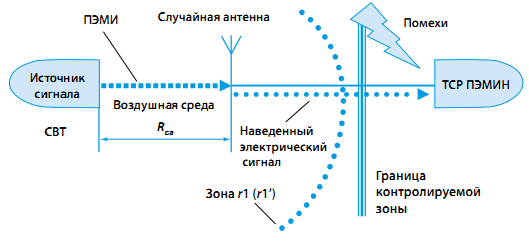
Наводки возникают при излучении элементами ТСПИ (в том числе и их соединительными линиями) информационных сигналов, а также при наличии гальванической связи соединительных линий ТСПИ и посторонних проводников или линий ВТСС. Уровень на­водимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины соединительных линий ТСПИ и посторонних проводников.

Пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше нормирован­ного уровня, называется (опасной) *зоной 1.*



Случайными антеннами могут быть цепи ВТСС или посторон­ние проводники, способные принимать побочные электромагнит­ные излучения.

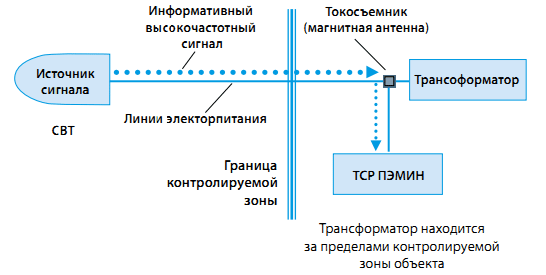
***Рис. Перехват наводок информативных сигналов с инженерных коммуникаций техническим средством разведки ПЭМИН***

*Пространство вокруг ТСОИ, на границе и за пределами которого уровень наведённого от ТСОИ информативного сигнала в сосредоточенных антеннах не превышает допустимого (нормированного) значения (U=Un), называется* **опасной зоной 1** (r1), а *в распределённых антеннах* - **опасной зоной 1'**

Размер зоны r1 (r1') зависит не только от уровня побочных электромагнитных излучений ТСОИ, но и от длины случайной антенны (от помещения, в котором установлено ТСОИ до места возможного подключения к ней средства разведки).

Зоны r1 и r1' для каждого СВТ определяются инструментально-расчётным методом, и их значения указываются в предписании на их эксплуатацию СВТ.

В случае нахождения трансформаторной подстанции или заземлителя контура заземления за пределами контролируемой зоны объекта, при подключении к ним средства разведки ПЭМИН возможен перехват наведённых в них информативных сигналов.

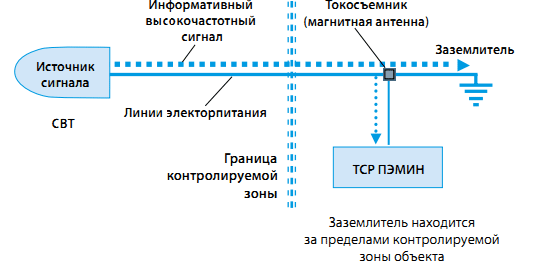
****

*Рис. Схема технического канала утечки информации,  
 возникающего за счёт наводок информативных сигналов  
 в линиях электропитания и заземления СВТ*

**Просачивание информационных сигналов в цепи заземления**

Кроме заземляющих проводников, служащих для непосредст­венного соединения ТСПИ с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны (металлические оболочки) соедини­тельных кабелей, металлические трубы систем отопления и водо­снабжения, металлическая арматура железобетонных конструкций и т.д. Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, в которой могут на­водиться информационные сигналы. Кроме того, в грунте вокруг заземляющего устройства возникает электромагнитное поле, кото­рое также является источником информации.

Перехват информационных сигналов по электрическим каналам утечки возможен путем непосредственного подключения к соеди­нительным линиям ВТСС и посторонним проводникам специаль­ных устройств съема информации. Для перехвата электромагнитных сигналов используются специальные средства радио- и радио­технической разведки.

*Рис. Схема технического канала утечки информации,   
возникающего за счёт наводок информативных сигналов  
 в цепях заземления СВТ*

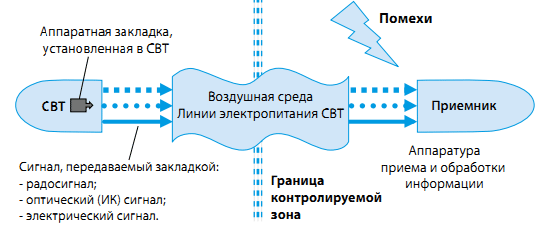
**Съем информации по электрическим каналам утечки информации**

Для съема информации, обрабатываемой в ТСПИ, применяют главным образом электронные устройства перехвата информации - *закладные устройства.* Электронные устройства перехвата ин­формации, устанавливаемые в ТСПИ, иногда называют *аппарат­ными закладками.* Они представляют собой мини-передатчики, из­лучение которых модулируется информационным сигналом. За­кладки устанавливаются в ТСПИ как иностранного так отечествен­ного производства.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала на­капливается на специальном запоминающем устройстве, а уже за­тем по сигналу извне передается на запросивший ее объект.

Закладные устройства, внедряемые в СВТ, по виду перехватываемой информации можно разделить на:

* аппаратные закладки для перехвата изображений, выводимых на экран монитора;
* аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ;
* аппаратные закладки для перехвата информации, выводимой на периферийные устройства (например, принтер);
* аппаратные закладки для перехвата информации, записываемой на жёсткий диск ПЭВМ.

*Рис. 16. Схема технического канала утечки информации,   
создаваемого путём внедрения в СВТ закладных устройств*

**Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры разведки к кабельным линиям связи**.

Самый простой способ - это непосредственное параллельное под­ключение к линии связи. Но данный факт легко обнаруживается, так как приводит к изменению характеристик линии связи за счет падения напряжения. Поэтому средства разведки к линии связи подключаются или через согласующее устройство, несколько снижающее падение напряжения, или через специальные устройства компенсации падения напряжения. В последнем случае аппаратура разведки и устройство компенсации падения напряжения включаются в линию связи после­довательно, что существенно затрудняет обнаружение факта несанк­ционированного подключения к ней.

Контактный способ используется в основном для снятия ин­формации с коаксиальных и низкочастотных кабелей связи.

Электрический канал наиболее часто используется для перехва­та телефонных разговоров. Устрой­ства, подключаемые к телефонным линиям связи и комплексированные с устройствами передачи информации по радиоканалу, час­то называют *телефонными закладками.*

Для бесконтактного съема информации с незащищенных теле­фонных линий связи могут использоваться специальные низкочас­тотные усилители, снабженные магнитными антеннами.

Некоторые средства бесконтактного съема информации, пере­даваемой по каналам связи, могут комплексироваться с радиопере­датчиками для ретрансляции в центр ее обработки.

Исходя из выше перечисленных особенностей ТСПИ и ВТСС, а также возможностей современных технических разведок можно заключить, что всегда существует потенциальная опасность воз­никновения технического канала утечки информации. И эта про­блема должна решаться за счет совершенствования применяемого оборудования (ТСПИ и ВТСС), так и применения средств активной защиты.

**Параметрический канал утечки информации**

Параметрический канал утечки информации используется для перехвата обрабатываемой в технических средствах информации путем их *«высокочастотного облучения».* При воздействии облу­чающего электромагнитного поля на элементы ТСПИ происходит переизлучение электромагнитного поля. В ряде случаев возможна модуляция вторичного излучающего поля информационным сиг­налом. Для исключения взаимного влияния облучающего и переиз­лученного сигналов может использоваться их временное или час­тотное разделение. Например, для облучения ТСПИ могут исполь­зовать импульсные сигналы, в промежутках между которыми осу­ществляется прием переизлученных сигналов.

При переизлучении параметры сигналов изменяются. Поэтому данный канал утечки информации часто называют *параметрическим.*

Для перехвата информации по данному каналу применяют специальные высокочастотные генераторы с антеннами, имеющи­ми узкие диаграммы направленности, и специальные радиоприем­ные устройства.

Информация после обработки в ТСПИ может передаваться по проводным каналам связи, где также возможен ее перехват.

**Литература**

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.
3. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И.К.Корнеев, Е.А. Степанов.- М.:Проспект,2011.-336 с.
4. Зегжда Д.П., Ивашко A.M. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2009.

**Лекции № 10-12**

**СПОСОБЫ СКРЫТОГО ВИДЕОНАБЛЮДЕНИЯ И СЪЕМКИ**

План:

1. Скрытая фото- и видеосъемка

2. Аппаратура для скрытой фото- и видеосъемки

3. Приборы ночного видения

4. Тепловизоры

5. Рентгеновские установки

6. Бинокли, монокуляры

1. Визуальное наблюдение является самым древним и очень эф­фективным методом сбора информации. Как известно, высокий уровень охраны субъекта или объекта предполагает значительное насыщение пространства вокруг охраняемого самыми разнообраз­ными техническими средствами и многочисленными сотрудниками охраны. Данное обстоятельство осложняет доступ к объекту и по­лучение информации о деятельности физических лиц. Поэтому для выявления интересующих подробностей в 99% случаев из ста при­меняется разнообразная оптика.

*Задача своевременного выявления и обнаружения ведущегося оптического наблюдения становится, таким образом, одной из важнейших при проведении как профилактических, так и специ­альных защитных и охранных мероприятий*. Ведь своевременное обнаружение факта несанкционированного наблюдения дает воз­можность установить, с какой целью оно проводится и определить угрозу, которая может исходить от наблюдающего за тем или иным объектом, персоной или группой лиц.

Для получения информации широко используется скрытая фото- и видеосъемка.

*В настоящее время для сбора информации могут использовать­ся миниатюрные скрытые и специальные (камуфлированные под обычные предметы) фото- и видеокамеры*:

* миниатюрные (скрытые). Встраиваются в бытовую технику и передают видеоинформацию по кабелю или по ВЧ каналу при по­мощи телевизионного передатчика;
* специальные, т.е. замаскированные под бытовые предметы, например пачку: сигарет, кейс, книгу, наручные часы и т.п.

2. *Аппаратура для скрытой фото- и видеосъемки, как правило, оборудуется специальными объективами и насадками*:

* *миниатюрными объективами*, предназначенными для съемки через отверстия небольшого диаметра (до 5 мм);
* *телескопическими объективами*, позволяющими вести съемку с дальних расстояний. Такие объективы обладают высокой кратно­стью увеличения (до 1,5 тыс. крат);
* *камуфляжными объективами*, используемыми для скрытой съемки из различных бытовых предметов, например из кейсов;
* *объективами, совмещенными с приборами ночного видения* (с инфракрасной подсветкой), и предназначенными для проведения съемки в темное время суток.

Спецслужбы давно и широко применяют различные оптические приборы для скрытного наблюдения и регистрации информации в дневных и ночных условиях при любой погоде.

*Для видеонаблюдения в дневное время применяются традици­онные оптические приборы*: бинокли, монокуляры, подзорные тру­бы, телескопы и др.

*Для наблюдения за объектами на значительном расстоянии ис­пользуются специальные телескопы*. Например, телескоп прибора РК 6500 позволяет опознать автомобиль на расстоянии до 10 км.

*Для ведения разведки ночью находят применение специальные телевизионные камеры*, работающие при низком уровне освещён­ности и приборы ночного видения.

3. *Приборы ночного видения*

Расширение возможностей визуализации недоступной для глаз информации является одной из наиболее важных и трудных задач. Первые успешные результаты в этом направлении были получены в 30-х годах XX века. Особенную актуальность проблема наблюде­ния в условиях низкой освещенности приобрела в ходе Второй мировой войны. Ее практическая реализация предоставила возмож­ность действовать в сумерках и ночью без использования источни­ков видимого света.

***Принцип действия классического прибора ночного видения*** *(ПНВ) основан на преобразовании ИК-излучения, создаваемого на наблюдаемом объекте свечением ночного неба, звездами и луной, в видимый свет*.

*На практике наиболее широко применяются приборы на основе оптикоэлектронных приборов (ОЭП) второго поколения*. Такие приборы содержат микроканальную пластинку, представляющую собой диск с большим числом микроскопических каналов. Каждый канал является миниатюрным усилителем вторичной эмиссии электронов, испускаемых катодом ОЭП. Приборы обеспечивают возможность регистрации изображения на фото- и видеокамеры. Они обладают высоким усилением (до 50000), устойчивостью к засветкам, например фар автомашин, равномерным по полю раз­решением и небольшими габаритами. Принцип их действия осно­ван на приёме отражённого местными предметами оптического ИК-излучения и многократного его усиления и преобразования в видимое изображение.

Современные приборы ночного видения работают при освещён­ности менее 0,01 лк. Например, для прибора ночного видения «Ворон- 3» пороговый уровень освещенности для визуального наблюдения составляет 0,001 лк, а для фотографирования - 0,0 1лк. Разрешающая способность в этих условиях - не менее 8 линий на мм.

*Для увеличения дальности наблюдения в условиях абсолютной темноты применяется искусственная подсветка объектов при помощи инфракрасных прожекторов*. В лазерных ИК-осветителях применяет­ся импульсной режим. Объект освещается короткими импульсами лазерного излучения, и прибор включается только тогда, когда его объектива достигают отраженные от цели импульсы. В результате этого паразитные импульсы, отраженные от местных предметов, на­ходящихся впереди и сзади объекта, а также отраженные от взвешен­ных в атмосфере частиц пыли, влаги, дыма не попадают в ПНВ.

Дальность наблюдения портативными приборами ночного ви­дения при использовании подсветки дополнительных инфракрас­ных прожекторов (точечная лампа мощностью 45 Вт) достигает более 500 м.

**4.** *Тепловизионные приборы (ТПВ), работающие в дальнем диапа­зоне инфракрасных волн (от 3 до 14 мкм), имеют преимущества по сравнению с ПНВ, так как их работа не зависит от уровня естественной освещенности*. Кроме того, они обладают скрытностью и большой дальностью действия, способны обнаруживать замаски­рованные объекты. На них слабо влияют задымление и запылен­ность атмосферы, слепящие засветки. *TПB способны обнаруживать следы автомашины и другой техники, способны непосредственно передавать информацию по каналам связи*.

Недостаток тепловизоров заключается в необходимости охла­ждения приемников излучения до температуры 77 К, что увеличи­вает их массу и габариты за счет усложнения конструкции. В по­следнее время появились тепловизоры, работающие при комнатной температуре.

*Своевременное выявление и обнаружение средств оптического наблюдения становится важной задачей при проведении как про­филактических, так и специальных защитных и охранных меро­приятий*.

Своевременное обнаружение несанкционированного наблюде­ния позволяет установить цель его проведения и определить по­тенциальную угрозу факта наблюдения.

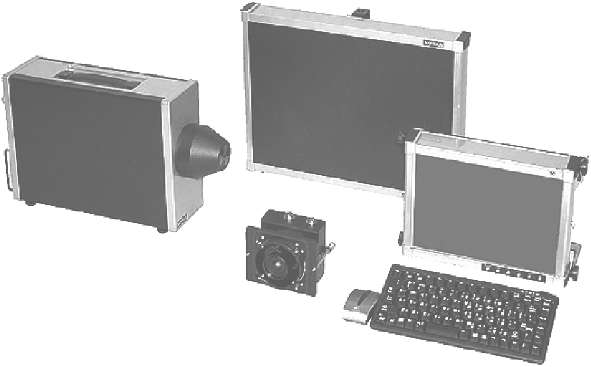
На рис. 1.16 - 1.30 показан внешний вид некоторых перечислен­ных устройств. Специальный телевизионный тюнер «РТВ-2.5» предназначен для приема сигналов изображения, поступающих от передатчиков «ТВФ- 2,5» (рис. 1.16,а). Один приемник обслуживает до 5 передатчиков. Период автоматического сканирования каналов 6 ... 8 с.

В общем случае прием осуществляется на штыревую антенну.

При использовании выносных направленных антенн серии «АТВ-2.5» дальность уверенного приема увеличивается в 5 - 10 раз, а при использовании антенны «АТВ-2.5 В» может достигать 15 км.



Рис. 1. 16. Передатчик телевизионного сигнала «ТВФ-2.5» (а) и система телевизионного наблюдения по ИК-каналу «Верба» (б).

Рис. 1.17. Переносная рентгенотелевизионная установка «НОРКА».

*Закладные устройства обнаруживаются рентгенотелевизионными устройствами типа «НОРКА».*

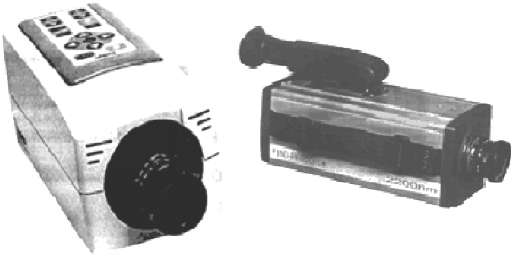


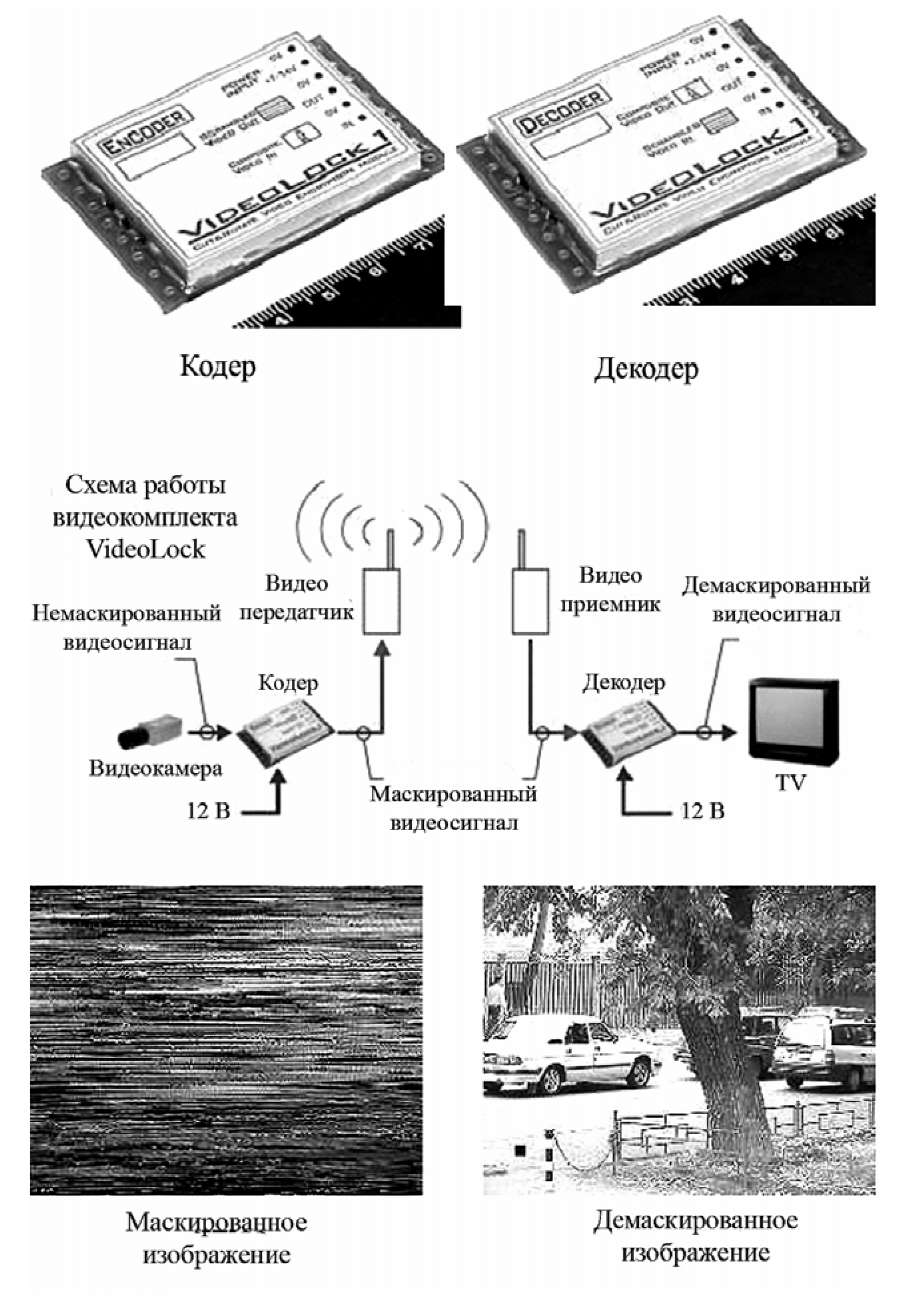
Рис. 1.18. Тепловизионная камера «Merlin-NEAR» (а) и ТВ-камера «Find-R-Scope 85400/95345» (б).

*Для наблюдения многих теплоизлучающих объектов применя­ются тепловизионные приборы на основе фокальных матриц HgCdTe и InSb. Примером такой камеры может служить модель Merlin-NEAR* (рис. 1.18,а) фирмы Indigo Systems (США), работаю­щей в области спектра 0,9 ... 1,68 мкм. Она имеет размер элемента 30x30 мкм, поле обзора 22x16° или 11x8°, массу 1,6 кг, габариты 102x114x203 мм. Камера может обеспечивать измерение темпера­тур в диапазоне от 250 до 2000 °С.

В США фирма Optical Systems Inc. разработала ТВ-камеру (мо­дель Find-R-Scope 85400/95345), работающую в области спектра до 2,2 мкм (рис. 1.18,6). Камера предназначена для видеонаблюдения. Является вариантом ТВ-системы на базе ИК-видикона, работаю­щей в области спектра 1-1,8 мкм.

ТВ-камера имеет массу 1,587 кг, габариты 305x89x114 мм, раз­решение 550 ТВ-линий, потребление по току 1,3 А при напряжении питания 24 В постоянного тока.

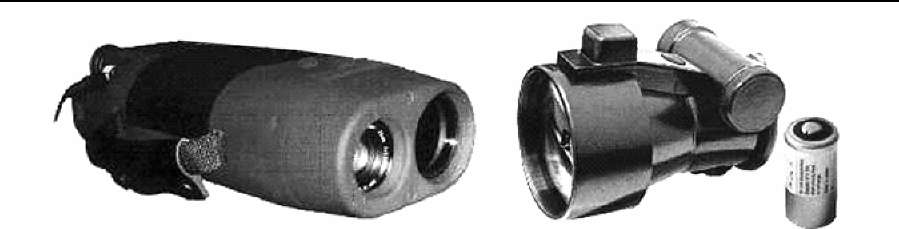
ТВ-камера, кроме эффективного наблюдения при пониженной прозрачности атмосферы, допускает визуализацию излучения ла­зерных дальномеров на длинах волн 1,06, 1,55, 1,7 и 2,1 мкм. Это не обеспечивается другими указанными выше средствами.

*Комплект маскирования видеоизображения «VideoLock»* (рис. 1.19) *предназначен для маскирования видеоизображения при передаче его по проводным или радиоканалам.* В комплекте применены новейшие цифровые технологии для передачи видеоизображения по проводным и радиоканалам. Комплект характеризуется следующими свойствами:

* простота использования;
* метод маскировки: переворот и разрезание видеострок;
* помехи, возникающие при передаче видеоизображения по ра­диоканалу, не оказывают влияния на качество восстановленного изображения;
* изделия выполнены в виде модулей и предназначены для дальнейшей установки в приборы и оборудование;
* совместим с любым TV оборудованием;
* наличие уникального цифрового ключа (индивидуального или группового);
* низкое напряжение питания и малая потребляемая мощность;
* малые габариты и низкая цена.

Рис. 1.19. Комплект маскирования видеоизображения «VideoLock»

*Система круглосуточного наблюдения и обнаружения оптиче­ских объектов «Мираж-1200»* (рис. 1.20) является одной из наибо­лее популярных и активно покупаемых на рынке систем безопасно­сти.



а) б)

Рис. 1.20. Система круглосуточного наблюдения «Мираж-1200» (а) и ма­логабаритный монокуляр-обнаружитель «Алмаз» (б)

Востребованность этой системы объясняется широким кругом решаемых задач. Фактически заказчик получает возможность ис­пользовать одно и то же устройство для различных нужд. Так, от­падает необходимость в использовании приборов ночного видения и обеспечивается возможность видеть круглосуточно. *Фактически предоставляется уникальная возможность получать комбинирован­ное лазерное и телевизионное изображение. Обеспечивается воз­можность видеть в условиях значительных световых помех.* На­пример, при вспышках, засветках, внезапных или постоянных ис­точниках сильного светового излучения.

Будучи компактным и удобным прибором, «Мираж-1200» практически не отличается от обычной видео- или кинокамеры. Это немаловажно для обеспечения скрытого контроля окружающе­го пространства. Наличие «Миража» в руках не будет расценено, как нечто нестандартное, а значит, опасное. Еще одним важным достоинством системы является возможность качественного распо­знавания людей на фоне подстилающей поверхности. От чуткого ока «Миража» не скроется полностью закамуфлированный чело­век. Система «Мираж» хорошо различает глаза людей. Но, пожа­луй, самой интересной особенностью системы является возмож­ность просмотра темных скрытых зон. Например, чердаков, темных комнат или полуподвалов. «Мираж» проникает внутрь помещений, уверенно распознавая находящиеся там предметы и объекты.

*Малогабаритный монокуляр-обнаружитель «Алмаз» (рис. 1.20,6) предназначен для борьбы со скрытыми мини-камерами всех видов и типов в помещениях на дальности до 10 м.* При этом камера мо­жет быть выключена, можно использовать волоконную оптику, различные фильтры, сетки, маскирующие бленды и насадки. «Ал­маз» помещается в руке оператора и практически не видим посто­роннему наблюдателю. Все системы отличаются высоким техниче­ским уровнем исполнения, в них широко используются распро­страненные источники питания, они просты и удобны в эксплуата­ции и обслуживании и могут быть совместимы с другими система­ми, в том числе комплексными системами безопасности.

Имеющийся опыт применения систем обнаружения оптики раз­личными пользователями, позволяет говорить о качественно новом подходе с преобладающей профилактической составляющей к обеспечению безопасности как в сфере коммерческой, так и в сфе­ре государственной.

Сегментация рынка по производителям ПНВ может служить демонстрацией лидерства фирм США. Практически все приборы сегодня выпускаются на основе ЭОП II и III поколений с предель­но высоким разрешением.

Очки «AN/PVS-5B» сегодня замещаются современными «AN/PVS-7B/D», IIT/Litton.

Некоторые из американских ПНВ производят обе фирмы под унифицированными или своими индексами.

Псевдобинокулярные очки ночного видения «AN/PVS-7B/D» (рис. 1.21,6), являются одними из самых распространенных очков в мире. Они практически открыто продаются в комплектации ЭОП II+ и выпускаются фирмами-компиляторами в кооперации с произ­водителями основных компонент.



а) б)

Рис. 1.21. Бинокль «F5010 (GEN III)» (а) и псевдобинокулярная модель «AN/PVS-7B/D» (б)

Выпускаются и другие модификации серии «AN/PVS-7A», на­пример бинокль «F5010 (GEN III)» (рис. 1.21,а) производства ITT, получившей 100% контракта на базовую модель «AN/PVS-7D» и авиационные очки «ANVIS» (III поколение).

Биноклем-псевдобинокуляром является модель «1ПН-94» (рис. 1.22,а) производства Казанского оптико-механического завода. По сути, здесь применена окулярная система ОНВ, выполненная со­вместно с объективом в неразъёмном полистироловом корпусе.



Рис. 1.22. Бинокль-псевдобинокуляр «1ПН-94» (а) и очки ночного видения «1ПН74» (б)

Аналогичный вариант предлагает и «Альфа» в модели «Альфа- 3122» с объективом Красногорского завода. Эта модель имеет пре­восходные характеристики, за исключением массы - 1,2 кг, из-за значительной массы объектива - 630 г.

Классическим примером многообразия однородных форм воз­можно считать очки ночного видения (ОНВ) «1ПН74» (рис. 1.22,6 и рис. 1.23), построенные по псевдобинокулярной схеме.

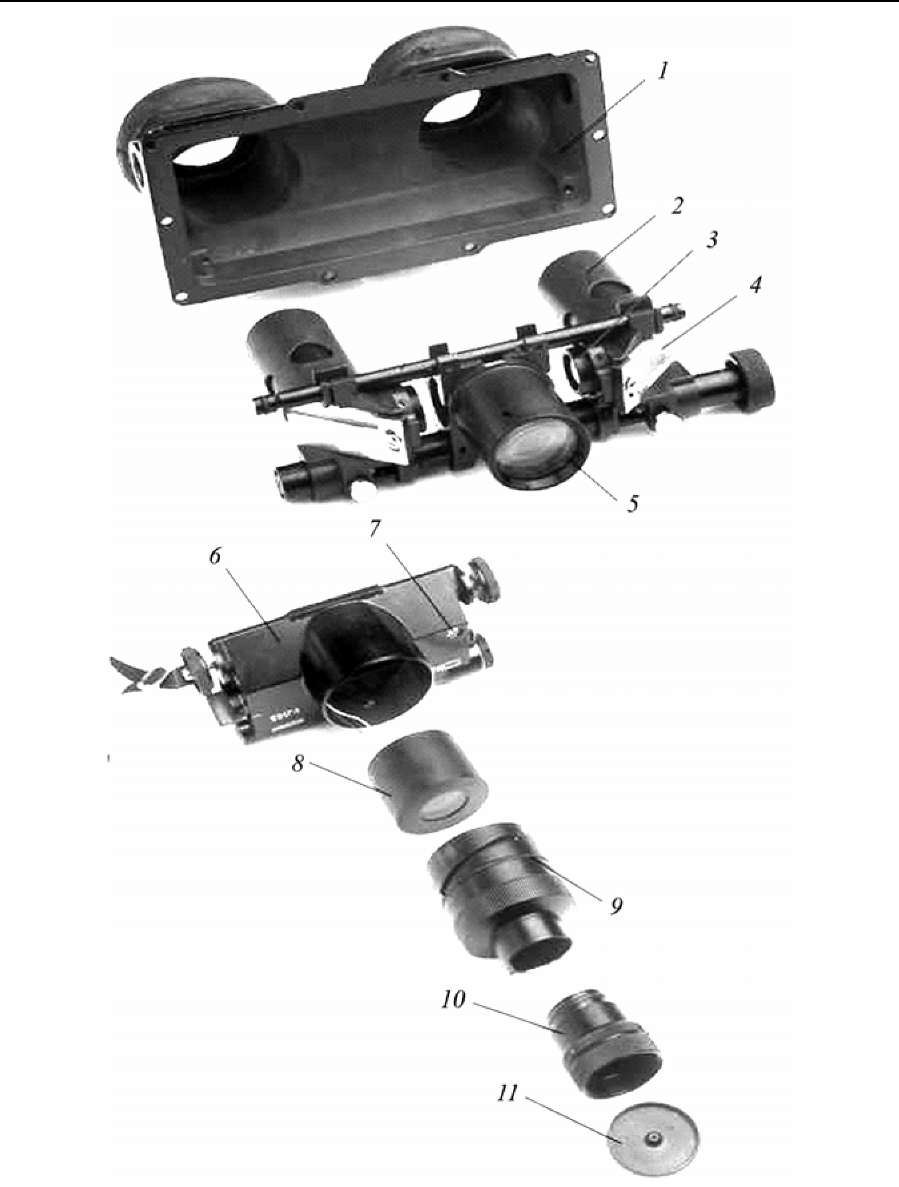


Рис. 1.23. Схема 1ПН74 1 - корпус ОНВ; 2 - окуляр; 3 - оборачивающий объектив; 4 - зеркало; 5 - коллиматор (лупа) с призмой; б - корпус ОНВ; 7 - ИК-подсветка; 8 - ЭОП; 9 - корпус объектива; 10- объектив; 11 - крышка объектива.

Подобные приборы крепятся на голове оператора на специаль­ных масках для обеспечения движения и ориентирования на мест­ности в ночное время, скрытного наблюдения объектов, выполне­ния различного рода инженерно-технических работ, управления транспортными средствами по пересечённой местности без исполь­зования источников видимого света в ночное время.

*«NightMaster NS-2023» (рис. 1.24) представляет собой много­функциональный прибор ночного видения монокулярного типа.* Он свободно умещается на ладони и может применяться как самостоя­тельно, так и в составе систем наблюдения и охранного телевиде­ния, а также фото- и видеосъемки.





Рис. 1.24. Малогабаритный прибор ночного видения «NIGHTMASTER-NS2023»

Электронно-оптический преобразователь «П+SUPER» обеспе­чивает высокую чувствительность и отличное качество изображе­ния. Прибор оборудован системой автоматической защиты от влияния ярких источников света.

*Система «Миф-350»* (рис. 1.25,а). Эта новая модификация хо­рошо известной потребителей надежной и удобной в эксплуатации «городской» системы, обеспечивающей тот же уровень решения оперативных задач, что и «Мираж-1200», но на дальностях до 400 м.

а) б)

Рис. 1.25. Система «Миф-350» (а) и бинокль-псевдобинокуляр «Байгыш-6» (б)

Более миниатюрная по габаритам система *«Миф-350» может использоваться и в помещениях, успешно обнаруживая скрытые камеры*. *Она эффективно «читает» автомобильные номера в темное время суток и устойчива к световым помехам*. Наглядным приме­ром эффективности системы «Миф-350» является ее способность обнаруживать людей скрытно стоящих в простенке между двумя ярко освещенными окнами. Она, как и система «Мираж», практи­чески не чувствительна к подобного рода световым помехам или включенным автомобильным фарам ближнего и даже дальнего све­та. Тогда как использование обычных оптических устройств или приборов ночного видения в подобных условиях невозможно.

Для оптимального решения задач по оптическому мониторингу пространства для «Миф-350» разработана оригинальная методика комплексного использования систем обнаружения оптики. Разра­ботаны приемы работы, позволяющие обнаруживать цели за тони­рованными стеклами помещений и автомобилей.

Осмотр парка псевдобинокулярных конструкций ПНВ будет не полным без упоминания *биноклей. Такие приборы не обеспечива­ют стереоэффекта, но оказываются значительно более дешёвыми за счёт использования одного электронно-оптического преобразова­теля (ЭОП) и объектива*. В этом классе приборов успешно работает Казанский оптико-механический завод (КОМЗ). Наибольшей попу­лярностью пользуется семейство «Байгышей» во главе со знамени­той моделью - «Байгыш-6» (рис. 1.25,6).

*Для разводки изображения в этих моделях используется не оку­лярная, а специальная линзовая система с призмой, обеспечиваю­щая эффект «панорамного видения» изображения экрана ЭОП* (т.е., панорамный окуляр).

«Байгыш-6» является одним из наиболее растиражированных псевдобиноклей и успешно продаётся в РФ и за рубежом, хотя и имеет значительные по современным меркам габариты.

Использовать ЭОП поколений ниже II в псевдобинокулярных ОНВ нецелесообразно из-за низкого коэффициента усиления све­тового потока предшествующих поколений (не более 103 против 2,5-5×104). Тем не менее, такие приборы выпускаются, например, «RECON-1» (рис. 1.26) производства «ЛОМО» (С.-Петербург). В этих ОНВ применён ЭОП 1-поколения.

«RECON-1» выпускается в пластмассовом корпусе и отличает­ся минимальным, для подобных конструкций, массой - 350 г, в ва­рианте псевдобинокля - 520 г.

Рис. 1.26. Псевдобииокуляр со сменным зеркально-линзовым объективом ОНВ «RECON-1»

Прибор «Dedal-41» (рис. 1.27) является псевдобинокулярной моделью и может поставляться как с обычным, так и с панорамным окуляром. Производится московским АО «Дедал-НВ» (торговая марка «Dedal»).



Рис. 1.27. Псевдобинокуляр «Dedal-41»

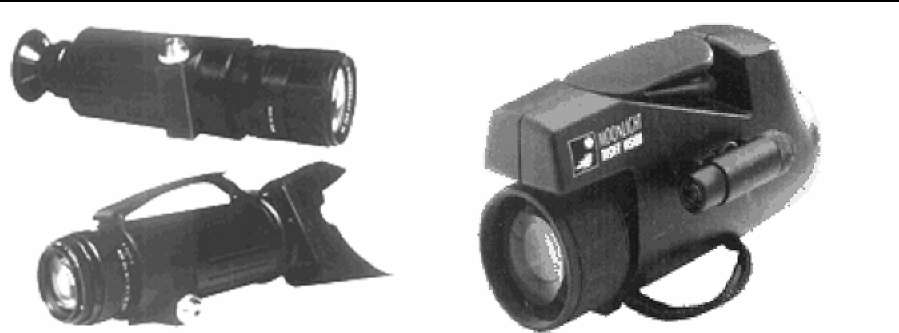
В модели «Dedal-41» используется ЭОП-П с диаметром фотока­тода 25 мм, и, кроме того, предусмотрен монтаж ИК-прожектора. Как развитие этой модели можно рассматривать новинку 1999 года - «Dedal-43» с зеркально-линзовым объективом.

Прибор ночного видения «Дедал-200» (рис. 1.28) построен на базе электронно-оптического преобразователя I-поколения и пред­назначен для наблюдения в условиях низкой освещенности на рас­стояниях до и 350 м. Дополнительно прибор может комплектовать­ся устройством инфракрасной подсветки, позволяющим проводить наблюдение в условиях полной темноты на расстоянии 50-80 м.

Рис. 1.28. Прибор ночного видения «Дедал-200»

Бинокли используются как носимые приборы для наблюдения «с руки» или на штативе. Модель «LYNX 10М-01» фирмы «ТУРН» (Москва) (рис. 1.29,а) конструктивно исполнена несколько по ино­му и может поставляться как с обычным, так и с панорамным оку­ляром.

Самым большим по количеству выпускаемых изделий сегментом ПНВ-рынка является рынок приборов нулевого поколения. Здесь ра­ботает большинство предприятий оптической промышленности Рос­сии. Подобные конструкции не предназначены для профессиональной деятельности.

В наибольшем количестве здесь представлены визиры, от малень­ких, легко умещающихся в руке монокуляров Красногорского оптико- механического завода им. Зверева, одного из крупнейших производи­телей изделий данного вида, до «трубок» и биноклей с 3-4-кратным увеличением, производства «РОМЗа», «Метрона», «Катода» и многих других фирм. Одним из таких приборов является прибор ночного ви­дения «Safari» (рис. 1.29,6).

а) б)

Рис. 1.29. Бинокль-псевдобинокуляр «LYNX 10М-01» (а) и прибор ночно­го видения «Safari» (б)

*Среди подобных ПНВ «общегражданского назначения», боль­шим успехом пользуются приборы с пьезокерамическим элемен­том, не требующие использования батареек или аккумуляторов.* Подобная разработка «РОМЗа» - визир «НЗТ-П», неоднократно отмечалась золотыми медалями на выставках.

В настоящее время ГУП «Альфа» разработан и выпускается монокуляр «А-9021» (рис. 1.30), являющийся самым эргономич­ным из имеющихся на мировом рынке ПНВ (масса -250 г) с наи­лучшим к тому же показателем цена/качество.

По конфигурации «А-9021» напоминает американский «М982/3», производства IIT/Litton, но снаряжается не одним, а двумя источниками питания АА-типа. Монокуляр имеет объектив, унифицированный с 1ПН74.



Рис. 1.30. Монокуляр «9021»

**Литература**

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.
3. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И.К.Корнеев, Е.А. Степанов.- М.:Проспект,2011.-336 с.
4. Зегжда Д.П., Ивашко A.M. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2009.

**Лекции № 13-14**

**СРЕДСТВА РАДИО- И РАДИОТЕХНИЧЕСКОЙ РАЗВЕДКИ**

План:

1.Сканирующие компьютерные радиоприемники, радиопеленгаторы

2. Анализаторы спектра. Радиочастотомеры

**1.Сканирующие компьютерные радиоприемники, радиопеленгаторы**

*В процессе контроля радиоэфира основными действиями яв­ляются поиск, обнаружение и прием требуемых радиосигналов.* *Возможности любого комплекса радиоконтроля, решающего эти задачи, определяются параметрами используемых в нем скани­рующих радиоприемных устройств.* По сути дела именно эти уст­ройства являются одним из важнейших функциональных элемен­тов такого комплекса. *Следует отметить, что сканирующие прием­ники в руках злоумышленников могут служить разведывательным средством.*

Сканирующие радиоприемники характеризуются следующими основными показателями:

* диапазоном принимаемых частот;
* чувствительностью;
* избирательностью;
* параметрами сканирования (скоростью перестройки, полосами обзора и т.д.);
* используемым методом или методами, если они есть, обнару­жения сигналов;
* видом принимаемых радиосигналов;
* оперативностью управления и возможностями его автомати­зации;
* выходными параметрами (качество воспроизведения сигнала на выходе приемника, наличие выходов по промежуточной и низ­кой частоте, значения полос пропускания сигнала по этим частотам и т.д.);
* эксплуатационными параметрами (массогабаритные характе­ристики, требования по электропитанию, надежность, ремонтопри­годность удобство транспортировки и т.п.).

Представленные на отечественном рынке модели сканирующих приемников обычно удовлетворяют требованиям по диапазону и скорости сканирования для поиска радиомикрофонов или других источников радиоизлучения, не использующих режим быстрой пе­рестройки рабочей частоты. В то же время возможность обнаруже­ния таких радиомикрофонов или способность контроля технически сложных каналов радиосвязи зависят не только от параметров ска­нирования радиоприемника, но и от наличия в составе комплекса других средств, обеспечивающих решение подобных задач. В каче­стве таких средств в настоящее время все чаще используются спе­циализированные комплекты программного обеспечения. В этих условиях особое значение приобретает способность сканирующего радиоприемника эффективно работать в составе автоматизирован­ного комплекса радиоконтроля под управлением персонального компьютера. С этой целью рядом зарубежных и российских компа­ний производителей были разработаны так называемые «компью­терные» радиоприемники, специально ориентированные на обес­печение эффективного взаимодействия с ЭВМ. Конструктивно та­кие приемники выполняются либо в виде плат, встраиваемых в ISA-слот компьютера, либо в виде отдельных модулей, подклю­чаемых к компьютеру через порты COM, LPT или PCMCIA. Благо­даря такому решению обеспечивается высокая скорость обмена информацией между радиоприемником и компьютером, а отсутст­вие дополнительных внешних органов управления позволяет дос­тичь небольших значений массогабаритных параметров приемника.

Технические характеристики некоторых сканирующих прием­ников приведены ниже.

**Сканирующий приемник AR5000** (рис. 3.1,а) предназначен для контроля радиоэфира в диапазоне частот от 10 кГц до 2,6 ГГц. Приемник обладает высокими эксплуатационными характеристи­ками и большим набором сервисных функций. Приемник имеет следующие технические характеристики:

* диапазон частот: 10 кГц-2600 МГц;
* виды модуляции: AM, FM, USB, LSB, CW;
* встроенный декодер DTMF и CTCSS кодов;
* полосы пропускания: 3, 6, 15, 40, 110, 220 кГц.



Рис. 3.1. Сканирующий приемник «AR5000» (а) и сканирующий ЧМ-приёмник «ПИТОН» (б)

**Сканирующий ЧМ-приемник «Питон»** (рис. 3.1,б) предназначен для обнаружения и демодуляции ЧМ сигналов, используемых в вещательных радиопередатчиках, а также для поиска несанкцио­нированных радиопередатчиков с использованием акустозавязки и индикатора уровня принимаемого сигнала. Работает в диапазоне частот 30... 1000МГц, имеет чувствительность не хуже 48 дБм, обеспечивает время сканирования диапазона не более 2 с.



Рис. 3.2. Анализатор электромагнитного поля в диапазоне частот до 2 ГГц «PROTEK 3200» (а) и сканирующий приемник «1СОМIC-R10» (б)

**Protek 3200 (**рис. 3.2,а) является ручным анализатором напря­женности электромагнитного поля и рассчитан на диапазон частот от 100 кГц до 2 060 МГц.

Protek 3200 - это компактный, легкий портативный анализатор, он идеально подходит для тестирования, ввода в действие и обслу­живания оборудования систем телекоммуникаций, сотовых теле­фонных сетей, радиотелефонов, радиостанций в полосе частот пер­сональной радиосвязи, пэйджинговых систем, кабельных и спутниковых систем телевидения, для измерения параметров антенн. Прибор имеет встроенный частотомер. В системе настройки при­бора использована система ФАПЧ для точной настройки и измере­ния частоты. Жидкокристаллический индикатор может отображать уровни сигналов до 160-ти каналов одновременно. В приборе реа­лизована функция автоматического отключения, которая срабаты­вает через 30 мин после последнего нажатия клавиш.

Сканеры японской фирмы ICOM завоевали широкое признание во всем мире. **Модель IC-R10** (рис. 3.2,6) воплотила в себе все со­временные технологические достижения, что позволило добиться вы­сококачественного приема сигналов всех видов модуляции в диапазо­не от коротких волн до СВЧ при сохранении небольших габаритов и массы. Ряд функций впервые реализованы в носимом сканере.

*Основные характеристики сканера*

Широкий диапазон: 0,5 - 1300 МГц с разрешением 100 Гц.

Виды модуляции: SSB (USB, LSB), CW, AM, FM, WFM.

Спектроскоп: работает в реальном времени, ширина полосы обзора ±50 или ±100кГц.

Расширенный набор типов и видов сканирования.

Каждый из 2-х основных типов сканирования разбит на три вида:

* сплошное, диапазонное;
* с автоматической записью частот, по каналам памяти, по видам модуляции:
* по банкам памяти.

Новая функция SIGNAVI позволяет в несколько раз увеличить реальную скорость сканирования. При сканировании в режиме FM используется дополнительный приемный контур, который продол­жает сканирование при нахождении основным приемником сигна­ла, таким образом, основной приемник сканирует «скачками» толь­ко по занятым каналам. Величина скачков составляет до 5 шагов настройки, но не более 100 кГц.

Компьютерный интерфейс. IC-R10 может быть подключен к компьютеру для клонирования или управления. Обмен данными осуществляется в разработанном ICOM формате CI-V через допол­нительный блок СТ-17 и позволяет как считывать данные (частоты, уровень сигнала), так и управлять всеми функциями приемника. Приемник IC-R10 поддерживается большинством управляющих программ.

**Высокоскоростной автоматический поисковый приемник радио­сигналов «Скорпион 2000»** (рис. 3.3,а) является портативным сред­ством радиотехнического контроля, предназначенным для автомати­ческого обнаружения радиосигналов и подавления каналов их прие­ма. Прибор позволяет работать со специальным программным обес­печением для анализа спектров сигналов. Имеет порт RC237 для управления, анализа и сбора информации. Характеризуется чувстви­тельностью 20 мкВ и диапазоном частот 20 - 2000 МГц.



Рис. 3.3. Поисковый приемник радиосигналов «Скорпион 2000» (а) и ска­нирующий приёмник «Yupitera MVT-7100» (б)

**Сканирующий приёмник Yupiteru MVT-7100** (рис. 3.3,б) пред­назначен для оперативного радиоконтроля в широком диапазоне частот и выявления активных радиомикрофонов в помещениях. Оснащенный микропроцессорной системой, приёмник позволяет запоминать до 1000 каналов, что значительно облегчает поиск ин­тересующей частоты. Диапазон рабочих частот 0,1 - 1650 МГц. Виды модуляции WFM, AM, NFM, LSB, USB.

**«Xplorer»** (рис. 3.4,а) является универсальным измерительным приёмником радиоизлучений передающих устройств, расположен­ных в непосредственной близости от точки приема. Но это не толь­ко измеритель конкретной радиочастоты или сканирующий прием­ник с высокой скоростью перестройки. Это также многофункцио­нальный прибор с возможностью обнаружения новых радиоизлу­чений менее чем за 1 с. Прибор определяет и детектирует частоту в «ближней зоне» излучения радиопередающего устройства, где его амплитуда значительно больше остальных источников. В режиме автоматического или ручного захвата частоты возможно запомина­ние и хранение в памяти до 500 частот, причём режим LOCK OUT позволяет исключить из дальнейшего анализа выбранные частоты. Прибор предлагает пользователю 12 режимов работы как для поис­ка и контроля, так и для проведения измерений.

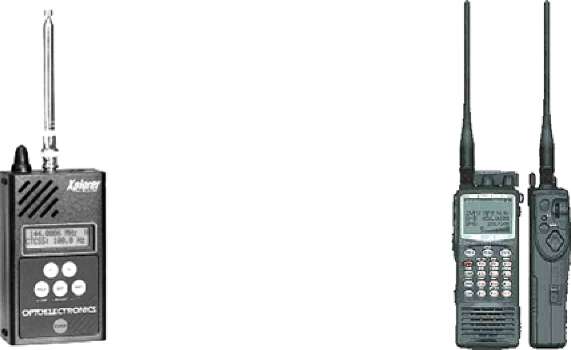


Рис. 3.4. Сканирующий детектор-приемник (интерсептор) «XPLORER» (а) и миниатюрный комплекс аппаратуры для поиска источников радио­излучений «КОМПАС» (б)

«Xplorer» может быть сконфигурирован для работы в стандарте NMEA-0183. При нахождении в режиме NMEA-0183 «Xplorer» может быть подключен к GPS приёмнику для отображения широты и долготы. Широта и долгота могут быть занесены в память при появлении навигационного сигнала. Качество работы с данными подобного типа определяется также наличием соответствующего программного обеспечения.

Обмен данными может производиться между «Xplorer» и GPS- приемником или ПЭВМ с использованием 8-контактного разъёма DATA, расположенного на верхней панели прибора. «Xplorer» мо­жет также передавать данные в ПЭВМ для последующей обработ­ки с использованием программы Xplorer/Scout Download Utility Disk, поставляемой в комплекте с прибором вместе с кабелем RS232 для подключения к последовательному порту ПЭВМ. Последовательный асинхронный интерфейс CI-V даёт возмож­ность соединения с ПЭВМ для дистанционного управления, авто­матического запоминания частот и для записи частот и параметров сигналов из памяти «Xplorer» в ПЭВМ. Причем устройство не требует дополнительного внешнего конвертера RS232C, преобразую­щего уровни ТТЛ-логики к уровням RS-232C, используемым в по­следовательных портах ПЭВМ.

В компьютер может быть загружена следующая информация: частота, количество регистраций, время регистрации, дата, широта, долгота, уровень сигнала, девиация, коды CTCSS/DCS/DTMF.

**Миниатюрный комплекс аппаратуры для поиска источников радиоизлучения в диапазоне частот 20-2000 МГц «КОМПАС»** (рис. 3.4,б) представляет собой доработанный широкодиапазонный приемник AR-8200.

Имеет комплект антенных модулей на диапазоны частот 20-200МГц, 200-500 МГц, 500-2000 МГц, устанавливаемых на ручке со встроенным малошумящим высокодинамичным усилите­лем 12 дБ и магнитным компасом.

Компьютерные сканирующие приемники серии 1000 WR-1000i и WR-ЮООе, показаны на рис. 3.5.

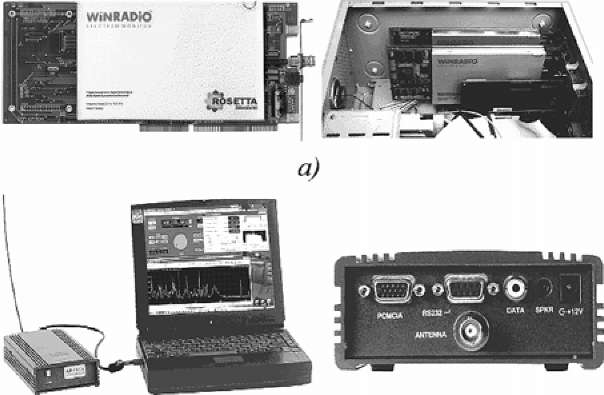


Рис. 3.5. Компьютерные сканирующие приемники серии 1000: а - «WR-1000i»; б - «WR-1000е»

**Приемник WR-1000i.** Эта модель выполнена в виде компьютер­ной карты и устанавливается в стандартный 16-разрядный ISA слот. Каждая установленная в компьютер плата может иметь один из 8 фиксированных адресов, которые устанавливаются на плате приемника с помощью перемычек. Таким образом, допускается ус­тановка нескольких приемников (до 8) в один компьютер по разным адресам. Программное обеспечение допускает независимое управление приемниками (для каждого приемника может быть от­крыто свое окно). Это дает возможность пользователю легко созда­вать свои канальные системы и настраивать каждый приемник для решения определенной задачи. Например; каждый приемник может сканировать определенный частотный диапазон с автоматической записью в файл памяти частоты обнаруженных сигналов.

**Приемники WR-1000e**. Внешние приемники появились совсем недавно и являются логическим продолжением модельного ряда. Они имеют ряд преимуществ, так как могут применяться как в мобильном, так и в стационарном варианте, хотя не обладают возмож­ностями многоканальности. По своим характеристикам и про­граммному обеспечению они не отличаются от внутренних моде­лей аналогичных серий. Питание внешних приемников осуществ­ляется через сетевой адаптер.

Приемники WR-1000еимеют два типа интерфейса и могут подключаться к компьютеру либо через стандартный последова­тельный порт СОМ, либо через порт PCMCIA (в варианте исполь­зования с переносными компьютерами). Для расширения возмож­ности подключения внешних декодеров или для приема и обработ­ки сигналов с помощью специального программного обеспечения, внешние модели имеют выход частотного дискриминатора 'DATA' на задней панели. Внешние приемники имеют внутренний дина­мик, также допускается подключение внешних усилителей или звуковых колонок через разъем 'SPKR'.

На рис. 3.6 показана аппаратура поиска несанкционированных излучений АРК-МК1М. Ее возможности:

* поиск несанкционированных излучений, пеленгование и опре­деление местоположения их источников;
* измерение параметров излучений и запись загрузки диапазона, сигналов и сообщений;
* автоматизированная обработка результатов.



Рис. 3.6. Аппаратура поиска несанкционированных излучений «АРК-МК1М»

Имеет модификации для размещения в автомобиле (АРК-МК1, АРК-МК1М).

В состав аппаратуры входят:

*Основное оборудование*.

1. Антенная система.
2. Дистанционно управляемые цифровые ВЧ тюнеры.
3. Процессор БПФ.
4. Аппаратура радиоперехвата.
5. Общесистемное оборудование.
6. Бортовой компьютер.
7. Пакеты специального программного обеспечения.
8. Система электропитания от сети переменного тока, бортовой сети и аккумуляторов.
9. Зарядное устройство.

*Дополнительное оборудование*.

1. Радиоприемное устройство AR-5000.
2. Аппаратура технического анализа цифровых сигналов.
3. Приемник GPS.
4. Цифровой магнитный компас.
5. Выносная антенная система на мачте.
6. Оборудованный автомобиль.

*При панорамном анализе аппаратура позволяет обнаруживать и измерять параметры излучений, отображать на экране монитора спектральный состав радиосигналов и записывать на жесткий диск данные о выявленных излучениях одновременно со служебной ин­формацией и текущими координатами на момент регистрации*.

Для обеспечения панорамного анализа в аппаратуре использует­ся дискретно-шаговая перестройка приемника с шагом, равным полосе широкополосного тракта. Напряжение с выхода широкополос­ного тракта доработанного приемника обрабатывается процессором БПФ, что обеспечивает параллельный анализ с высокой скоростью перестройки в сочетании с высоким разрешением по частоте.

В основу работы данного класса комплексов положен принцип фазометрического интерферометра с определенными особенностя­ми. При пеленговании используются два широкополосных парал­лельных канала с когерентно связанными гетеродинами. Напряже­ния с выходов каналов, подключенных к выходам опорной антенны и коммутируемой антенной решетки, обрабатываются синхронно процессорами БПФ, что дает возможность устранить влияние мо­дуляции, повысить точность пеленгования в условиях города и обеспечить возможность получения амплитудно-частотнопеленговой панорамы. Сигналы с выходов всех антенн во всем диапазоне обрабатываются совместно.

Для обеспечения технического анализа принимаемый радиосиг­нал представляется совокупностью комплексных отсчетов, что по­зволяет сохранить всю информацию о его амплитудных, фазовых и частотных параметрах при регистрации на жесткий диск и опреде­лить его спектрально-временные параметры в масштабе времени, близком к реальному. Оператору предоставлена возможность широ­кого выбора алгоритмов цифровой обработки и фильтрации.

При радиоконтроле каналов с речевыми передачами аппаратура обеспечивает поиск и сканирующий прием с заданным шагом с за­писью уплотненного сигнала одновременно со служебными пара­метрами на жесткий диск и возможностью последующего воспро­изведения. Речевой сигнал благодаря использованию специальных алгоритмов цифровой обработки представляется в виде совокупно­сти отсчетов со скоростью 1.7 кБ/с без ухудшения разборчивости.

1. **Анализаторы спектра, радиочастотомеры**

Кроме сканирующих приемников для радиотехнической раз­ведки могут применяться и ряд других устройств, таких как анали­заторы спектра, радиочастотомеры, интерсепторы, селективные микро вольтметры.

Характерной особенностью большинства таких устройств яв­ляются их портативное исполнение и высокая чувствительность как следствие достижений в области радиоэлектроники.

*Анализаторы спектра позволяют анализировать спектр приня­тых сигналов в заданном диапазоне частот*.

*Радиотестеры измеряют параметры сигналов, работают со все­ми типами модуляции*.

*Радиочастотомеры предназначены для измерения частоты ис­точника радиосигнала*.

*Для перехвата разговоров, ведущихся по каналам радиосвязи в ближней зоне, могут использоваться интерсепторы*. *Интерсептор автоматически настраивается на частоту наиболее мощного сигна­ла и осуществляет его детектирование*.

Примеры технической реализации перечисленных устройств приведены ниже.

**Искатель радиопомех П4-14** предназначен для:

* измерения уровня полезных сигналов и радиопомех;
* измерения радиопомех;
* радиоконтроля и радиоразведки;
* анализа электромагнитной обстановки в комплексе с внешни­ми измерительными антеннами.

**Портативный частотомер MICRO-COUNTER** (рис. 3.7,а) обла­дает высокой чувствительностью и дает возможность решать ши­рокий круг задач для измерения и тестирования радиопередающих устройств. По своим функциям частотомер MICRO-COUNTER не отличается от функций ранее рассмотренных частотомеров.



Рис. 3.7. Портативный частотомер «MICRO-COUNTER» (а) и частотомер OPTOELECTRONICS «CUB» (б)

Частотомер имеет диапазон измерения 10... 1200 МГц, цифровой фильтр, функцию автозахвата, ЖКИ-дисплей, с разрешением до 10 Гц, а также память для хранения трех последних результатов измерений.

Частотомер содержит 3 режима измерения, непрерывный, ре­жим автозахвата и режим автозахвата с автоматической записью частоты в память. При использовании со штатной антенной ТМС100, частотомер позволяет измерять частоту источников ра­диоизлучения мощностью 5 Вт с расстояния до 30 м.

**Частотомер OPTOELECTRONICS «CUB»** (рис. 3.7,б) предна­значен для измерения частоты радиосигналов и поиска подслуши­вающих устройств. Является усовершенствованной версией модели 3300. По сравнению с ней имеет в два раза большее время работы от батарей, более скоростной вход, большее количество переклю­чаемых скоростей счета. Прибор имеет цифровой фильтр, функцию автозахвата, девятизначный дисплей.

Частотомеры ROGER RFM-12 (13, 21, 22, 31, 32)» (рис. 3.8,а) предназначены для поиска радиопередатчиков («жучков»).

Благодаря довольно высокой чувствительности (около 2 мВ) дальность обнаружения может варьироваться от 20 см до несколь­ких метров. Эти легкие портативные устройства имеют малые раз­меры (100x68x31 мм) и питаются от встроенных аккумуляторов, энергии которых хватает на 6 ч работы. Они имеют прочный кор­пус черного цвета из анодированноого алюминия и большой ЖК- индикатор с подсветкой и отображением режимов.

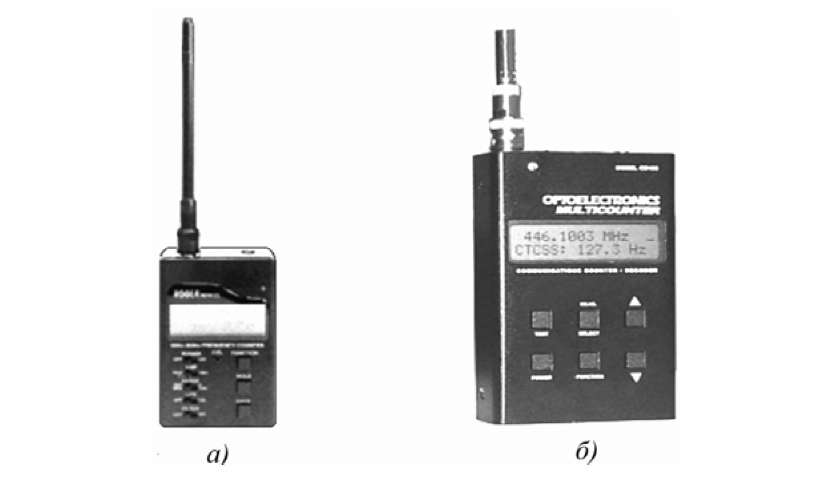


Рис. 3.8. Частотомеры ROGER RFM-12 (а) и CD100 (б)

Частотомеры ROGER отличает высокая точность и широкий диапазон частот (до 3000 МГц). Время измерения - переключаемое от 0,1 до 4 с. Имеет­ся функция удержания показаний индикатора HOLD. Функция фильтра позволяет устранять влияние случайных помех. Возможен вывод обратной к частоте величины периода. Большой диапазон входных напряжений (до 1 В при входном сопротивлении 50 Ом и до 100 В при 1 мОм) позволяет работать при различной величине сигнала и на различном удалении от источника. Все модели имеют индикацию уровня сигнала, необходимую при локализации источ­ника сигнала. После измерения частоты приборы могут передавать ее на приемник (RFM-31, RFM-32).

**Портативный частотомер CD100** (рис. 3.8,б) является много­функциональным прибором со следующими возможностями:

* измерение частоты в диапазоне от 10 до 1000 МГц;
* декодер сигналов CTCSS, DTMF, LTR и DCS;
* 100 ячеек памяти для хранения результатов измерений;
* перестройка сканирующих приемников на частоту захваченно­го сигнала (режим 'REACTION TUNE').
* возможность подключения к компьютеру для сохранения на­копленной информации.

**Частотомер 3000А Plus** (рис. 3.9) сочетает в себе вычислитель­ные возможности внутреннего микропроцессора с высокоскорост­ным счетчиком на базе микросхемы ОЕЮ, специально разработан­ной для этого фирмой Optoelectronics, для достижения характери­стик, которыми не обладает ни один портативный частотомер. Цифровой фильтр на базе микропроцессора позволяет не фиксиро­вать некогерентные фоновые сигналы, что практически сводит на нет вероятность ложных срабатываний в режиме цифрового авто­захвата измерений.

Входные усилители перекрывают диапазон от 10 Гц до 3000 МГц, а максимальная точность измерения составляет 1 Гц. Такие харак­теристики позволяют применять 3000А Plus практически в любых областях радиотехники, где необходимо быстро и с высокой точно­стью проводить измерения частот.



Рис. 3.9. Портативный многофункциональный частотомер 3000А Plus

Для достижения максимальной чувствительности, частотомер имеет три входных усилителя и два входа для подключения антенн. Измеряться могут как частоты источников радиоизлучения, так и частоты в электрических схемах при контактном подключении с помощью щупов. При контактных подключениях измеряться могут не только частоты, но и временные характеристики сигналов (в том числе и длительность одиночных импульсов). В этом случае ис­пользуются усилители с входным сопротивлением 1 МОм.

Частотомер 3000А Plus имеет прямой интерфейс RS-232C для подключения к последовательному порту компьютеру. Все данные в режиме непрерывного измерения или цифрового автозахвата па­раллельно, с отображением на дисплее, могут быть введены в ком­пьютер. Частотомер имеет простую систему команд, которая по­зволяет пользователю легко разработать собственное программное обеспечение для ввода измеряемых частот через последовательный порт или получать данные в терминальном режиме

Соединение с компьютером в режиме работы с цифровым фильтром может находить применение в области радиоконтроля и радиобезопасности. Частотомер может автоматически фиксировать любые (даже самые короткие по длительности) сигналы радиопе­редатчиков в «ближней зоне». Это могут быть как радиостанции, так и маломощные источники, такие как радиомикрофоны и теле­фонные микропередатчики.

Усилители с входным сопротивлением 1 МОм позволяют ис­пользовать 3000А Plus для измерения частот и временных характе­ристик сигналов в электронных схемах. Измеряться могут как пе­риодические, так и импульсные сигналы напряжением до 50 В.

**Многофункциональный универсальный частотомер 8040** (рис. 3.10) является самым многофункциональным прибором для измерения частотных и временных характеристик сигналов из всей серии частотомеров, производимых фирмой Optoelectronis.



Рис. 3.10. Многофункциональный универсальный частотомер 8040

Прибор выполнен в настольном варианте, но благодаря внут­ренним Ni-Cd аккумуляторам, он одинаково хорошо подходит для эксплуатации, как в полевых, так и в стационарных условиях. 8040 вобрал в себя все самые последние достижения и технические ре­шения инженеров фирмы Optoelectronics в вопросах разработки и производства приборов для контроля и измерения частотных и временных характеристик сигналов. Частотомер 8040 имеет ту же чувствительность, частотные характеристики и разрешение ЖКИ- дисплея, что и модель частотомера 3000А+. В нем реализованы за­патентованный цифровой фильтр, функция автозахвата сигнала и 16-сегментный индикатор уровня сигнала. Однако, у этой модели значительно более широкие возможности по обработке входных сигналов. Частотомер имеет полный набор регулировок входных сигналов, установку необходимой полярности, настройки уровня переключения, фильтр низких частот и аттенюатор. Это дает при­бору большую гибкость по измерению частот и временных харак­теристик сигналов, чем любой другой частотомер Optoelectronics.

Частотомер 8040 имеет четыре переключаемых входных усили­теля с низкоомным и высокоомным входным импедансом со свя­зью по постоянному и переменному току. Низкоомные усилители применяются при измерении частот радиосигналов. Входное со­противление 50 Ом дает возможность согласовывать частотомер по входу с большинством применяемых антенн и фидеров. Высокоом- ные входы позволяют с успехом использовать частотомер для из­мерения частот и временных характеристик сигналов при настрой­ке и регулировке любых электронных приборов.

**Ручной измеритель частоты РИЧ-3** (рис. 3.11, а) предназначен для определения частоты и интенсивности источников радиоизлучений, как в процессе проведения поисковых работ, так и в процес­се наладки и проверки малогабаритных радиопередающих моду­лей, так как частота и интенсивность (мощность) наиболее важные параметры ВЧ сигнала.

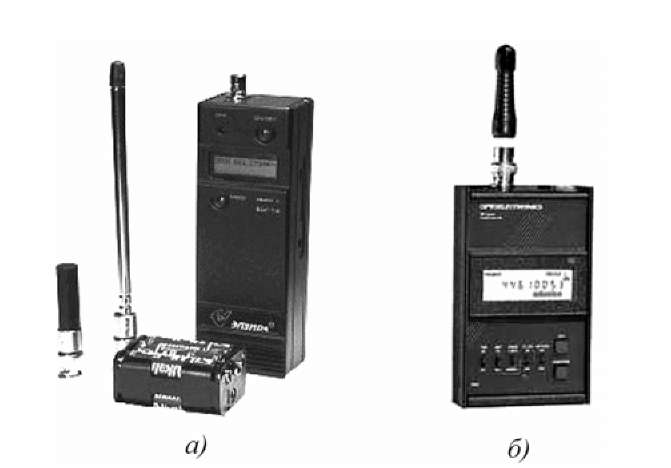


Рис. 3.11. Ручной измеритель частоты «РИЧ-3» (а) и поисковое устройство «РТ- 025» (б)

Его предшественник, прибор РИЧ-2, выпускаемый фирмой «ЭЛВИРА», уже длительное время пользуется устойчивым спро­сом на рынке систем безопасности. Это объясняется, прежде всего, его достаточно высокими потребительскими качествами, умерен­ной ценой и постоянной работой специалистов фирмы над повы­шением его тактико-технических характеристик.

К началу 1999 г. фирмой был накоплен богатый материал, обобщающий опыт длительной эксплуатации РИЧ-2, анализ кото­рого с учётом современных тенденций развития рынка спецтехни­ки показал своевременность разработки нового ручного измерителя частоты.

Новый прибор не только вобрал в себя лучшие черты своего предшественника, но и существенно расширил его функциональ­ные возможности.

В РИЧ-3 реализованы следующие новые режимы работы:

* введена функция определения момента появления сигнала (с измерением частоты) радиопередатчика, работающего в стандар­те GSM-900;
* введена функция автоматической настройки (через порт RS- 232) приёмников типа AOR3000 или AOR8OOO на частоту сигнала, зафиксированного прибором РИЧ-3;
* введена функция запоминания (в энергонезависимой памяти прибора) значения частоты сигнала, превышающего фон или за­данный порог, а также даты, времени начала и продолжительности этого превышения (до 32 записей).

Кроме того, улучшены следующие характеристики прибора РИЧ-2:

* повышена чувствительность в диапазоне рабочих частот;
* повышена равномерность шкалы при индикации уровня ВЧ сигнала;
* повышена акустическая чувствительность в режиме «акустозавязки»;
* форма представление графической информации на индикато­ре.

**Поисковое устройство РТ-025** (рис. 3.11,б) *предназначено для обнаружения и локализации источников радиоизлучения и опреде­ления их рабочей частоты*.

От приборов аналогичного функционального применения поис­ковое устройство РТ-025 отличается:

* встроенным измерителем частоты источника радиоизлучения;
* наличием режекторных фильтров повышающих реальную чув­ствительность прибора в сложной помеховой обстановке.

Генератор переменного тока и режим «акустической завязки» позволяют определять направление поиска источников радиоизлу­чения и идентифицировать радиопередающие устройства.

**Частотомер OPTOELECTRONICS «М1»** (рис. 3.12,а) предна­значен для измерения частот радиосигналов, а также для обнару­жения и локализации радиопередатчиков, работающих в диапазо­нах частот от 10 Гц до 2.8 ГГц. Встроенный микроконтроллер обеспечивает цифровую фильтрацию, цифровой автозахват, сохра­нение и последовательный вывод данных. Подключение конверто­ра модели СХ 12 RS-232 позволяет протоколировать данные на PC.



Рис. 3.12. Частотомер OPTOELECTRONICS «М1» (а) и частотомер STARTEK «АТН-30» (б)

Основные характеристики:

* максимальный входной сигнал +15 дБм (50 мВт);
* дисплей жидкокристаллический, 10-разрядный;
* индикация частоты, разряда батарей, режимов работы, уровня сигнала (16 сегментов, по 3 дБ);
* габариты 125x70x35 мм.

**Ручной частотомер STARTEK АТН-30** (рис. 3.12,б) представля­ет собой счётчик частоты карманного размера с 10-сегментной шкалой уровня сигнала и цифровой индикацией частоты. Устрой­ство имеет режим «удержания» частоты, индикацию разряда встро­енных аккумуляторов, режим быстрого и медленного счёта часто­ты, характеризующий точность измерений. Диапазон рабочих час­тот 1 - 2800 МГц.

**Анализатор спектра НР8591Е** (рис. 3.13,а) предназначен для проведения специальных исследований электронно-вычислитель­ной техники и слаботочного оборудования на наличие и уровень побочных электромагнитных излучений и наводок; для контроля радиоэлектронной обстановки в проверяемых помещениях с воз­можностью накопления информации об объекте и сравнительного анализа с уже имеющимися, полученными ранее, данными; для проверки эффективности принимаемых мер по защите информации при проведении пуско-наладочных работ и функционировании технических средств обработки информации. Имеется возможность управления работой анализатора с использованием ПЭВМ и СПО.



Рис. 3.13. Анализаторы спектра «НР8591Е НР» (а) и «ESA-L1500A» (б)

Анализатор имеет интерфейс HP-IB, интерфейс RS-232 для обес­печения взаимодействия с ПЭВМ, обеспечивает возможность оценки электромагнитной совместимости радиоэлектронных средств, локали­зации излучения, возможность гальванического контроля сетей пита­ния на наличие опасного сигнала. Имеется возможность управления работой анализатора с использованием ПЭВМ и СПО.

**Анализатор спектра HP ESA-L1500A** (рис. 3.13,б) предназначен для проведения специальных исследований электронно-вычисли­тельной техники и слаботочного оборудования на наличие и уро­вень побочных электромагнитных излучений и наводок; для кон­троля радиоэлектронной обстановки в проверяемых помещениях с возможностью накопления информации об объекте и сравнитель­ного анализа с уже имеющимися, полученными ранее, данными; для инженерных исследований изымаемых органами МВД техни­ческих средств (радиостанций, радиомикрофонов, систем съема информации и т.д.); для проверки эффективности принимаемых мер по защите информации при проведении пуско-наладочных работ и функционировании технических средств обработки информации. Имеется возможность управления работой анализатора с использо­ванием ПЭВМ и СПО. Диапазон рабочих частот - 9... 1,5 ГГц.

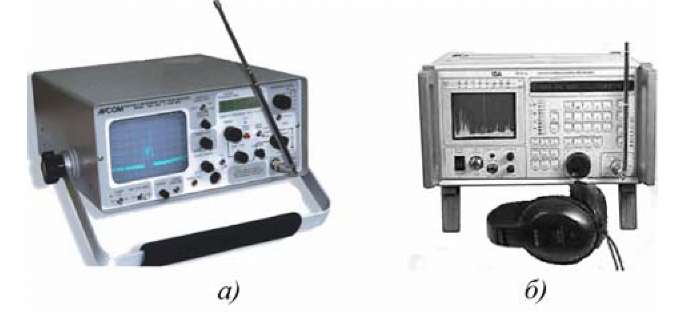
**Ализатор спектра PSA-65C** (рис. 3.14,а) является последней разработкой анализаторов спектра серии 65. Отличительной особенностью прибора является его универсальность. PSA-65C с успехом может применяться для измерения спектральных характеристик сигналов в лабораторных и полевых условиях, а также использоваться как высокоэффективный прибор при проведении поисковых мероприятий по выявлению каналов утечки информации. Кроме визуального анализа спектра, PSA-65C имеет возможность детектировать и прослушивать сигналы с амплитудной и частотной модуляций.

Рис. 3.14. Анализаторы спектра «PSA-65C» (а) и «ECR-2» (б)

В отличие от предшествующих моделей этой серии, PSA-65C имеет ряд принципиальных отличий. Функция 'Digital Frequency Lock', позволяет осуществлять захват и удержание частоты (полез­ная функция при акустическом контроле фиксированных частот).

Применение нового микропроцессора для управления разверт­кой позволило не только производить настройку на определенную частоту, но и с высокой точностью устанавливать границы частот­ного диапазона, отображаемого спектроанализатором.

При применении дополнительного полосового фильтра, анализ спектра может проводиться в полосе от 200 кГц до 1250 МГц с раз­решением по частоте 10 кГц.

**ECR-2** (рис. 3.14,б) представляет собой высокоточный анализа­тор спектра с функциями обнаружения подслушивающих уст­ройств. Прибор позволяет обнаруживать передатчики подслуши­вающих устройств с низкой мощностью, а также передатчики с не­стандартной модуляцией. Простота управления позволяет эксплуа­тировать ECR-2 персоналом без специальной подготовки.

Узкополосный и широкополосный ЧМ и AM демодуляторы по­зволяют быстро идентифицировать подозрительный сигнал.

Прослушивание осуществляется на встроенный динамик или наушники. ECR-2 имеет видеовыход для просмотра TV сигналов на мониторе.

Надежная работа в зоне мощных сигналов ISA гарантирует на­дежную работу прибора даже в условиях мощных сигналов стан­ций крупных городов. На ECR-2 не действуют мощные локальные сигналы, вызывающие перегрузки входных каскадов. Обладая высокой чувствительностью, ECR-2 позволяет обна­руживать передатчики на площади в несколько тысяч квадратных футов. Это позволяет оператору эффективно и качественно прово­дить поиск. Спектрограмма радиочастотного спектра может быть распечатана на встроенном принтере, и использоваться в дальнейшем для сравнения при следующих проверках. Упаковка ECR-2 в кейсе позволяет использовать прибор для работы в полевых усло­виях. Диапазон рабочих частот находится в пределах от 10 кГц до 1000 МГц.

Питание прибора осуществляется от сети 110/220 В, встроенной батареи 12 В, внешнего источника 12 В (бортовая сеть автомобиля).

**Литература**

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.
3. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И.К.Корнеев, Е.А. Степанов.- М.:Проспект,2011.-336 с.
4. Зегжда Д.П., Ивашко A.M. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2009.

**Лекция № 15**

**КОНТРОЛЬ И ПРОСЛУШИВАНИЕ ТЕЛЕФОННЫХ** **КАНАЛОВ СВЯЗИ**

План:

1. Прослушивание телефонных переговоров

2. Непосредственное подключение к телефонной линии

3. Подкуп персонала АТС

4. Прослушивание через электромагнитный звонок

5. Прослушивание помещений через микрофон телефонного аппарата

6. «Атаки» на компьютеризованные телефонные системы

**1. Прослушивание телефонных переговоров**

Одним из основных способов несанкционированного доступа к информации частного и коммерческого характера является прослу­шивание телефонных переговоров. Для прослушивания телефонных переговоров используются следующие способы подключения:

* параллельное подключение к телефонной линии (телефонные закладки труднее обнаруживаются, но требуют внешнего источника питания).
* последовательное включение телефонных закладок в разрыв провода телефонной линии (питание телефонные закладки осуществляется от телефонной линии и на передачу она выходит с момента подъема телефонной трубки абонементом).

*Подключение телефонного радиоретранслятора может осуще­ствляться как непосредственно к телефонному аппарату, так и к любому участку линии от телефона абонента до АТС*.

Существуют телефонные радиоретрансляторы, позволяющие прослушивать помещение через микрофон лежащей трубки. Для этого на один провод телефонной линии подключается генератор ВЧ колебаний, а к другому - амплитудный детектор с усилителем. ВЧ колебания проходят через микро­фон или элементы телефонного аппарата, обладающие «микрофон­ным эффектом», и модулируются акустическими сигналами про­слушиваемого помещения. Модулированный ВЧ сигнал демодулируется амплитудным детектором и после усиления прослушивается или записывается.

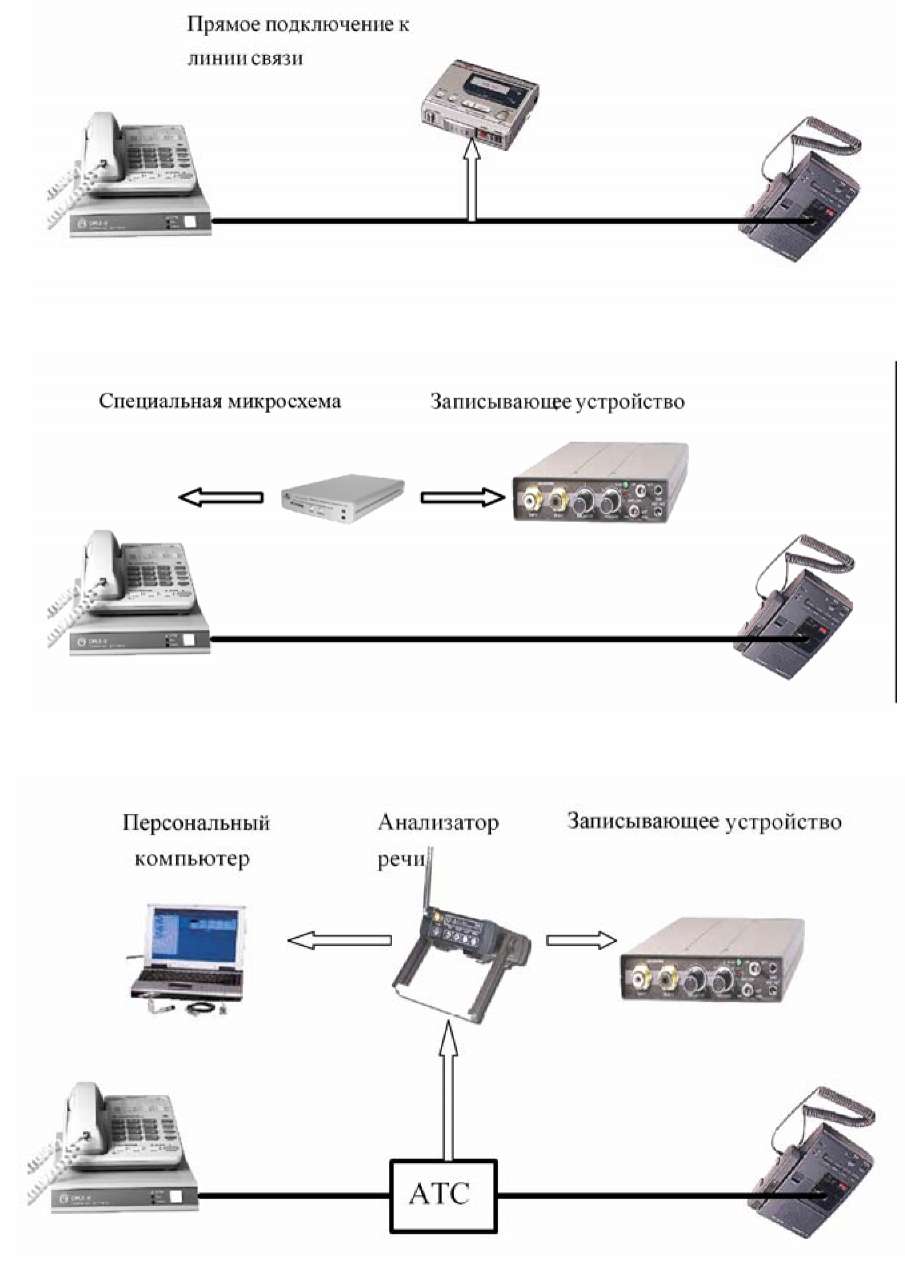
*Дальность действия такой системы из-за затухания ВЧ сигнала в двухпроводной, линии не превышает нескольких десятков мет­ров.*

Имеются системы прослушивания телефонных разговоров, которые не требуют непосредственного электронного соединения с телефонной линией. Эти *системы основаны на индуктивном спо­собе съема информации при помощи специальных катушек*. Они сложны и громоздки, поскольку содержат несколько каскадов уси­ления слабого низкочастотного сигнала и обязательный внешний источник питания. Поэтому такие системы не нашли широкого практического применения.

Для приема информации от телефонных радиотрансляторов применяют такие же приемники, как в акустических устройствах съема информации по радиоканалу.

Существуют системы перехвата факсовой и модемной связи, которые при использовании ПК со специальным ПО позволяют получить расшифровку информации. Однако такие системы очень дорогие и пока не нашли широкого применения в нашей стране.

Способы, которыми может вестись прослушивание телефонных линий и какая при этом используется аппаратура, наглядно пред­ставлены на рисунках.

Схемы возможных вариантов подключения к телефонной линии без использования радиоканала

2. **Непосредственное подключение к телефонной линии** – наибо­лее простой и надежный способ получения информации. В про­стейшем случае применяется трубка ремонтника-телефониста, подключаемая к линии в распределительной коробке, где произво­дится разводка кабелей. Чаще всего это почерк «специалистов» нижнего звена уголовного мира (верхнее звено оснащено аппара­турой не хуже государственных секретных служб). Применение аппаратуры подслушивания с низкоомным входным сопротивлением можно достаточно быстро обнаружить. Если слышны щелчки в линии или перепады громкости, т. е. вероятность того, что имеет место по­пытка прослушать не совсем профессиональным способом.

Схемы возможных вариантов подключения к телефонной линии с использованием радиоканала

****

**3. Подкуп персонала АТС**

Подкуп обслуживающего персонала на АТС - весьма распро­страненный способ добывания конфиденциальной информации. В особенности это касается небольших городов, где до сих пор используются старые декадно-шаговые АТС. Чаще всего таким спо­собом могут воспользоваться преступные группы либо конкури­рующие фирмы.

**4. Прослушивание через электромагнитный звонок**

Телефонные аппараты, в которых в качестве вызывного устрой­ства используется электромагнитный звонок, пока еще широко распространены в нашей стране. Звонок обладает микрофонным эффектом, т.е., если на электромагнитный звонок действуют звуко­вые волны, он начнет вырабатывать соответствующим образом мо­дулированный ток. Амплитуда его достаточна для дальнейшей об­работки. Эксперименты показали, что амплитуда ЭДС, наводимая в линии, для некоторых типов телефонных аппаратов может дости­гать нескольких милливольт. Корпус аппарата является дополни­тельным резонирующим устройством.

**5. Прослушивание помещений через микрофон телефонного аппарата**

В этом случае телефонная линия используется не только для передачи телефонных сообщений, но и для прослушивания поме­щения. Микрофон является частью электронной схемы телефонно­го аппарата: он либо соединен с линией (через отдельные элементы схемы) при разговоре, либо отключен от нее, когда телефонный аппарат находится в ожидании вызова (трубка находится на аппа­рате). На первый взгляд, когда трубка лежит на аппарате, нет ника­кой возможности использовать микрофон в качестве источника съема информации. На самом деле это не так.

Рассмотрим способ, который не является эквивалентом непо­средственного подключения к линии. Он основан на высокочастот­ной накачке. Для его реализации к одному из проводов телефонной линии подключают относительно какой-то общей массы (труб ка­нализации, отопления и т.д.) регулируемый в диапазоне 50 - 300 кГц высокочастотный генератор. Путем плавной перестройки находят частоту его резонанса с телефоном и оставляют работать на этой частоте. При положенной на рычаг телефонной трубке внешние высокочастотные колебания через конструктивные элементы аппа­рата и паразитные связи проникают в его схему и активно модули­руются микрофоном, реагирующим на звуки в комнате. Несущий информацию сигнал через провод телефонной линии поступает на пост перехвата, располагающийся в пределах нескольких десятков метров от контролируемого аппарата, обрабатывается и регистри­руется.

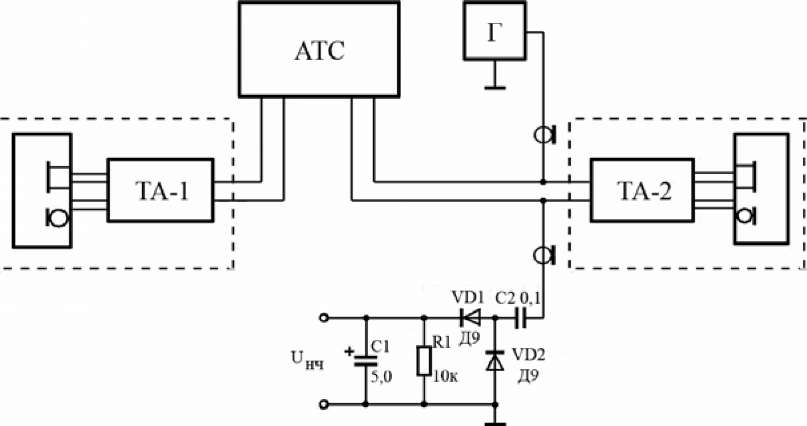
На рис. приведена схема прослушивания помещения спосо­бом, называемым высокочастотным навязыванием. Этот способ ана­логичен способу высокочастотной накачки и состоит в следующем.

Рис. Прослушивание через микрофон телефонного аппарата

На один из проводов телефонной линии, идущий от АТС к те­лефонному аппарату ТА-2, подаются колебания частотой 150 кГц и выше от генератора Г. К другому проводу линии подключается де­тектор, выполненный на элементах CI, С2, VD1, VD2 и R1. Корпус передатчика (генератор Г) и приемника (детектор) соединены меж­ду собой или с общей землей, например с водопроводной трубой.

Высокочастотные колебания через элементы схемы телефонно­го аппарата ТА-2 поступают на микрофон (даже если трубка ТА-2 опущена) и модулируются речью. Детектор приемника выделяет речевую информацию, которая усиливается до необходимого уров­ня и обрабатывается. Вследствие существенного затухания ВЧ сиг­нала в двухпроводной линии, дальность съема информации таким методом не превышает нескольких сотен метров.

Для защиты телефонного аппарата от снятия информации та­ким способом достаточно параллельно микрофону подключить конденсатор емкостью 0,01 - 0,05 мкФ. При этом последний будет шунтировать микрофон по высокой частоте и глубина модуляции ВЧ колебаний уменьшится более чем в 10 000 раз, что делает даль­нейшую демодуляцию сигнала практически невозможной.

Следует отметить, что высокочастотная накачка позволяет снимать информацию также с бытовой и специальной аппаратуры (радиоточек, электрических часов, противопожарной сигнализа­ции), при наличии у нее проводного выхода из помещения. Недостаток этого метода состоит в том, что его случайно может обнаружить всякий, кто позвонит по тому же номеру, а также необъ­яснимая занятость контролируемой линии для других абонентов.

Еще один способ просушивания *реализуется установкой в ап­парате устройства, блокирующего выключатель трубки после ее снятия*. Техника использования этого метода такова: при установ­ленном в телефоне блокирующем устройстве злоумышленник зво­нит по номеру контролируемого телефона. Владелец телефона поднимает трубку, но услышав молчание с вызывающей стороны, кладет трубку на рычаг. Сработавшее при этом устройство блоки­рует отключение трубки до тех пор, пока слушающий на противо­положном конце не положит на рычаг и свою трубку.

Более скрытым методом является установка в аппарат устрой­ства, активизируемого специальным кодом через любой внешний телефон. В упрощенном варианте в схему телефонного аппарата вводят небольшое резонансное реле, настроенное на определенную частоту. Подслушивающий набирает номер контролируемого ап­парата с любого другого телефона, в том числе и междугородного, и подносит к своей трубке портативный звукоизлучатель (бипер), тональный сигнал которого соответствует частоте срабатывания реле. Реле быстро отключает звонок аппарата и переводит трубку во включенное состояние, позволяя звонившему прослушивать все разговоры в комнате. Устройство работает независимо от самого телефона и, как правило, требует дополнительной телефонной ли­нии. Такие устройства широко продаются на Западе для домашнего мониторинга.

Описанная схема имеет несколько модификаций, в частности, усложненный код (чтобы затруднить случайное обнаружение факта перехвата), использование специального усилителя и микрофона (для улучшения качества сигнала).

Следует подчеркнуть, что иногда звонок может кратковременно сработать до того, как резонансное реле его отключит. Такой со­кращенный звонок может стать возможным признаком того, что телефон используется для подслушивания. Дополнительным на­стораживающим моментом является занятость рабочей линии в те периоды времени, когда она должна быть свободной. Самым скрытым является распространенный сейчас на Западе вариант, когда устройство, блокирующее выключатель телефонной трубки, подсоединяется где-нибудь на линии одновременно к контролируемому телефону и специально арендуемому телефону, пара которого находится в том же телефонном кабеле. Злоумышленник звонит по номеру арендованного им телефона, активизируя при этом устройство, которое переводит трубку контролируемого те­лефона во включенное состояние и автоматически соединяет кон­тролируемую линию с арендуемой. Такой метод обладает большей скрытностью и позволяет прослушивать разговоры в комнате прак­тически из любого места в мире.

**6. «Атаки» на компьютеризованные телефонные** **системы**

В последнее время объектом повышенного внимания злоумыш­ленников стали компьютеризованные телефонные системы (АТС и офисные мини-АТС, управляемые компьютером). В таких системах все телефонные соединения осуществляются компьютером в соот­ветствии с заложенной в него программой. В общем виде «атака» на такую телефонную систему состоит в том, что злоумышленни­ки, используя хорошо отработанные способы, дистанционно про­никают в локальную компьютерную систему или в сам управляю­щий компьютер и изменяют программу, по которой он выполняет телефонные соединения или предоставляет доступ абонентов в систему. В результате они получают возможность перехватывать со своего телефона все виды информационного обмена, ведущегося в контролируемой системе. При этом обнаружить факт такого пе­рехвата чрезвычайно сложно.

**Литература**

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.
3. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И.К.Корнеев, Е.А. Степанов.- М.:Проспект,2011.-336 с.
4. Зегжда Д.П., Ивашко A.M. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2009.

**Лекции № 16-17**

**ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ**

План:

1. Классификация объектов охраны

2. Особенности задач охраны различных типов объектов

3. Общие принципы обеспечения безопасности объектов

4. Некоторые особенности построения периметровой охраны

5. Функциональные зоны охраны

6. Оптимизация построения системы охранной безопасности

7. Контроль доступа к защищаемым помещениям

8. Охрана оборудования и перемещаемых носителей информации

**1. Классификация объектов охраны**

По степени важности, следовательно, и необходимой надеж­ности охраны объекты принято разделять на категории. Например: *особо важные (ОВ), важные, общего назначения* и т.п.

*Последствия действий нарушителей оцениваются по размеру нанесенного ущерба объекту, окружающей среде, общественным структурам*.

Воздействие злоумышленников на **ОВ объекты** (некоторые во­енные, ядерно-опасные, объекты топливно-энергетического ком­плекса, химические и другие предприятия с вредным производст­вом) может привести к непоправимым последствиям, связанным с нанесением вреда здоровью и жизни людей, экологии и т.д. Такой ущерб не всегда поддается оценке в денежном выражении.

Действия нарушителей на объектах промышленно-коммерческого назначения (ПК) могут привести к ущербу, который в боль­шинстве случаев оценивается в денежном эквиваленте.

**2. Особенности задач охраны различных типов объектов**

В случае несанкционированного проникновения злоумышлен­ников на ОВ объекты наиболее вероятны диверсионные акты, направленные на уничтожение объекта, нарушение его нормального функциони­рования, а также действия, связанные с хищением ядерных мате­риалов, оружия, секретной информации. Величина ущерба может возрастать со временем (например, увеличение числа пораженных лиц в результате взрыва на ядерно-опасном объекте).

При несанкционированном проникновении на ПК объекты наи­более реальны действия, имеющие корыстные цели, и только в от­дельных случаях – диверсионные, причем объем ущерба снижается по истечении времени.

Действия сил охраны на ОВ и других объектах должны иметь различный характер. *На ОВ объектах зло­умышленник в обязательном порядке должен быть нейтрализован до того, как он выполнит намеченные действия*.

*На ПК объектах нарушитель* (если это не связано с диверсией или актом терроризма) может быть нейтрализован как до, так и не­посредственно после совершения акции.

Особенности задач системы охраны объекта определяются так­же исходным положением нарушителя. На *ОВ объектах наруши­тель (внешний) находится за территорией объекта, на котором не­допустимо присутствие посторонних лиц*. На ПК объектах потен­циальный нарушитель в принципе имеет право находиться на ох­раняемой территории и не может быть выявлен как злоумышлен­ник, пока не совершит противоправные действия.

*В связи с общей тенденцией роста объема конфиденциальных сведений в любой организации особую актуальность приобретает задача выработки правил обеспечения защиты информации, созда­ние надежной охранной системы предприятия*. Возросла и необхо­димость обеспечения безопасности данных на физическом уровне.

**К техническим средствам защиты информации (ЗИ) относят механические, электронно-механические, электромеханические, оптические, акустические, лазерные, радио-, радиолокационные и другие устройства, системы и сооружения, предназначенные для создания физических препятствий на пути к защищаемой инфор­мации и способные выполнять самостоятельно или в комплексе с другими средствами функции защиты информации**.

К моменту возникновения проблемы защиты информации фи­зические средства защиты уже существовали, так как они в прин­ципе не отличаются от давно используемых средств охраны таких объектов как банки, музеи, магазины и т.п. Однако для защиты информации и объектов, где она хранится и обрабатывается, ис­пользуются более сложные и совершенные методы средства.

*Физические средства представляют собой первую линию защи­ты информации* и элементов вычислительных систем, и поэтому обеспечение физической целостности таких систем и их устройств является непременным условием защищенности информации. Развитию и внедрению физических средств защиты уделяется большое внимание в ведущих зарубежных странах, а в последнее время и в России стали уделять этому внимание.

*Основные задачи, решаемые физическими средствами:*

1. Охрана территории.
2. Охрана оборудования и перемещаемых носителей информа­ции.
3. Охрана внутренних помещений и наблюдение за ними.
4. Осуществление контролируемого доступа в контролируемые зоны.
5. Нейтрализация наводок и излучений.
6. Препятствия визуальному наблюдению.
7. Противопожарная защита.
8. Блокирование действий злоумышленника.

Центры электронной обработки информации на предприятиях, в банках, коммерческих организациях должны располагаться вда­ли от промышленных предприятий, имеющих мощные источники электромагнитных полей, крупных общественных центров. Терри­тория по возможности должна быть окружена забором, а периметр здания иметь просматриваемую контролируемую зону. Наблюде­ние за контролируемой зоной может осуществляться различными телевизионными, радиолокационными, лазерными, оптическими, акустическими, кабельными и другими системами, а также систе­мами различных датчиков, которые соединяются с центральным пультом, откуда подаются сигналы тревоги. Назначение заборов, решеток, ставней, экранов, специального остекления очевидно.

В помещении центрального пульта могут размещаться монито­ры, наглядные схемы охраняемой территории с идентификацией места нарушения, а также ЭВМ, предназначенная для обработки сиг­налов от различных устройств управления, связанных с датчиками и другими системами охранной сигнализации, и других целей. ЭВМ поочередно опрашивает периферийные устройства управления.

**3. Общие принципы обеспечения безопасности** **объектов**

В общем случае *обеспечение безопасности объекта* базируется на двух принципах:

* определение и оценка угроз объекту;
* разработка и реализация адекватных мер защиты.

Меры предусматривают:

* тотальный контроль несанкционированного проникновения на территорию объекта, в здания и помещения;
* ограничение и контроль доступа людей в «закрытые» здания и помещения с возможностью документирования результатов кон­троля;
* обнаружение злоумышленника на самых ранних этапах его продвижения к цели акции;
* оценку ситуации;
* создание на пути продвижения нарушителя физических пре­пятствий, обеспечивающих задержку, необходимую силам охраны для его перехвата;
* принятие немедленных действий по развертыванию сил охра­ны и пресечению действий злоумышленников;
* видеодокументирование действий персонала на особо ответст­венных участках объекта.

Значительная роль в обеспечении реализации отмеченных мер отводится периметровым системам охраны.

**4. Некоторые особенности построения периметровой охраны**

**Периметр** - **первая линия защиты**

Современные электронные системы охраны весьма разнообраз­ны и в целом достаточно эффективны. Однако большинство из них имеют общий недостаток: *они не всегда могут достоверно обеспе­чить раннее обнаружение вторжения на территорию объекта.* Такие системы, как правило, ориентированы на обнаружение нарушителя, который уже проник на охраняемую территорию или в здание. Это касается, в частности, систем видеонаблюдения; они зачастую с помощью устройства видеозаписи могут лишь фиксируют факт вторжения после того, как он уже свершился. *Опытный наруши­тель всегда рассчитывает на определенное временное «окно», ко­торое проходит от момента проникновения его на объект до мо­мента обнаружения охранными средствами*. *Минимизация этого интервала времени является основным свойством, определяющим эффективность любой охранной системы*, и в этом смысле пре­имущества периметровой охранной сигнализации неоспоримы.

Периметровая граница объекта является наилучшим местом для раннего обнаружения вторжения, так как нарушитель сталкивается прежде всего с физическим периметром и *создает возмущения*, которые можно зарегистрировать специальными датчиками. Если периметр представляет собой ограждение в виде металлической решетки, то ее приходится перерезать или преодолевать сверху; если это стена или барьер, то через них нужно перелезть; если это стена или крыша здания, то их нужно разрушить; если это откры­тая территория, то ее нужно пересечь.

Все это вызывает физическое взаимодействие нарушителя с пе­риметром, который предоставляет хорошую возможность для элек­тронного обнаружения, так как нарушитель создает определенный уровень вибраций, содержащих специфический звуковой «образ» вторжения.

*При определенных условиях нарушитель может избежать фи­зического контакта с периметром*. В этом случае применяют «объ­емные» датчики вторжения, играющие роль вторичной линии за­щиты.

Датчик любой периметровой системы реагирует на появление нарушителя в зоне охраны или определенные действия нарушите­ля. Сигналы датчика анализируются электронным блоком (анали­затором или процессором), который, в свою очередь, генерирует сигнал тревоги при превышении заданного порогового уровня ак­тивности в охраняемой зоне. **Периметровый рубеж, проходящий по внешней границе территории объекта, первый и обязательный в системе охраны**.

*Периметровая система охраны* должна отвечать определенному набору требований, часть из которых перечислена ниже:

* Возможность раннего обнаружения нарушителя (еще до его проникновения на объект).
* Точное следование контурам периметра, **отсутствие «мерт­вых» зон**.
* По возможности скрытая установка датчиков системы.
* Независимость параметров системы от сезона (зима, лето) и по­годных условий (дождь, ветер, град и т.д.).
* Невосприимчивость к внешним факторам «нетревожного» ха­рактера – индустриальные помехи, шум проходящего рядом транс­порта, мелкие животные и птицы.
* Устойчивость к электромагнитным помехам – грозовые разря­ды, источники мощных электромагнитных излучений и т.п.

*Особенность периметровых систем* состоит в том, что обычно они конструктивно интегрированы с ограждением и формируемые охранной системой сигналы в сильной степени зависят как от фи­зико-механических характеристик ограды (материал, высота, жест­кость и др.), так и от правильности монтажа датчиков (выбор места крепления, метод крепления, исключение случайных вибраций ог­рады и т.п.). Большое значение имеет правильный выбор типа ох­ранной системы, наиболее полно отвечающей конкретному типу ограды.

Периметровые системы используют, как правило, систему *рас­пределенных или дискретных датчиков*, общая протяженность ко­торых может составлять несколько километров. Такая система должна обеспечивать высокую надежность при большом диапазоне изменения окружающей температуры и внешних условий (дождь, снег, сильный ветер). Поэтому любая система должна *обладать свойством автоматической адаптации к погодным условиям* и воз­можности дистанционной диагностики.

Периметровая система должна интегрироваться с другими ох­ранными системами, в частности, с системой видеонаблюдения.

Периметровые средства охраны (СО) используются в тех слу­чаях, когда:

* вокруг объекта нужно организовать четко регламентирован­ную зону обеспечения возможности адекватного воздействия на злоумышленников для их обезвреживания на подступах к объекту охраны;
* необходимо четко очертить границы территории объекта, в том числе для повышения дисциплины и порядка на предпри­ятии.

Обычно периметровые средства охраны используются совмест­но с ограждениями, которые обозначают границу территории объ­екта и тем самым создают вокруг него некую зону для обеспечения возможности адекватного воздействия на злоумышленника для его нейтрализации, т. е. **обеспечивают юридическую правомерность действий охраны внутри огороженной территории**.

В пользу необходимости сооружения периметровых сигнализа­ционных рубежей как для ОВ, так и для ПК объектов говорит сле­дующий факт. Отсутствие сигнализационных периметровых рубе­жей может привести к тому, что злоумышленник будет обнаружен несвоевременно и силам охраны просто не хватит времени для его нейтрализации. Кроме того, рубежи препятствуют несанкциониро­ванному выносу с объекта материальных ценностей.

**5. Функциональные зоны охраны**

При создании периметровой охраны ОВ объекта его внутренняя территория (охраняемая площадь) должна быть условно разделена на несколько функциональных зон: обнаружения, наблюдения, сдерживания, поражения, в которых располагаются соответствую­щие технические средства.

**Зона обнаружения** (ЗО) – зона, в которой непосредственно рас­полагаются периметровые средства обнаружения, выполняющие автоматическое обнаружение нарушителя и выдачу сигнала «Тре­вога». Размеры зоны в поперечном сечении могут изменяться от нескольких сантиметров до нескольких метров.

**Зона наблюдения** (ЗН) – предназначена для слежения с помо­щью технических средств (телевидение, радиолокация и т.д.) за обстановкой на подступах к границам охраняемой зоны и в ее про­странстве, начиная от рубежей.

**Зона физического сдерживания** (ЗФС) предназначена для задер­жания нарушителя при продвижении к цели или при побеге. Органи­зуется с помощью инженерных заграждений, создающих физические препятствия перемещению злоумышленника. Инженерные заграж­дения представляют собой различные виды заборов, козырьков, спи­ралей из колючей ленты и проволоки, рвов, механических задержи­вающих преград и т.п. Во многих случаях ЗО и ЗФС совмещаются.

**Зона средств физической нейтрализации и поражения** (ЗНП) предназначена соответственно для нейтрализации и поражения злоумышленников. В большинстве случаев располагается в ЗО и ЗФС. В этой зоне помещаются средства физического воздействия, которые в общем случае подразделяются на электрошоковые, ос­лепляющие (вспышки), оглушающие, удушающие, ограничиваю­щие возможность свободного перемещения (быстро застывающая пена), средства нейтрализации и поражения – огнестрельное ору­жие, минные поля и т.п.

**6. Оптимизация построения системы охранной безопасности**

Очевидным кажется, что задачи охраны могут быть эффективно решены путем отдаления внешнего ограждения, поскольку в этом случае злоумышленнику потребуется больше времени для преодо­ления расстояния до цели и, соответственно, больше времени оста­ется для действий сил охраны. Однако в этом случае удлиняется периметр объекта. Соответственно увеличиваются затраты на до­рогостоящие технические средства и их эксплуатацию, а также не­обходимая численность сил охраны.

**Таким образом, при построении эффективной системы охран­ной безопасности (СОБ) объекта необходимо решить задачу опти­мизации конфигурации и длины периметра, количества рубежей, выбора СО, физических барьеров (ФБ), средств нейтрализации и поражения, дислокации персонала охраны** и т.п.

На практике в подавляющем числе случаев приходится иметь дело с уже существующим, а не с проектируемым объектом. Поэто­му при построении **СОБ** в первую очередь ставится *задача миними­зации расходов на создание и эксплуатацию СО, ФБ и содержание персонала охраны при заданной эффективности защиты и особенно­стей (конфигурации, длины и т.д.) имеющегося периметра*.

Для многих предприятий актуальна проблема хищения матери­альных ценностей, которые перебрасываются через периметровое ограждение. Не всегда лучшими способами ее решения являются увеличение высоты ограждения или *расстояния до преграды с внутренней стороны*. Зачастую более целесообразно использовать с этой целью периметровые СО, расположенные с внутренней сто­роны ограждения на максимально допустимом расстоянии от него. Такое расположение СО обеспечивает наилучшие условия задер­жания как злоумышленников, пытающихся перебросить матери­альные ценности за пределы объекта или покинуть с ними охра­няемую территорию, так и внешних нарушителей. Это объясняется тем, что *по очередности срабатывания СО, расположенных на раз­личных рубежах, силы охраны могут определить направление дви­жения нарушителя.*

Организация единой периметровой охраны предприятия, в со­став которого входит несколько расположенных на выделенной территории ПК объектов, связанных единым технологическим циклом (рис. 1), экономически целесообразна в том случае, если защита отдельных объектов в сумме обходится дороже общего пе­риметра.

В качестве дополнительного довода в пользу решения вопроса об организации периметровой охраны служит то, что она является непременной составной частью общей системы, *без которой невозможна организация эффективной системы доступа на предприятие*. *Ее наличие обеспечивает полную гарантию входа и выхода персо­нала исключительно через регламентированные проходные*. Это также является одним из необходимых условий для организации эффективного учета рабочего времени персонала предприятия, со­стоящего из нескольких корпусов, расположенных на единой тер­ритории, но не соединенных крытыми переходами.

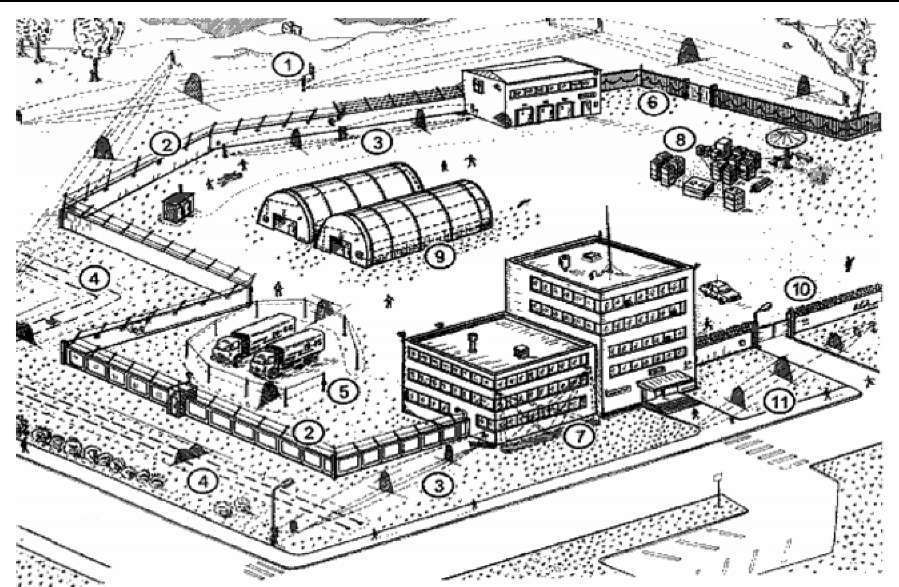


Рис. 6.1. Пример применения средств обнаружения различных типов на участках периметра условного объекта (размеры зон обнаружения, элек­тронные блоки и элементы показаны в разных масштабах): 1 - радиолучевое; 2 - радиоволновое; 3 - радиолучевое; 4 - радиоволно­вое (на основе «линии вытекающей волны»); 5 - радиоволновое однопро водное; 6 - вибросейсмическое; 7 - инфракрасное пассивное; 8 - обрыв­ное с указанием места обрыва микропровода; 9 - вибрационное кабель­ное; 10 - емкостное; 11 - радиолокационное (с возможностями организации прохода)

Существенным фактором, препятствующим созданию перимет­ровой системы охраны ПК объектов, является ее сравнительно вы­сокая стоимость. *Из соображений экономической целесообразно­сти принято, что периметровая охрана ПК объектов необходима там, где ее стоимость не превышает 10% от стоимости охраняемых материальных ценностей*. Поэтому необходимо проводить деталь­ное обоснование состава и структуры построения комплекса тех­нических средств периметрового рубежа охраны, исходя из воз­можных угроз, моделей нарушителей и концепции организации противодействия.

**7. Контроль доступа к защищаемым помещениям**

*Устройства и системы идентификации человека применяются в основном в системах контролируемого доступа в защищаемые по­мещения*. Контролируемый доступ предполагает ограничение круга лиц, допускаемых в определенные защищаемые зоны, и кон­троль за передвижением лиц внутри таких зон. *Эта задача решается не только физическими, но и аппаратными или программными средствами*. Только при комбинированном использовании всех средств возможно эффективное решение проблемы. Физические средства в системах контролируемого доступа могут использовать различные принципы идентификации, приведенные в табл. 1.

*Задача каждой системы контролируемого доступа заключается в том, чтобы позволить уполномоченному лицу получить доступ в помещение или к аппаратуре и воспрепятствовать проникновению в охраняемые зоны несанкционированному лицу*. При этом воз­можно появление двух типов ошибок: отказ санкционированному лицу в доступе и допуск несанкционированного лица. Идеальным решением всех проблем была бы идентификация каждого пользо­вателя. Зарубежные специалисты четко разграничивают задачи идентификации и опознавания. ***Под идентификацией*** *они понима­ют присвоение объектам и субъектам персональных идентифика­торов* (имен, кодов, паролей и т.п.).

Таблица 1

|  |  |
| --- | --- |
| **Метод опознавания** | **Средство или признак опознавания** |
| Непосредственное обще­ние | Взаимодействие с охранником или вахте­ром |
| Персональный:  квазиста­тический | Отпечатки пальцев, строение лица, гео­метрия руки, особенности глаз, отпечатки ладони, кровеносные сосуды |
| Персональный:  квазиди­намический | Пульс, баллистокардиография, энцелография, динамические реакции, речь, почерк, стиль печатания |
| Атрибутный:  карты | Фотокарты (стандартные, ИК); с электри­ческим кодированием (пассивные, ак­тивные); магнитные (ферритовые), с ме­ханическим кодированием; с оптическим кодированием; (светопроводимость, отра­жение, флюоресценция, голограммы); ме­таллические ярлыки |
| Документы | Паспорт, идентификационные карты, во­дительские права |
| Основанный на знаниях | Изображения, специальные символы, лич­ный номер, код, пароль |

Считается, что идентификация является планомерной задачей, *точность решения которой убывает при возрастании числа канди­датов*. Под кандидатом понимается лицо, желающее пройти в за­щищаемую зону.

**Опознавание (аутентификация)** *предполагает сравнение теку­щей информации о кандидате с эталонной, хранящейся в памяти ЭВМ* (эталонная информация собирается заранее и приписывается определенному человеку).

*Точность решения задачи опознавания в общем случае не зави­сит от числа кандидатов* (когда это не связано с ограничением объ­ема памяти).

Рассмотрим более подробно способы опознавания личности. Атрибутные способы достаточно ясны и не требуют по­яснений. Заметим, что они наиболее подвержены различного рода подделкам и мошенничеству (включая подкуп, шантаж и даже гип­ноз). Персональные способы наиболее совершенны. Во-первых, они полно описывают каждого отдельного человека, а во-вторых, не­возможно, или крайне трудно передать или подделать индивиду­альные характеристики. Квазистатические способы включают ана­лиз внутренних физических характеристик, таких, как отпечатки пальцев. Они дают очень малую вероятность ошибок обоих типов, так как не требуют каких-либо сложных действий кандидата и ста­бильны во времени.

Квазидинамические способы используют изменяющиеся во времени преобразованные сигналы. Физиологические характеристи­ки внутри этой группы являются наименее изученными и перспек­тивными с точки зрения уменьшения ошибок в опознавании. Харак­теристики, зависящие от привычек и навыков, являются не только наиболее простыми для подделок, но и наиболее дешевыми с точки зрения практической реализации. Способы опознавания, основан­ные на чем-либо запоминаемом (код, пароль и т.п.) могут применят­ся в случаях наиболее низких требований к безопасности, так как часто эта информация записывается пользователями на пропусках или в записных книжках, что может свести на нет все усилия. Кроме того, имеется возможность подсмотреть, подслушать или получить эту информацию другим путем (шантаж, подкуп и т.п.).

Новые возможности дает применение *магнитных карточек* в системах безопасности для контроля доступа в помещения, к ком­пьютерам, к компьютерным сетям, как устройство хранения полно­мочий пользователя. В настоящее время получило широкое приме­нение в системах контроля физического доступа использование маг­нитных карточек типа Smart Card. В этом случае карточка использу­ется как ключ к замку. Благодаря большому объему информации, который может быть записан на карточку, одна карточка может быть ключом к разным замкам. Такой подход позволяет организовать доступ строго определенных лиц в различные помещения. Исполь­зование идентификационных данных с карточки позволяет *органи­зовать эффективный контроль доступа в помещения и хранение этих данных в компьютерной базе данных*. При этом в любой момент можно узнать, кто в каком помещении находится, а также время входа и выхода из помещения. Помимо этого, карточки могут также применяться как электронные ключи не только к дверям, но и к раз­личному оборудованию, автомобилям и т.д. Существуют устройства контроля физического доступа (специ­альные замки) управляемые с помощью ИК-луча. Замок имеет бло­кировку, снимаемую только после облучения специальным ИК- лучем с помощью специального электронного ключа.

**8. Охрана оборудования и перемещаемых носителей** **информации**

*Для защиты сейфов, стальных и деревянных шкафов, витрин и других подобных объектов служит система, состоящая из двух частей: контрольного устройства с комплектом датчиков, которое устанавливается в помещении, где находится защищаемый объ­ект, и блока сигнализации, который монтируется в помещении для дежурного персонала* (примером может служить система «Электрогард» выпускаемая венгерским предприятием «Электро­техника»).

Контрольный блок устанавливается в любом месте вблизи ох­раняемого объекта: на столе, на полке или крепится на стене. Дат­чик (или несколько датчиков при защите нескольких объектов) размещается в замочной скважине охраняемого объекта. При этом становится невозможным незаметное вскрытие объекта даже с по­мощью ключа к данному замку, так как смонтированный в скважи­не датчик не дает возможности вставить ключ. Удаление датчика или его повреждение влечет за собой немедленную подачу сигнала тревоги.

Сигнал тревоги подается и при любой попытке вывести систе­му защиты из строя. Такими попытками могут быть: удаление дат­чиков, перерезание проводов, короткое замыкание цепей, выклю­чение источника питания, механическое повреждение корпуса кон­трольного блока и т.п.

В системе предусмотрены контакты для подключения дополни­тельных датчиков защиты дверей, окон и стен охраняемого помеще­ния. Наряду со сложными системами защиты, в которых использу­ются ЭВМ и сложные электронные устройства, широкое распро­странение получили и довольно простые системы из электрических и магнитных элементов.

В качестве таких элементов применяются микровыключатели, фиксирующие открывание или закрывание дверей и окон, специаль­ные коврики, срабатывающие под весом тела злоумышленника, пет­ли из проводников, фиксирующие положение аппаратуры, простей­шие инерционные датчики и т.п.

Используя различные комбинации этих элементов, можно соз­давать достаточно разветвленные системы защиты. Для подключе­ния таких датчиков и для соединения их с центральным пунктом систем защиты *допустимо использование осветительной сети, те­лефонных проводов и проводки ТВ-антенн*.

*Для предотвращения выноса различных материалов и малога­баритной аппаратуры из помещения ВЦ в одной из систем на все документы и на приборы наклеиваются специальные наклейки из фольги или другого магнитного материала. При этом около выхода из помещения монтируется специальная установка, принцип дейст­вия которой аналогичен принципу действия детектора металличе­ских объектов*.

Эта установка подает сигнал тревоги при любой попытке вы­нести за пределы помещения предмет с наклейкой. По утвержде­нию разработчиков, ни тело человека, ни другие объекты не экра­нируют наклейку, что гарантирует надежную работу такой систе­мы предотвращения краж.

**Литература**

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.
3. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И.К.Корнеев, Е.А. Степанов.- М.:Проспект,2011.-336 с.
4. Зегжда Д.П., Ивашко A.M. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2009.

**Лекции № 18-20**

**СИСТЕМЫ ЗАЩИТЫ ТЕРРИТОРИИ И ПОМЕЩЕНИЙ**

План:

1. Инфракрасные системы

2. Элементы защиты ИК-датчиков

3. Оптоволоконные системы

4. Емкостные системы охраны периметров

5. Вибрационные системы с сенсорными кабелями

6. Вибрационно-сейсмические системы

7. Радиолучевые системы

8. Системы «активной» охраны периметров

**1. Инфракрасные системы**

*Инфракрасные элементы применяются главным образом внутри помещений*, так как при использовании их на открытом воздухе воз­можны ситуации, вызывающие появление ложных тревог (порывы воздуха, перемещение различных животных, ИК-облучение и т.д.). *Существует два типа ИК-систем: активные и пассивные*. *Активные системы требуют использования передатчика (излучающего пучок ИК-энергии) и приемника и точной установки этих устройств по отношению друг к другу*. К тому же ИК-лучи могут быть довольно просто обнаружены. Все это является причиной более широкого использования *пассивных систем. Функционирование системы ос­новано на фиксации невидимого излучения движущегося человека ИК-датчиком*. Человек генерирует тепловое излучение, эквива­лентное излучению 500-ватной лампы и имеющее длину волны 10 мкм*. Радиус обнаружения одного датчика лежит в пределах 5... 15 м, охраняемая площадь - до 150 м2 и углы приема в горизон­тальной и вертикальной плоскостях до 70°.* Для увеличения этих параметров достаточно простого наращивания элементов системы. При попадании идущего человека в поле обнаружения системы на выходе датчика появляются два характерно поляризованных им­пульса, которые подлежат усилению. Логическое устройство в кон­трольном приборе выделяет эти сигналы из фоновых и, если сигна­лы не исчезают в течение определенного времени, подает звуковой или визуальный сигнал тревоги. Датчик, используемый в системе должен быть чувствительным, недорогим и простым в производ­стве. *Он должен реагировать только на излучение с длиной волны 10 мкм и не срабатывать от источников света.*

Если сравнивать пассивные и активные системы то можно сде­лать следующие выводы:

* В пассивных системах нет излучения, поэтому они не могут быть «обмануты» даже опытным нарушителем.
* Отсутствие эмиссии энергии позволяет делать устройства простыми, надежными, не требующими технического обслужива­ния, дешевыми и долгоживущими. Отсутствие движущихся частей ведет к отсутствию износа.
* Установка пассивной системы проста, поле зрения велико и не требует точной взаимонастройки передатчика и приемника, как в активных системах.
* Датчики не реагируют на большинство источников ложных тревог. Перед подачей сигнала тревоги логические схемы должны обнаружить два импульса противоположной полярности в течение установленного промежутка времени. Конвекционные потоки, сис­темы отопления, кондиционирования не вызывают появления та­ких сигналов.
* Системы имеют широкое поле зрения, достаточно двух дат­чиков для полей защиты помещения от проникновения с любого направления.
* Активные системы (ИК, УЗ, СВЧ и др.) могут реагировать на события вне данного помещения (шум, источники света, вибрация и т.д.), что может вызвать появление ложных тревог. Пассивные системы этого недостатка не имеют. Единственным, но не принци­пиальным недостатком пассивных ИК-систем является необходи­мость установки большого числа датчиков для защиты длинных коридоров. Активные системы, имеющие большой радиус дейст­вия (до 100 м), требуют только установки отражателей.

**Активные лучевые ИК системы**

*Лучевые инфракрасные системы (их часто называют также ли­нейными активными оптико-электронными извещателями) состоят из передатчика и приемника, располагаемых в зоне прямой взаим­ной видимости*. *Такой датчик формимует сигнал тревоги при пре­рывании луча, попадающего на фотоприемный блок*. *Отличитель­ная особенность активных лучевых систем - возможность созда­ния очень узкой зоны обнаружения.* На практике сечение чувстви­тельной зоны определяется размером используемых в оптических блоках линз. Это особенно важно для объектов, вокруг которых невозможно создать зону отчуждения. Однако, как и радиолучевые, ИК-лучевые системы могут применяться только на прямолинейных участках периметров или оград.

Основная проблема лучевых ИК-охранных приборов – ложные срабатывания при неблагоприятных атмосферных условиях (дождь, снегопад, туман), уменьшающих прозрачность среды. На­дежность в таких случаях обеспечивают за счет многократного превышения энергии луча над минимальным пороговым значени­ем, необходимым для срабатывания датчика.

Источником помех может быть также прямая засветка прием­ника солнечными лучами. Чаще всего это случается на закате или рассвете, когда солнце стоит низко над горизонтом. Согласно рос­сийским стандартам датчик должен сохранять работоспособность при естественной освещенности не менее 10000 лк и не менее 500 лк – от электрических осветительных приборов. Большинство со­временных отечественных и зарубежных лучевых датчиков имеют специальные средства фильтрации фонового излучения и отвечают указанным выше требованиям. Однако для обеспечения высокой помехозащищенности от засветки очень важно правильно юстиро­вать датчик при его настройке и выполнять все рекомендации изго­товителя по монтажу.

Кроме того, ИК системы могут срабатывать при попадании в луч птиц, листьев и веток деревьев или др. Для повышения устой­чивости и надежности ИК-лучевых систем их делают многолуче­выми (обычно используют 2 или 4 независимых луча), а также применяют схемы автоматической обработки сигналов, минимизи­рующие влияние внешней среды.

Специальные меры принимают для сохранения работоспособ­ности датчиков в зимних условиях, при возможности обмерзания или налипания снега на оптические поверхности блоков. Достаточ­но надежными методами борьбы с указанными явлениями служат специальные козырьки на оптических фильтрах и внутренние обогреватели оптико-электронных блоков.

Одними из самых распространенных отечественных ИК-лучевых охранных приборов являются извещатели серии СПЭК. **Комплект СПЭК-75** содержит блок излучателя, блок фото­приемника и комплект для монтажа. Система обеспечивает угол расходимости оптического пучка 3° и позволяет организовать однолучевой рубеж охраны длиной до 75 м (на улице). Излучатель генерирует в диапазоне ближнего ИК-спектра на длине волны 0,8...0,9 мкм, сигнал тревоги включается при прерывании луча на заданный промежуток времени. Для обеспечения работы в небла­гоприятных условиях (дождь, снегопад, туман) излучатель имеет 100-кратный запас по мощности излучения. Приняты меры для ис­ключения ложных срабатываний от солнечной засветки (10000 лк).

Электронные блоки идентичны по конструкции, они имеют размеры 140x145x65 мм. Для юстировки системы можно использо­вать специально подключаемый для этой цели вольтметр. Номи­нальное напряжение питания –12 В, потребляемый ток – не более 60 мА. Диапазон рабочих температур от – 40 до +50°С. Для органи­зации двухлучевого барьера используют второй комплект извещателя.

Выпускаются также модификации серии СПЭК для зон охраны до 175 м.

Более совершенным и мощным является отечественный **ИК- лучевой извещатель «Рубеж-ЗМ»**. Комплект включает две пары приемо-передающих блоков, управляемых общим блоком контро­ля. В приборе применена импульсная модуляция ИК-излучения и синхронный прием, что позволило повысить дальность действия и реализовать параллельную работу нескольких излучателей в мно­голучевых барьерах. Комплект позволяет организовать двухлучевой контур охраны на длине участка 300 м или два отдельных однолучевых рубежа на длине до 600 м. С помощью двух комплектов Рубеж-ЗМ можно также создать 4-лучевой барьер с повышенной помехозащищенностью. Система работоспособна даже при густом тумане, когда «метеорологическая дальность видимости» умень­шается до 180 м. Аппаратура выдает сигнал тревоги, если луч пе­рекрывается на время не менее 100 мс, что соответствует движе­нию человека со скоростью до 5 м/с (18 км/ч).

Блоки излучателя и фотоприемника системы Рубеж-ЗМ поме­щены в идентичные металлические корпуса, укрепляемые на пово­ротных кронштейнах. Габаритные размеры блока (с кронштейном) – 275x190x120 мм. Внутри блоков имеются устройства подогрева, что обеспечивает работоспособность при температуре до – 45°С. На неогороженных территориях блоки устанавливают на специальных стойках. Минимальная рекомендуемая высота луча над землей – 0,3 м, что позволяет обнаружить ползущего нарушителя. При на­личии оград блоки обычно укрепляют вдоль верхнего края ограды.

Практически все зарубежные ИК-лучевые охранные приборы объ­единяют в общем корпусе двухлучевую или четырехлучевую син­хронную систему. На российском рынке широко представлены **ИК- лучевые датчки фирм С&К, Atsumi, Visonic, Optex, Alarmcom и др**.

На рис. 1 показана конструкция одного из блоков двухлучево- го ИК датчика ерии АХ-100/АХ-200 фирмы Optex (Япония).



Рис. 1. Лучевой ИК-датчик серии АХ фирмы Optex

По конструкции блоки передатчика и приемника аналогичны. Лицевая крышка выполнена из ударопрочного пластика, прозрачного толь­ко для ИК-излучения. Крышка имеет специальный выступающий козырек, препятствующий осаждению инея на наружной поверхно­сти. Под крышкой находится электронно-оптический блок с двумя линзами, смонтированными на поворотной платформе. Угловое положение платформы регулируется при юстировке в пределах ±90° по горизонтали и ±5° по вертикали винтами. Для облегчения юстировки в поворотную платформу встроен специальный миниа­тюрный видоискатель, позволяющий точно навести линзы на вто­рой блок системы. Для точной юстировки системы по уровню принимаемого сигнала в блоке приемника имеются гнезда для под­ключения вольтметра. Здесь же расположены регулятор времени срабатывания датчика и светодиодные индикаторы («грубая на­стройка» и «тревога»), используемые при настройке прибора. Оп­тико-электронный блок фиксируется на монтажной плате, которую обычно крепят к вертикальной штанге с помощью хомута.

Регулятор допустимого времени перекрытия лучей, установ­ленный в блоке приемника, позволяет изменять время срабатыва­ния от 500 мс (сравнительно медленное перелезание через ограду) до 50 мс (очень быстро бегущий человек). Обычно рекомендуется устанавливать время пересечения луча не более 70... 100 мс, чтобы обеспечить достаточную чувствительность системы. Датчики се­рии АХ фирмы ОРТЕХ обеспечивают дальность обнаружения от 22 до 150 м на улице и от 40 до 300 м в помещении. Для питания используется источник постоянного тока с напряжением 10,5...28 В, потребляемый ток – не более 46 мА, диапазон рабочих температур от –35 до +55 С при влажности до 95%.

Для объектов с высокой степенью защиты иногда применяют ИК-лучевые системы с числом лучей от 4 до 8. Среди таких много­лучевых систем можно упомянуть датчик IPS 600 фирмы GPS (Италия), датчики серии IS 400 фирмы Alarmcom (Швейцария) или датчики серии IPID фирмы ECSI (США). Конструктивно многолу­чевые ИК датчики обычно выполняют в виде вертикальных штанг высотой примерно до 3,5 м. Многолучевые системы используют чаще всего для охраны военных объектов, объектов атомной энер­гетики, крупных промышленных предприятий.

**Пассивные ИК-системы**

*Такие «однопозиционные» системы представляют собой пас­сивные ИК-детекторы с пространственной диаграммой чувстви­тельности в виде луча.* Они проще в монтаже и настройке, чем двухпозционные *ИК-лучевые системы и используются в основном там, где нужно перекрыть короткие участки периметра - зоны въезда транспорта, разрывы в ограждениях, ворота, оконные про­емы и т.п.* *Для таких датчиков характерно большее поперечное се­чение чувствительной зоны, чем для лучевых оптических датчиков.*

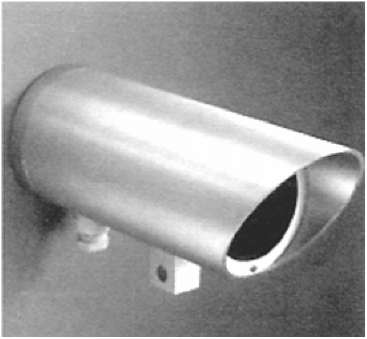
**Пассивные ИК барьеры IS 402 и IS 412 фирмы Alarmcom** (Швейцария) предназначены для уличной эксплуатации в сложных атмосферных условиях. **Датчик IS 402** (рис. 2) выполнен в проч­ном алюминиевом корпусе с козырьком, защищающим от солнеч­ной засветки. Датчик IS 402 формирует зону чувствительности в виде «занавеса» длиной 100 м и высотой до 4 м. Датчик IS 412 име­ет повышенную чувствительность и обеспечивает зону длиной 150 м.

Рис. 2. Пассивный ИК-датчик IS 402 фирмы Alarmcom

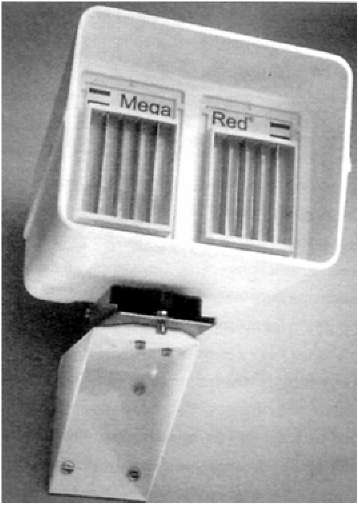
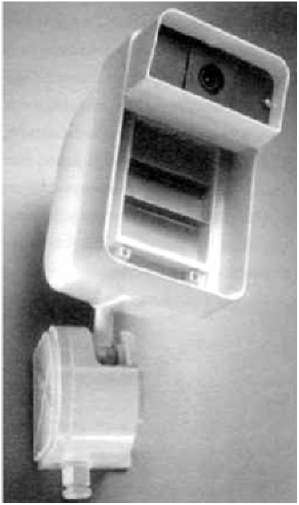
**Однопозиционные пассивные ИК-датчики для охраны перимет­ров выпускает английская компа­ния Security Enclosures Ltd (SEL)**. В открытом пространстве датчик Redwall-100Q, использующий тех­нологию «квадруплексного» (четы- рехканального) детектирования, обеспечивает зону чувствительно­сти длиной 100 м и поперечным сечением 3 м. Усовершенствован­ный двухсекционный датчик Megared-180Q (рис. 3) позволяет защищать зону длиной до 180 м. Одна из секций датчика предназначена для детектирования в «ближней» зоне, а другая - в «дальней». Сигналы от секций датчи­ка можно использовать, например, для управления поворотной ви­деокамерой.

Рис. 3. Пассивный ИК-датчик Megared-180Q фирмы SEL



Одна из модификаций детектора фирмы SEL - **комбинирован­ный датчик Redwatch-100Q** - *объединяет в себе пассивный ИК- датчик и встроенную миниатюрную видеокамеру, поле зрения ко­торой совпадает с чувствительной зоной ИК-датчика* (рис. 4).

Рис. 4 Комбинированный ИК-датчик Redwatch-100Q

Возможность оперативной визуальной проверки ситуации в «тревожной» зоне сильно повышает общую эффективность охраны. *Для повышения устойчивости к внешним факторам и снижения частоты ложных срабатываний периметральные ИК-детекторы иногда конструктивно объединяют с СВЧ-датчиками*. Примером такого комбинированного прибора (иногда их называют датчиками двойной технологии) является **детектор серии DT-900 фирмы С&К** (рис. 5).

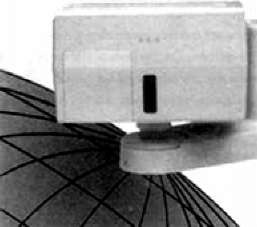


Рис. 5. Датчик двойной технологии (ИК+СВЧ) серии DT-900 фирмы С&К

*Два канала обнаружения – пассивный инфракрасный и радио­волновой – позволяют обеспечить высокую обнаруживающую спо­собность при хорошей устойчивости к помехам*.

Датчик снабжен тройной системой самодиагностики; он имеет специальный активный оптический датчик, сигнализирующей о попытке умышленной блокировки прибора путем перекрытия чув­ствительной зоны. Микропроцессор с памятью событий позволяет выбирать оптимальный алгоритм обнаружения вторжения в раз­личных окружающих условиях. В зависимости от используемой фокусирующей оптики дальность действия датчика составляет 37 м (сечение зоны 3 м) или 61м (сечение зоны 5 м).

Очевидно, что периметровая охранная система должна обла­дать максимально высокой чувствительностью, чтобы обнаружить даже опытного нарушителя. В то же время эта система должна обеспечивать по возможности низкую вероятность ложных срабатываний. Причины лож­ных тревог могут быть различными. Система может, например, среагировать при появлении в зоне охраны птиц или мелких животных. Сигнал тревоги мо­жет появиться при сильном ветре, граде или дожде.

Кроме того, ложная тревога может возникнуть из-за «технологических» причин: неграмотный монтаж датчиков на ограде, неправильная настройка электронных блоков или просто неудовлетворительное инженерное состояние самой ограды, кото­рая может, например, вибрировать при сильном ветре

**2. Элементы защиты ИК-датчиков**

*В ИК-датчиках, предназначенных для профессионального ис­пользования, применяются так называемые схемы антимаскинга*. Суть проблемы состоит в том, что обычные *ИК-датчики могут быть выведены нарушителем из строя путем предварительного (ко­гда система не поставлена на охрану) заклеивания или закрашива­ния входного окна датчика*. Для борьбы с этим способом обхода ИК-датчиков и используются схемы антимаскинга. Метод основы­вается на использовании специального канала ИК-излучения, сра­батывающего при появлении маски или отражающей преграды на небольшом расстоянии от датчика (от 3 до 30 см). Схема антимас­кинга работает непрерывно, пока система снята с охраны. Когда факт маскирования обнаруживается специальным детектором, сиг­нал об этом подается с датчика на контрольную панель, которая, однако, не выдает сигнала тревоги до тех пор, пока не придет вре­мя постановки системы на охрану. Именно в этот момент операто­ру и будет выдана информация о маскировании. Причем, если это маскирование было случайным (крупное насекомое, появление крупного объекта на некоторое время, вблизи датчика и т.п.) и к моменту постановки на сигнализацию самоустранилось, сигнал тревоги не выдается.

*Еще одним защитным элементом, которым оборудованы прак­тически все современные ИК-детекторы, является контактный дат­чик вскрытия, сигнализирующий о попытке открывания или взлома корпуса датчика*. Реле датчиков вскрытия и маскирования подклю­чаются к отдельному шлейфу охраны.

*Для устранения срабатываний ИК-датчика от мелких животных используются либо специальные линзы с зоной нечувствительно­сти (Pet Alley) от уровня пола до высоты порядка 1 м, либо специ­альные методы обработки сигналов*.

*Для защиты от электромагнитных и радиопомех используется плотный поверхностный монтаж и металлическое экранирование*.

Рассмотрим подробнее возможности и характеристики ИК-датчиков на примере продукции известных фирм.

ИК-датчики российского производства представлены серией ФОТОН (рис. 6).

Рис. 6. Датчик ФОТОН-8

В датчиках используются линзы Френеля (в ФОТОН-4 – многосегментное зеркало) и сдвоенные пироприемники.

Конфигурация зон чувствительности имеет вид:

ФОТОН-4, ФОТОН-6, ФОТОН-8 – объемная трехъярусная зона длиной до 12 м, 90° в горизонтальной плоскости;

ФОТОН-5, ФОТОН-6Б, ФОТОН-8Б – сплошной занавес длиной 10 м, 5° в горизонтальной плоскости;

ФОТОН-6А, ФОТОН-8А – лучевой барьер длиной 20 м, 5° в горизонтальной плоскости;

ФОТОН-СК – объемная трехъярусная зона длиной до 10 м с двумя антисаботажными зонами или поверхностная одноярусная зона (защита от животных) длиной до 10 м.

Диапазон обнаруживаемых скоростей 0,3... 3 м/с.

*Датчики предназначены для использования в закрытых отапли­ваемых и неотапливаемых помещениях в диапазоне температур от* 0°С (ФОТОН-СК), –10°С (ФОТОН-8), –30°С (ФОТОН-4, ФОТОН- 6), –40°С (ФОТОН-5) до +50°С.

Фирма **CROW Electronic Engineering Ltd** (Израиль) выпускает широкую номенклатуру относительно дешевых, но надежных и хо­рошо зарекомендовавших себя моделей **ИК-пассивных детекторов**.

Датчики фирмы CROW изготавливаются по ASIC-технологии - с использованием импульсных микросхем специального назначе­ния. В датчиках используются как традиционные, так и уникальные решения.

В ИК-детекторах применяются высококачественные пылезащищенные сменные линзы, формирующие зоны защиты типа вер­тикальный барьер длиной 22 м, многоярусная объемная зона 88° размером 18x22 м, коридорная зона 30x6 м, одноярусная зона 100° размером 15x18 м с проходом для животных. Применяются сдвоен­ные и счетверенные пироэлементы, обеспечивается высокая степень защиты от попадания прямого света, электромагнитного и радиочас­тотного излучения (до 30 В/м в диапазоне 10... 1000 МГц). Преду­смотрена автоматическая термокомпенсация, обеспечивающая по­стоянную чувствительность в рабочем диапазоне температур.

В **ИК-датчике GENIUS** используется двойная оптика, имити­рующая трехмерное стереовидение, при обработке производится счет импульсов с возможностью переключения пределов подсчета до 2 или 4. Этот датчик позволяет игнорировать сигналы от мелких животных. ИК-детектор D&D является аналогом GENIUS в улич­ном исполнении - в нем обеспечены влагозащита и адаптация к изменениям температуры, ветра и фонового шума. Датчики пред­назначены для сложных условий.

 В новой **серии SRP** (рис. 7) *применяется комбинированная оптика на линзах Френеля и зеркалах для защиты зоны непосредст­венно под датчиком*. При обработке используется спектральный анализ и фильтрация сигналов с пироприемника, а также «настоя­щая» двусторонняя термокомпенсация.

Рис. 7. Датчики SRP-600/700

Предусмотрена также воз­можность счета до 1, 2, 3. Датчики SRP-600 и SRP-700 могут ком­плектоваться линзами черного цвета для повышения защиты от за­светки.

Для более простых условий предназначены **ИК-датчики LYNX и LYNX-100**. В детекторе LYNX-100 обеспечена возможность ре­гулировки чувствительности и переключения режима обработки: счет до 2 или автоматический выбор предела счета.

Фирма **PYRONIX Ltd** (Великобритания) производит **ИК-пассивные датчики**, в которых используется герметичная оптика, сдвоенные и счетверенные пироприемники, детекторы изготовлены по технологии поверхностного монтажа. Сменные линза Френеля обеспечивают различные конфигурации зоны чувствительности: трехъярусная объемная зона 90° (34 или 54 луча по 15 м), одноярус­ная поверхностная зона 142° (24 луча по 30 м), вертикальный луче­вой барьер 10° (24 луча по 30 м). Для потолочных датчиков (серия OCTOPUS) зона чувствительности представляет собой 172 луча в четырех плоскостях, угол охвата 360°. Регистрируемая датчика­ми скорость движения человека составляет 0,3...3 м/с.

При обра­ботке сигналов с пироприемников используются следующие запа­тентованные алгоритмы:

IFT (независимые плавающие пороги) – порог срабатывания устанавливается на низком уровне внутри частотного диапазона полезного сигнала (0,6...10 Гц) и на более высоком уровне вне это­го частотного диапазона;

SPP (алгоритм чередующихся знаков) – подсчет импульсов ведется только для сигналов с чередующимися знаками (противо­положной полярности);

SGP3 (счетчик групповых последовательностей) – подсчитываются только группы импульсов, имеющих противоположную полярность, и состояние тревоги возникает при появлении трех та­ких групп в течение установленного времени.

В некоторых **датчиках PYRONIX** *используется регистрация фонового теплового излучения окружающего пространства и инди­кация его уровня свечением светодиода*. Эта функция помогает при установке датчика на объекте выбрать его рациональное размеще­ние и оптимальный для конкретных условий метод обработки сиг­налов.

Фирма **SENTROL** (США), выпускающая широчайшую номенк­латуру ИК-датчиков как под своей торговой маркой, так и под тор­говой маркой ARITECH Europe (последние имеют в своем назва­нии префикс EV). Наиболее интересны следующие датчики.

Серия АР использует прецизионную зеркальную оптику со сменными зеркальными масками, формирующую зоны чувстви­тельности типа одиночный или многовеерный занавес с равномер­ной чувствительностью по всей охраняемой зоне. Длина занавеса – до 25 м, рекордсменом является АР643 с длиной луча до 60 м. Ис­пользуется микропроцессорная обработка, учитывающая двухполярность, симметрию и длительность сигналов, а также адаптив­ный порог, дополненный 2- или 4-имульсным счетом.

Серия датчи­ков **Sharpshooter 6100** (рис. 8) использует сменные линзы Фре­неля, формирующие разнообразные зоны чувствительности: оди­ночный длинный луч, лучевой барьер, трех-четырехярусные объ­емные зоны с количеством лучей до 25, углами раскрыва в гори­зонтальной плоскости от 6 до 140°, максимальной длиной луча от 6 м до 27 м.



Рис. 8. Датчик Sharpshooter-6187

Используются сдвоенные и счетверенные пироприемники, цифровая обработка сигналов. Чувствительность по темпера­туре 1...1,25°С. Диапазон рабочих температур от – 40 до +50°С. Имеются модификации в пылевлагозащитном исполнении, в том числе в высокопрочном алюминиевом корпусе. Допускается внут­ренняя и наружная установка. Рекомендуются производителем для любых применений - от школ до военных объектов.

В серии **датчиков PI** используются специальные методы обра­ботки сигналов, позволяющие подавлять срабатывания от мелких животных. Фирма С&К Systems, Inc. (США) является одним из за­конодателей мод в разработке ИК-детекторов. Ее последними дос­тижениями в этой области являются датчики нового поколения **МС-550Т и МС-760Т**. Датчики комплектуются сменными линзами Френеля, формирующими различные варианты зоны чувствитель­ности: четырехярусную объемную (33 луча) и лучевой барьер с до­полнительными антисаботажными зонами, поверхностную с аллеей для животных (максимальная дальность составляет 15 м для МС-550Т и 18 м для МС-760Т (рис. 9). В конструкции датчиков применяется специальная защита от проникновения насекомых к пироэлементу.

Рис. 9. Датчик МС-760Т

В этих датчиках применены микроконтроллеры со встроенными аналогово-цифровыми преобразователями, позво­ляющими не только регистрировать наличие сигнала, но и анали­зировать такие его параметры, как амплитуду, длительность самих сигналов и интервалов между импульсами, неизменность величины сигнала от импульса к импульсу.

Объем программы обработки сигналов, зашитой в памяти мик­роконтроллера, превышает 2000 байт. Цифровая обработка значи­тельно увеличивает надежность обнаружения при одновременном снижении количества ложных срабатываний. В датчике МС-760Т применяется усовершенствованный алгоритм, использующий эле­менты статистического обнаружения и распознавания.

Особенностями этих ИК-детекторов являются:

* отсутствие реакции на мелких животных на расстоянии более 1,9 м от датчика (масса животных не более 7 кг для МС-550Т и не более 11 кг для МС-760Т) за счет цифровой обработки;
* использование прецизионной оптики (для МС-760Т), обеспе­чивающей равномерную чувствительностью по всей диаграмме направленности;
* «настоящая» двухсторонняя температурная компенсация;
* широкий диапазон рабочих температур (0...+55 С для датчика МС-550Т и -10...+55С для МС-760Т);
* динамическая самодиагностика, которая автоматически про­водится раз в сутки, при этом тестируются как цепи обработки ин­формации (RAM, ROM, пороги, питание), так и сам канал обнару­жения, включая пироэлемент;
* режим самодиагностики может быть также активирован с кон­трольной панели;
* улучшенная помехозащищенность (по свету 6500 лк, по элек­тромагнитным и радиопомехам 30 В/м для МС-550Т и 40 В/м для
* МС-760Т);
* специальный режим поиска зон диаграммы направленности, позволяющий существенно упростить подключение и настройку датчика при установке;
* наличие реле вскрытия корпуса датчика.

**3. Оптоволоконные системы**

*Оптоволоконные кабели*, используемые обычно для передачи информации, *можно* *использовать также и в качестве датчиков для периметровых охранных систем*. *Деформация оптоволоконно­го кабеля изменяет его оптические параметры (показатель пре­ломления и др.) и, как следствие, характеристики прошедшего через волокно лазерного излучения*. В силу специфики исполь­зуемых физических принципов *оптоволоконные системы* *отлича­ются очень малой восприимчивостью к любым электромагнитным помехам, что позволяет использовать их в неблагоприятной элек­трофизической обстановке*.

Оптоволоконные кабели проявляют несколько физических эффектов, позволяющих применять их в качестве периметровых датчиков. *Во всех случаях к одному концу кабеля подключен ми­ниатюрный полупроводниковый лазер, генерирующий когерент­ное излучение. Противоположный конец кабеля состыкован с фо­тодиодом (приемником), преобразующим оптический сигнал в электрический.* *Анализатор сравнивает принимаемый сигнал с эталонным, который соответствует невозмущенному состоянию сенсора, и детектирует внешние воздействия на периметр* (сме­щения, вибрации или сжатия кабеля).

В охранной **системе Model М106Е фирмы Fiber SenSys** (США) используется метод регистрации межмодовой интерференции. Лазер излучает несколько десятков близких по частоте мод (спек­тральных линий) с определенным распределением энергии по спектру. *Если оптоволоконный кабель подвергается механиче­ским воздействиям, то на его выходе регистрируемый приемни­ком спектр излучения меняется, что позволяет детектировать де­формации кабеля*.

В **оптоволоконной системе фирмы Sabreline** (США) *исполь­зуется эффект изменения распределения излучения по попереч­ному сечению при деформации волокна*. На выходе многомодового оптоволокна наблюдается так называемая «спекл-структура» (speckle-structure), представляющая собой нерегулярную систему светлых и темных пятен. Для детектирования дефор­маций кабеля здесь применяют пространственно-чувствительные фотоприемники.

**Оптоволоконные системы серии FOIDS** (изготовитель фирма Mason & Hanger, США) используют принцип двухлучевой интерфе­рометрии. Луч лазера расщепляется на два и направляется в два идентичных одномодовых оптических кабеля, один из которых яв­ляется детектирующим, а другой – опорным. На приемном конце оба луча образуют интерференционную картину. *Механические воздей­ствия на детектирующий кабель приводят к изменениям интерфе­ренционной картины, которые регистрируются фотоприемником*.

*Интересной особенностью оптоволоконных систем является возможность их применения для защиты не только оград, но и не огражденных территорий*. *В последнем случае волокно распо­лагают под поверхностью земли, в канавке, заполненной гравием.* При этом, как показали испытания в Sandia National Laboratories (США), система способна регистрировать шаги идущего или бе­гущего человека.

Среди отечественных разработок оптоволоконных периметраль­ных систем можно отметить **систему «Ворон»**. Основой системы являются серийно выпускаемые извещатели, состоящие из двух гер­метичных блоков — лазерного передатчика и фотоприемника.

Между этими блоками располагается чувствительный элемент – специальный оптоволоконный кабель. Обработка сигналов осуществ­ляется с помощью анализатора или с помощью специального обучае­мого процессора, использующего принципы искусственного интел­лекта. Обучение процессора происходит после монтажа на конкрет­ном объекте с имитацией реальных сигналов вторжения.

**4. Емкостные системы охраны периметров**

*Датчик емкостной системы представляет собой один или несколько металлических электродов, укрепленных на изоляторах вдоль ог­рады, и является, по сути дела, антенной системой*. Такая система часто выполняется в виде металлического козырька и устанавли­вается с помощью специальных стоек и изоляторов на уже сущест­вующем ограждении. *Наиболее эффективны на объектах, оборудо­ванных прочными жесткими оградами* (железобетонные плиты, кирпичные стены, сварные металлические панели и т.п.).

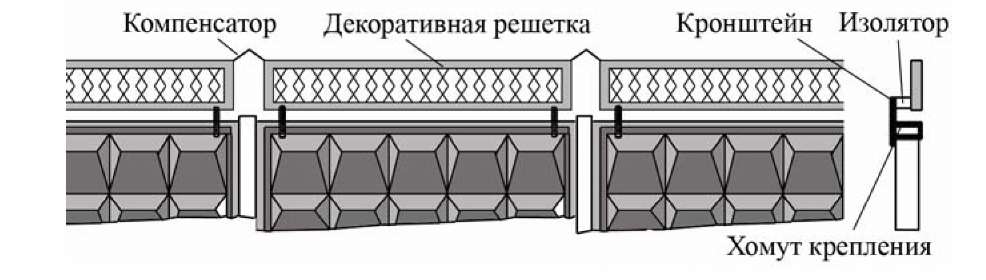


Рис. 10. Антенная система емкостного датчика – декоративный козырек на бетонной стене

На рис. 10 показана конструкция антенной системы емкостно­го датчика в виде декоративной металлической решетки, укреплен­ной на бетонной стене. Все секции решетки соединены в общий электрический контур и изолированы от основной ограды.

*Антенная система подключается к электронному блоку, гене­рирующему электрический сигнал и измеряющему емкость антен­ной системы. Когда человек приближается к электродам или каса­ется их, емкость антенной системы изменяется, что регистрируется электронным блоком, выдающим сигнал тревоги*.

Конфигурация зоны обнаружения определяется методом креп­ления электродов. При установке основного электрода вдоль верх­него торца ограды система эффективно регистрирует лишь попыт­ки перелезания. Если электроды смонтированы вдоль средней ли­нии ограды, то система срабатывает уже при приближении нару­шителя к периметру.

Наиболее широко применяемыми отечественными средствами охраны периметров, использующими емкостный метод обнаруже­ния, являются приборы серии «Радиан». **Системы «Радиан-М» и «Радиан-13»** предназначены для защиты металлических оград и козырьков, имеющих вид сетчатого, решетчатого или проволоч­ного барьера. Протяженность зоны обнаружения составляет от 10 до 500 м; в комплект поставки входят электронный блок и спе­циальные изоляторы для крепления козырька. Электронный блок имеет размеры 326x207x540 мм; он питается от источника посто­янного тока напряжением 20 ... 31 В, потребляемый ток - 70 мА, диапазон рабочих температур от -50 до +50°С. Система обеспечена мерами грозозащиты.

Усовершенствованная модификация приборов этой серии – **система «Радиан-14».** Она отличается использованием двухканального алгоритма обработки сигналов с анализом «активной» и «ре­активной» составляющих сигнала. Это позволяет отстроиться от помех, создаваемых атмосферными осадками и снизить вероят­ность ложных срабатываний от импульсных радиопомех. Кроме этого, в системе предусмотрено более простое крепление чувстви­тельных электродов на ограде. Конструкторы отказались от специ­альных изоляторов-переходников и проводники антенной системы крепятся на пластмассовых кронштейнах, монтируемых непосред­ственно на ограде.

Типичный чувствительный элемент состоит из трех параллель­ных проводников, образующих над основной оградой барьер высо­той около 0,8 м. В комплект поставки системы «Радиан-14» входят электронный блок, пластмассовые кронштейны, провод антенной системы и крепежный комплект. Длина охраняемого участка – до 500 м, диапазон рабочих температур от -50 до +50°С. Электрон­ный блок имеет размеры 320x223x95 мм; напряжение питания 20 ... 30 В, потребляемая мощность 0,5 Вт.

Одним из наиболее известных у нас зарубежных охранных уст­ройств емкостного типа является **система «Е-Field» фирмы Senstar-Stellar** (США). Сенсор такой системы представляет собой конст­рукцию из трех проводников, устанавливаемых на кронштейнах, которые крепятся к ограде (крыше) или устанавливаются вокруг открытых не огражденных территорий. Центральный передающий электрод антенной системы подключен к источнику сигнала, а два боковых – анализатору (однозонному или двухзонному). Как гене­ратор, так и анализатор смонтированы в общем корпусе.

При попадании нарушителя в зону обнаружения анализатор от­слеживает изменения сигналов и при превышении заданного поро­га активности выдает сигнал тревоги.

Анализатор системы «Е-Field» оценивает сигнал по трем харак­теристикам:

* амплитуда изменения сигнала – она пропорциональна массе нарушителя;
* скорость изменения сигнала – она характеризует скорость движения нарушителя;
* продолжительность возмущения – т.е. время нахождения на­рушителя в зоне охраны.

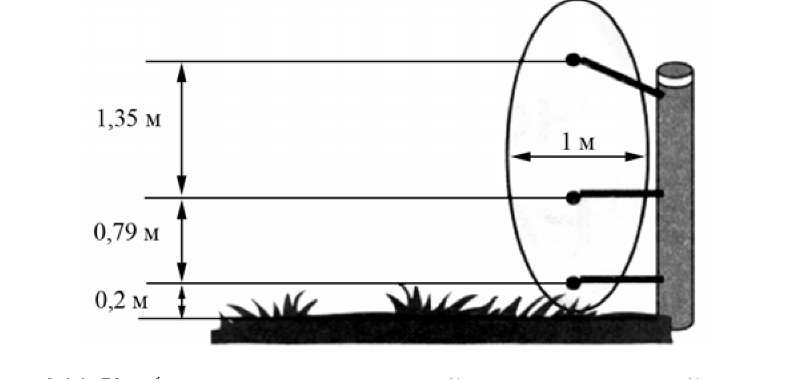


Рис. 11. Конфигурация трехпроводной антенны емкостной системы «Е-Field» и сечение чувствительной зоны

Сигнал тревоги выдается при одновременном наличии всех трех факторов, что обеспечивает весьма низкую вероятность лож­ных срабатываний. На рис. 11 показана типовая конфигурация трехпроводной антенной системы «Е-Field» и поперечное сечение чувствительной зоны. Система «Е-Field» может эффективно при­меняться для обнаружения разрушения ограды или перелезания через нее, а также для обнаружения подкопов или приближения нарушителя к линии периметра.

*Емкостные периметровые системы весьма универсальны и при­влекательны своей нечувствительностью к неровностям профиля почвы или линии ограды*.

Отечественные емкостные охранные системы в целом отлича­ются достаточно высокой надежностью и широко используются на различных объектах в течение последних 20-30 лет.

**5. Вибрационные системы с сенсорными кабелями**

*Принцип действия таких систем основан на регистрации меха­нических вибраций или перемещений ограды, возникающих при попытках нарушителя разрушить или преодолеть периметр. Чувст­вительным элементом таких систем обычно является сенсорный кабель, преобразующий механические вибрации в электрический сигнал*. Кабель крепят либо непосредственно к ограде, либо к спе­циальному легкому металлическому козырьку над ней. Сигналы кабеля обрабатываются анализатором, который в соответствии с заданным алгоритмом выдает сигнал тревоги. Ниже мы кратко рас­смотрим некоторые отечественные и зарубежные системы с сен­сорными виброчувствительными кабелями.

В широко известных российских периметровых **системах Арал и Дельфин** в качестве чувствительного элемента используется многопроводный телефонный кабель. При деформации кабеля в изоли­рующих оболочках наводятся электрические заряды (трибоэлектрический эффект), которые создают импульсные потенциалы ме­жду проводниками. Чувствительный элемент является своеобраз­ным протяженным микрофоном, поэтому такой кабель иногда на­зывают также микрофонным.

*Система Арал предназначена для установки на сварных метал­лических сетках типа ССЦП*. В качестве чувствительного элемента используется 10-парный телефонный кабель типа ТППэп 10x2x0,35, который на ограде высотой около 2 м рекомендуется монтировать в два прохода. Кабель подключается к электронному блоку системы (анализатору), который обрабатывает сигналы сен­сора и выдает сигнал тревоги, если нарушитель пытается перере­зать ограду или перелезть через нее.

Длина зоны обнаружения в благоприятных условиях может достигать 500 м, однако рекомендуемая длина реальной зоны обычно не превышает 250-300 м. Электронный блок системы Арал имеет габариты 95x225x320 мм; он питается от источника посто­янного тока с напряжением 10 – 30 В, номинальная потребляемая мощность – 0,5 Вт, диапазон рабочих температур от –50 до +50°С. Система снабжена элементами грозозащиты.

Более совершенная **система Дельфин-М** (рис. 12) по своим техническим характеристикам и тактике применения аналогична системе Арал, но отличается более современными схемными реше­ниями.

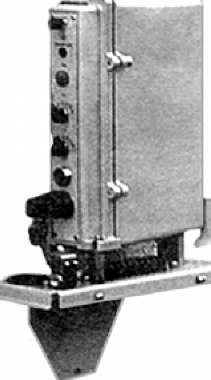


Рис. 12. Электронный блок (анализатор сигналов сенсо­ра) периметровой охранной системы Дельфин-М

*Дельфин-М также предназначен для защиты оград из свар­ных металлических сеток; рекомендуемая длина одной зоны охра­ны составляет 250 м* (до 500 м для прямых однородных участков периметра). Система Дельфин-М обеспечивает возможность ка­либровки чувствительности под конкретную ограду и позволяет автоматически отстраиваться от индустриальных помех. Электрон­ный блок Дельфин-М (рис. 12) выполнен в пылевлагозащищенном корпусе с габаритами 90x220x330 мм; потребляемая мощность составляет 0,1 Вт при напряжении питания 20...30 В, диапазон рабочих темпе­ратур от -50 до +50°С.

В большин­стве зарубежных вибрационных пе­риметровых систем используется специальный коаксиальный кабель, работающий также на трибоэлектрическом эффекте. Такой кабель применен, например, в системе Intelli-Flex, выпускаемой американ­ской компанией Senstar-Stellar. Трибоэлектрический коаксиальный ка­бель позволяет защищать ограды из сварной решетки или проволочной сетки типа «рабица». *Система реги­стрирует попытки перелезть через ограду, перекусить ее ячейки или приподнять сетку*. **Электронный блок системы Intelli-Flex** анализирует количество импульсов в за­данном временном окне (перерезание ограды), а также интеграль­ную энергию сигнала при длительных воздействиях (перелезание). На стандартном для США и Европы ограждении из сетки высотой до 2,5 м кабель можно устанавливать в один проход; двухпроходная конфигурация рекомендуется для обеспечения большей надеж­ности. В последнем случае кабель крепится вдоль верхней и ниж­ней кромок на расстояниях, равных одной трети высоты ограды. Максимальная длина защищаемой зоны может достигать 300 м (2x300 м при использовании двухзонного анализатора).

Для настройки системы Intelli-Flex используется специальный программатор (рис. 13), который подключается к электронному блоку и фиксирует сигналы, сопровождающие попытки реального преодоления периметра.



Рис. 13. Программатор для настройки анализатора сис­темы Intelli-Flex фирмы Senstar-Stellar (США)

Записанные программатором сигналы ис­пользуются затем в качестве критериев обнаружения вторжения. Для каждой зоны охраны требуется индивидуальная настройка анализатора на нескольких участках зоны. Предусмотрена возмож­ность установки на каждом анализаторе специального погодного датчика для мониторинга текущих погодных условий и адаптации алгоритма обработки сигналов.

Двухзонный электронный блок обработки (анализатор) системы Intelli-Flex имеет размеры 260x210x108 мм. Питание осущест­вляется от источника напряжением 11 ... 24 В; потребляемый ток –70 мА. Диапазон рабочих темпера­тур от – 40 до +70°С.

Английская компания Advanced Perimeter Systems (APS) выпускает **систему Flexiguard**, также исполь­зующую в качестве чувствительного элемента специальный коаксиальный трибоэлектрический кабель. Для типовых периметров система выпускается в двух основных модификациях: FG2000 - для легких металлических оград (сетка типа «рабица» и сварная проволочная решетка) и FG2500 - для так называемых «палисадных» европейских оград, выполненных из штампованных стальных тонкостенных элементов.

**Система FG5000** фирмы APS предназначена для охраны пери­метров взрывоопасных объектов – нефтехимических предприятий, газовых станций, складов взрывчатых веществ и т.п. Модификация FG3000 используется для охраны стен и крыш зданий.

Сенсорный кабель Flexiguard крепится непосредственно к сет­чатой ограде с помощью пластиковых стяжек, устанавливаемых через каждые 100 мм. Кабель отличается высокой гибкостью и прочностью, что упрощает процесс его монтажа. Сенсор подклю­чается к анализатору FS200, оснащенному системой автоматиче­ского контроля окружающей среды. Эта система позволяет отстро­иться от сигналов, вызванных климатическими воздействиями (дождь, ветер, град), и тем самым заметно снизить частоту ложных срабатываний.

Максимальная длина зоны охраны составляет 300 м; для управ­ления системой фирма APS выпускает специальные контрольные панели FG10 и FG20 на 10 и 20 зон соответственно. Кроме визу­ального контроля сигналов тревоги эти панели позволяют прослу­шивать звуковые сигналы сенсора, помогающие идентифицировать тип вторжения.

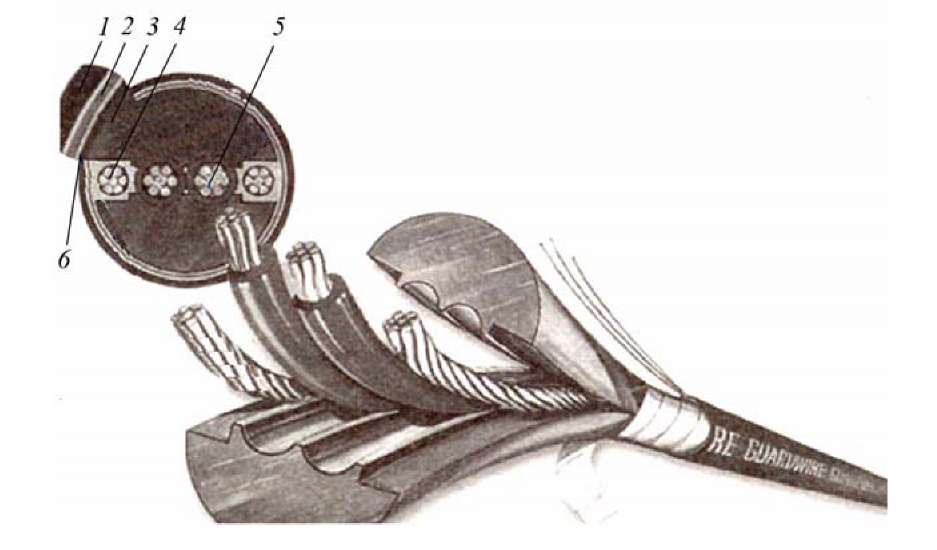
Интересен принцип, положенный в основу работы **отечествен­ной периметровой системы Дрозд**. *Роль сенсорного кабеля выполняет обычный полевой провод П-274, который, перемещаясь в маг­нитном поле земли, генерирует электрический сигнал. Сигналы сенсора обрабатываются специальным электронным блоком*. Сис­тема выпускается в нескольких вариантах. *На бетонных, кирпичных и деревянных оградах* (вариант системы под названием Дрозд-01) чувствительный элемент монтируется в несколько лучей на крон­штейнах, устанавливаемых по верхнему торцу ограды. *При монта­же на сетчатых оградах* (вариант Дрозд-02) сенсор закрепляют не­посредственно на ограде; при этом система регистрирует как пере­резание ограды, так и перелезание через нее. *При использовании на колючей проволоке* (вариант Дрозд-03) кабель крепят на опорах параллельно основной ограде; для перекрытия зоны высотой 2,4 м требуется 12... 13 лучей чувствительного кабеля. Варианты поста­вок отличаются комплектацией монтажных приспособлений. Мак­симальная протяженность участка периметра, защищаемого систе­мой Дрозд, равна 500 м. Электронный блок системы питается на­пряжением 10 ... 30 В и потребляет мощность всего 0,12 Вт. Габа­риты электронного блока – 220x330x90 мм, диапазон рабочих тем­ператур от –50 до +50°С.

Обнаруживающая способность и вероятность ложных срабаты­ваний периметровых систем определяется главным образом каче­ством чувствительного элемента (сенсорного кабеля или другого датчика).

Поэтому к наиболее совершенным виброчувствительным рас­пределенным сенсорам можно отнести специально разработанные электромагнитные микрофонные кабели. При перемещении или вибрациях кабеля в его проводниках индуцируется напряжение по­добно тому, как это происходит в обычных электромагнитных микрофонах. Для таких сенсоров характерна высокая верность вос­произведения вибраций ограды и высокое отношение сигнал/шум, обусловленное низкоомной природой самого датчика.

Примером *электромагнитного микрофонного кабеля является* **сен­сор GW400k серии Guardwire**, разработанный и выпускаемый ком­панией Geoquip (Великобритания). Сенсорный кабель (рис. 14) содержит два неподвижных и два подвижных проводника, распо­ложенных в зазоре между двумя полосками полукруглого сечения, выполненными из гибкого магнитного полимера. Сердечник кабеля покрыт изолирующим слоем майлара и экраном из алюминиевой фольги, к которому подключен провод заземления. Снаружи сенсорный кабель защищен прочной полиэтиленовой оболочкой.

*Сенсорный кабель Guardwire монтируется непосредственно на ограде и воспринимает вибрации, создаваемые нарушителем*. Под­вижные проводники при этом перемещаются в зазорах полимерных магнитов и в них наводится электрическое напряжение, которое регистрируется и обрабатывается анализатором.

Рис. 14. Конструкция электромагнитного микрофонного сенсорного

кабеля типа GW400k:

1 - внешняя защитная оболочка; 2 - металлический экран; 3 - полимер­ные гибкие магниты; 4 - подвижные проводники; 5 - неподвижные про­водники; б - майларовая пленка

Анализаторы системы Guardwire обеспечивают двухканальную обработку сигналов, необходимую для регистрации двух основных типов вторжения: перелезания через ограду (продолжительное воз­действие) или разрушения ограды (ударное воздействие). Чувстви­тельность системы устанавливается независимо по каждому кана­лу. Сменные фильтры позволяют подавлять помехи (например, от ветра или дождя) и оптимизировать отклик системы для заданного типа ограды. В канале регистрации ударных воздействий («переле­зания ограды») задается длительность временного окна и опреде­ленное количество событий, после которых анализатор включает сигнал тревоги. Максимальная длина зоны охраны - 400 м.

Аппаратура серии Guardwire предназначена для защиты периметровых оград из металлической сетки, тонкой сварной решетки, колючей проволоки или сравнительно легких оград из дерева. *Для более массивных оград (тяжелых сварных или кованых решеток и т.п.) компания Geoquip выпускает* **систему Defensor** *с усовершенст­вованным сенсорным кабелем типа GDALPHA* (рис. 15).

Этот кабель содержит только два проводника, которые поме­щены в полиэтиленовые трубки с силиконовой смазкой, обеспечи­вающие повышение подвижности проводников и, соответственно, уровня сигнала. Для минимизации внешних наводок активные про­водники сформированы в виде витой пары. Центральный много­жильный провод выполняет роль упрочняющего элемента и огра­ничивает термические деформации сенсорного кабеля.

Рис. 15. Сенсорный кабель GD ALPHA

Анализатор системы Defensor по своим техническим и эксплуа­тационным характеристикам близок к системе Guardwire. Он имеет размеры 140x220x75 мм; напряжение питания 10 – 24 В, потреб­ляемый ток - 60 мА. Система работоспособна при температурах от –50 до +70°С.

Оба анализатора имеют стандартные релейные выходы, конфигу­рируемые как нормально замкнутые или нормально разомкнутые.

Кроме реле тревоги, анализатор содержит реле отказа, сигнали­зирующее о повреждении кабеля, вскрытии блоков системы или отключении питания в зоне. *Анализаторы Guardwire и Defensor также имеют выходы звукового канала, что позволяет оператору прослушивать обстановку в каждой зоне и идентифицировать сиг­нал вторжения на слух*.

Обе системы Guardwire и Defensor отличаются тем, что не нуж­даются в адаптации к погодным условиям или сезонной подстройке параметров. Обе системы также не требуют программатора или компьютера со специальным программным обеспечением при на­стройке и эксплуатации.

Американская компания Senstar-Stellar предлагает **радиоволно­вое устройство «Н-Field» с кабелями**, укладываемыми непосредст­венно в землю. *Такая система предназначена для охраны открытых пространств, подступов к объектам* и т.п. Два параллельных кабеля (приемный и передающий) закапываются в любой грунт на глубину 10 - 15 см и на расстоянии примерно 2 м друг от друга (рис. 16). Вокруг кабелей над поверхностью почвы формируется электромаг­нитное поле (зона обнаружения) шириной З м и высотой 1 м. Мак­симальная длина одной зоны обнаружения – 150 м. Кабели под­ключаются соответственно к приемнику и передатчику (или к об­щему приемо-передающему блоку – трансиверу).

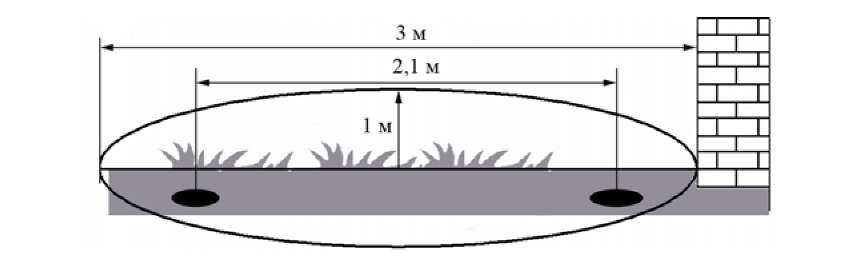


Рис. 16. Схема расположения кабелей системы «Н-Field»

Эффективность детектирования нарушителя обеспечивается тем, что для выбран­ной частоты человеческое тело представляет собой как бы антенну размером в 1/4 длины радиоволны и поэтому нарушитель сильно изменяет параметры принимаемого сигнала.

Алгоритм обработки сигналов в системе «Н-Field» предполага­ет выполнение трех условий:

* масса попавшего в зону объекта должна быть больше заранее установленного значения (масса человеческого тела);
* объект должен двигаться со скоростью, не меньшей опреде­ленного значения (в диапазоне скоростей человека);
* оба указанных условия выполняются в заданном интервале времени.

Система «Н-Field» обеспечивает скрытную установку датчиков при произвольном профиле линии охраны. Кабели нечувствитель­ны к сейсмическим и акустическим воздействиям, их можно мон­тировать в грунте, под асфальтовыми дорогами и др.

**6. Вибрационно-сейсмические системы**

*Эти системы, также как и системы с виброчувствительными ка­белями, реагируют на колебания или деформации контактирующей с ними среды. Однако здесь обычно используются датчики, уста­навливаемые непосредственно в грунт или на массивные стены, и регистрирующие низкочастотные (сейсмические) колебания (сме­щения) почвы или стены*.

Системы, как правило, обеспечивают скрытую установку и позво­ляют защитить как огражденные, так и не огражденные периметры.

**Российская система «Дуплет»** *относится к сейсмомагнитометрическим средствам обнаружения*. Чувствительным элементом уст­ройства является специальный кабель КТПЭДЭП 10x2x0,5 с двойным экранированием, укладываемый непосредственно в грунт на глу­бине 30 – 40 см вдоль охраняемого периметра. Кабель регистриру­ет как сейсмические сигналы (колебания грунта), возникающие при прохождении нарушителя, так и локальные изменения магнитного поля при движении ферромагнитных предметов. Три линии кабеля располагаются параллельно (рис. 17) на расстоянии 1 м друг от друга, обеспечивая зону чувствительности шириной 3 м; макси­мальная протяженность одной зоны равна 500 м. *Замаскированность подземных сенсоров делает систему невидимой для наруши­теля*. При необходимости под землей можно установить и элек­тронные блоки, поместив их в специальные контейнеры.

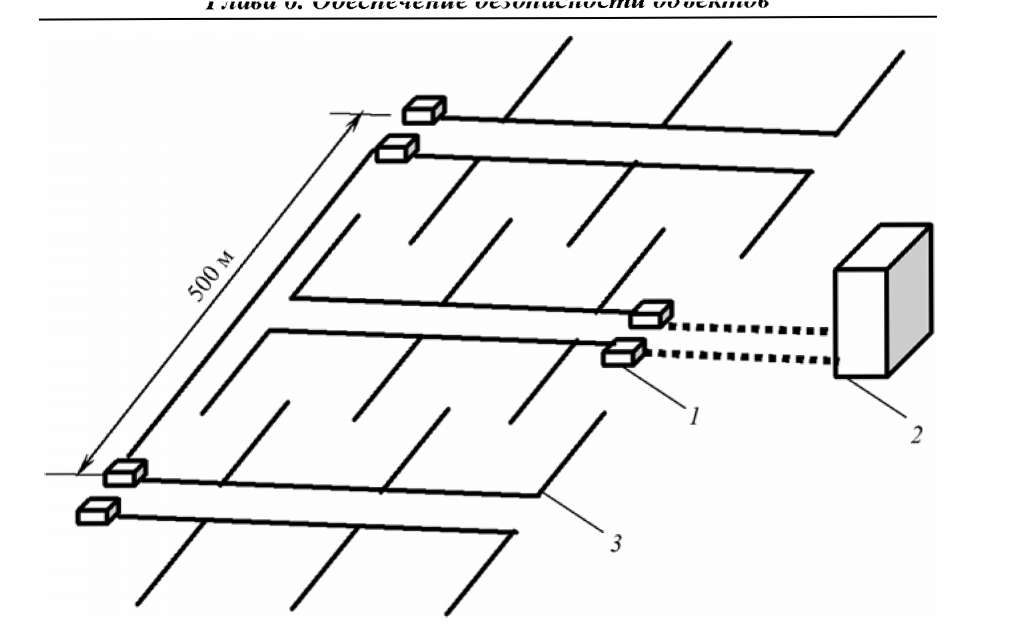


Рис. 17. Сейсмомагнитометрическая периметровая система «Дуплет»: 1 - коммутационные коробки; *2 -* блоки усилителей; 3 – чувствительный кабель

В однозонный комплект системы «Дуплет» входят шесть лучей сенсорного кабеля с коммутационными коробками, два блока уси­лителей, блок обработки сигналов и комплект монтажных принад­лежностей. Электронные блоки питаются от источника с напряже­нием 20 ... 30 В и потребляют мощность 1,5 Вт; диапазон рабочих температур системы от -50 до +50°С.

К сожалению, система воспринимает не только сигналы наруши­теля, но другие сейсмические сигналы, поэтому в полосе обнаружения не должно быть деревьев или крупных кустов, так как система может срабатывать при перемещениях их корней. По этим же при­чинам минимальное расстояние от сенсора до дорог с автомобиль­ным движением должно составлять 10 м, а до высоковольтных ли­ний электропередач – 50 м.

При обслуживании системы предусмотрены сезонные регла­ментные работы, во время которых производится подстройка систе­мы с учетом реального состояния грунта.

Одной из наиболее совершенных вибросейсмических **систем является периметральный комплекс Psicon**, выпускаемый англий­ской компанией Geoquip.

*Здесь в качестве сенсоров использованы дискретные сейсмиче­ские датчики, иногда называемые геофонами* (рис. 18). Такой датчик представляет собой проводящую обмотку и помещенный внутрь нее магнитный сердечник, который может свободно коле­баться вдоль оси обмотки.

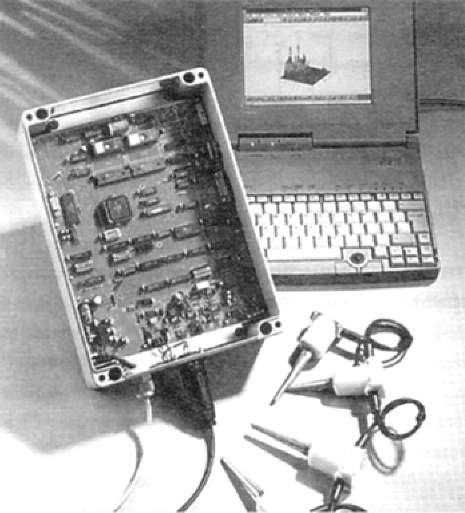


Рис. 18. Геофонные датчики и анализатор вибросейсмической периметральной системы Psicon фирмы Geoquip (Великобритания)

При колебании магнита в катушке наводится напряжение, реги­стрируемое анализатором. *Геофонные датчики собирают в луч необходимой длины и помещают под землю или прикрепляют к ог­раде*. Высокая чувствительность геофонных датчиков позволяет регистрировать весьма слабые сигналы и обнаруживать нарушите­ля, преодолевающего, например, массивную бетонную или кир­пичную стену. При монтаже геофонов под землей система Psicon надежно обнаруживает осторожно идущего или ползущего челове­ка или нарушителя, спрыгнувшего с ограды.

В типовой конфигурации однозонная система Psicon содержит 4 луча, в каждый из которых включено по 16 дискретных геофон­ных датчиков. Расстояние между датчиками равно 3,2 м и общая длина одной охраняемой зоны составляет около 100 м. Все 64 дат­чика подключены к общему анализатору, который обрабатывает сигналы и выдает сигнал тревоги при локализации вторжения с точностью, соответствующей длине одного луча (50 м). Геофонные датчики помещают в герметические жесткие корпуса размерами 110x75x35 мм. Все датчики соединяются армированным много­жильным кабелем и поставляются в виде готовых к укладке в зем­лю лучей. Диапазон рабочих температур датчиков от – 40 до +100°С.

Высокая чувствительность геофонных датчиков системы делает необходимой использование мощного «интеллектуального» про­цессора для обработки сигналов и фильтрации помех, создаваемых окружающей средой (шум транспорта, движение корней деревьев, дождь и т.п.). В системе Psicon для этого используется разработан­ная фирмой Geoquip технология, получившая название TESPAR. Система преобразует аналоговый сигнал датчиков в цифровую ко­довую последовательность, которая затем подвергается матрично­му преобразованию в анализаторе. Последний использует принцип распознавания образов и сравнения их с эталонными, записанными в памяти анализатора.

Сравнение происходит в реальном времени и позволяет надеж­но распознать слабые сигналы нарушителя на фоне даже весьма интенсивных помех или шумов. Систему можно «обучать» непо­средственно на объекте, сохраняя в памяти процессора как «тре­вожные», так и «нетревожные» сигналы. Для настройки системы используется портативный компьютер, подключаемый к порту электронного блока.

Анализатор Psicon имеет габариты 400x300x110 мм и потреб­ляет ток 500 мА при номинальном напряжении источника 12 В. Диапазон рабочих температур анализатора от -25 до +70°С.

**7. Радиолучевые системы**

Такие *системы содержат приемник и передатчик СВЧ сигналов, которые формируют зону обнаружения в виде вытянутого эллип­соида вращения* (рис. 19).

Длина отдельной зоны охраны определятся расстоянием между приемником и передатчиком, а диаметр зоны варьируется от долей метра до нескольких метров.

*Принцип действия таких систем основан на анализе изменений амплитуды и фазы принимаемого сигнала, возникающих при появ­лении в зоне постороннего предмета*.

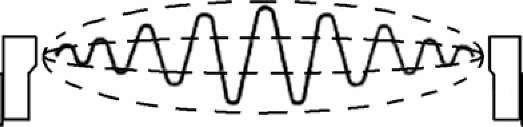


Рис. 19. Принцип действия радиолучевой системы

Системы применимы там, где обеспечивается прямая видимость между приемником и передатчи­ком, т.е. профиль поверхности должен быть достаточно ровным и в зоне охраны должны отсутствовать кусты, крупные деревья и т.п.

Перекрытие площади поперечного сечения электромагнитного луча телом нарушителя можно представить формулой:

*Рип* = β0(1 + *т*)*Ри*,

где Ри – мощность сигнала передатчика на входе передающей ан­тенны; *Рип* – мощность полезного сигнала на выходе приемной ан­тенны; β0 – коэффициент передачи радиолокационного сигнала при отсутствии нарушителя; *т* – коэффициент модуляции полез­ного сигнала нарушителем.

При движении нарушителя в полный рост (*т* = 0,5...0,9) изме­нение β0 (1 + *т*) составляет 3-10 дБ. При перемещении нарушителя ползком (т = 0,1...0,25) изменение β0 (1 + *т*) составляет 0,4... 1,0 дБ.

*Применяют радиолучевые системы как при установке вдоль ог­рад, так и для охраны не огражденных участков периметров. Эти системы обычно рассчитаны на обнаружение нарушителя, который преодолевает рубеж охраны в полный рост или согнувшись*.

Общим недостатком радиолучевых систем является наличие «мертвых» зон – чувствительность системы понижена вблизи при­емника и передатчика, поэтому приемники и передатчики соседних зон должны устанавливаться с перекрытием в несколько метров. Кроме того, радиолучевые системы недостаточно чувствительны непосредственно над поверхностью земли (30 - 40 см), что может позволить нарушителю преодолеть рубеж охраны ползком.

Относительно широкая зона чувствительности системы обу­славливает ограниченность ее применения на объектах, где воз­можно случайное попадание в зону обнаружения людей, транспор­та и т.п. В таких ситуациях для предотвращения ложных срабаты­ваний рекомендуется с помощью дополнительной ограды оборудо­вать предзонник.

Блоки радиолучевых систем устанавливают либо на грунте (с помощью специальных стоек), либо на ограде или стене здания. При установке системы на грунте требуется подготовить охраняе­мую зону - спланировать территорию, удалить кустарники, деревья и посторонние предметы. При эксплуатации необходимо периоди­чески выкашивать траву и убирать снег. При значительной высоте снежного покрова (более 0,5 м) необходимо изменить высоту креп­ления блоков на стойках и провести их дополнительную юстировку.

Широкий спектр радиолучевых охранных приборов выпускает итальянская компания CIAS. **Приборы серии Ermusa** отличаются ком­пактностью и предназначены для использования как в помещениях, так и на улице для барьеров протяженностью 40 — 80 м. На рис. 19 показаны блоки радиолучевой системы ERMO 482 фирмы CIAS.

Рис. 19. Система ERMO 482

Приборы выпускаются в не­скольких модификациях – для ру­бежей протяженностью 50, 80, 120 и 200 м. *Используемые в блоках па­раболические антенны обеспечива­ют малую расходимость луча, что позволяет использовать эту систему даже в условиях интенсивного го­родского движения*. Частота излу­чения передатчика составляет 10,58 ГГц, питание – от аккумуляторной батареи или сетевого адаптера. Диаметр блока – 310 мм, глубина – 270 мм, масса – 3 кг. Блоки монти­руются на сборных металлических штангах, позволяющих устанавли­вать излучатель и приемник на вы­соте до 1 м. Со штангой конструк­тивно объединена коробка для бло­ка питания и аккумулятора. Диапа­зон рабочих температур от –25 до +55°С.

Все перечисленные системы обеспечивают только одну зону охраны и применяются на прямолинейных участках периметра. На участках с непрямолинейной границей или при сложном рельефе местности нужно использовать многозонную систему, состоящую из нескольких комплектов аппаратуры. Для небольших объектов были разработаны многозонные радиолучевые системы, имеющие один общий блок обработки сигналов.

**8. Системы «активной» охраны периметров**

*В некоторых случаях систему периметровой сигнализации объ­единяют со средством активного отпугивания нарушителя с помо­щью короткого электрического импульса (электрошока), неопасно­го для жизни человека*. Английская компания APS в своей **системе Electro-Fence** предлагает использовать для этих целей барьер или козырек из нескольких параллельно натянутых проводников. На­рушитель, пытающийся перелезть через такой барьер, подвергается действию короткого (менее 1 мс) электрического импульса, кото­рый не угрожает его жизни и не приносит вреда его здоровью, но является весьма неприятным для человека и заставляет отказаться от попыток перелезть через барьер или перерезать его. *При контак­те нарушителя с барьером, кроме отпугивающего импульса, систе­ма генерирует также сигнал тревоги*.

Такие барьеры можно устанавливать на уже существующих ог­раждениях или ставить отдельно от них. Стальные проводники диаметром 2,5 мм располагают на расстояниях 95 мм друг от друга и натягивают между металлическими стойками по всей высоте барьера (от 1 до 3 м). Эти проводники одновременно выполняют роли сенсоров и электрошоковых электродов. Контроллер системы Electro-Fence может управлять одной, двумя или шестью зонами охраны. Он регистрирует попытки вторжения и генерирует сигнал тревоги, контролирует напряжение на проводниках, а также детек­тирует попытки обрезать или замкнуть проводники.

**Электрошоковое устройство периметровой охраны фирмы G.M.** (Израиль) – это активная система обнаружения нарушителя, кото­рая реагирует на попытку вторжения, отражает нападение наруши­теля, замедляет время преодоления рубежа.

Конструктивно линей­ная часть устройства представляет собой проводное электризуемое заграждение различной конфигурации и может применяться:

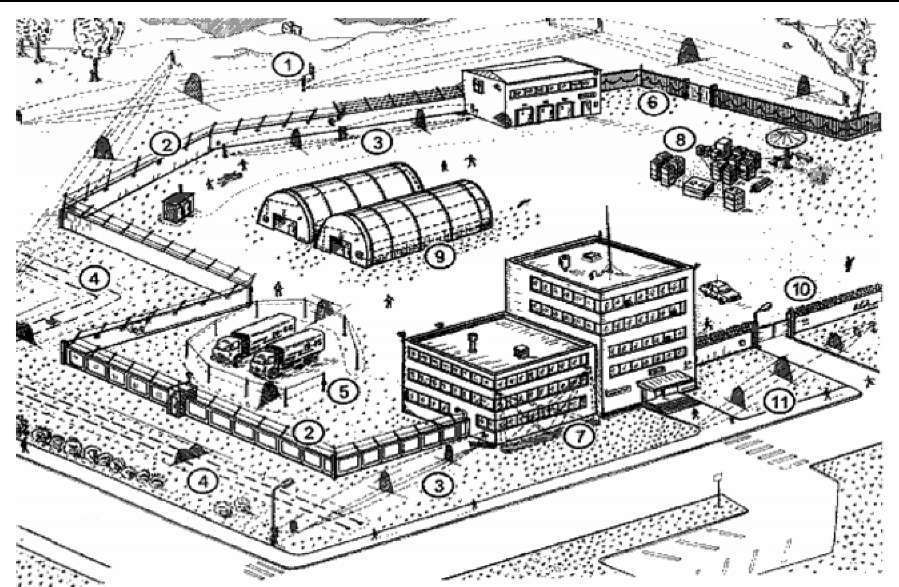
* на заборах любого типа в виде козырька;
* поверху стен и крыш в виде козырька;
* совместно с существующим забором в виде второго забора;
* как отдельно стоящий забор.

Устройство имеет выходное реле с «сухими контактами» для подключения к любому приемно-контрольному оборудова­нию. Управляющий контроллер с цифровым микропроцессорным управлением и преобразователем напряжения обеспечивает свето­диодную индикацию:

* импульсов высокого напряжения на выходе;
* тревоги по шлейфам высокого и низкого напряжения раздельно;
* разряда батарей.

**Пример применения средств обнаружения различных типов на участках периметра условного объекта**

(размеры зон обнаружения, элек­тронные блоки и элементы показаны в разных масштабах)



1 - радиолучевое; 2 - радиоволновое; 3 - радиолучевое; 4 - радиоволно­вое (на основе «линии вытекающей волны»); 5 - радиоволновое однопроводное; 6 - вибросейсмическое; 7 - инфракрасное пассивное; 8 - обрыв­ное с указанием места обрыва микропровода; 9 - вибрационное кабель­ное; 10 - емкостное; 11 - радиолокационное (с возможностями организации прохода).

**Литература**

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.
3. Корнеев И.К. Защита информации в офисе: Учебник/Гос. ун-т управления; И.К.Корнеев, Е.А. Степанов.- М.:Проспект,2011.-336 с.
4. Зегжда Д.П., Ивашко A.M. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2009.